Guide to working with authentication and single sign-on support in ForgeRock® Access Management (AM). ForgeRock Access Management provides intelligent authentication, authorization, federation, and single sign-on functionality.
Table of Contents

Overview ....................................................................................................................... v
1. Introducing Authentication ....................................................................................... 1
   About Multi-Factor Authentication ........................................................................ 2
2. Configuring AM for Authentication ......................................................................... 3
   Authentication Nodes and Trees ........................................................................... 4
   Authentication Modules and Chains ..................................................................... 17
   Configuring Success and Failure Redirection URLs ............................................. 50
   Configuring Realm Authentication Properties ...................................................... 54
3. Authenticating (Browser) ......................................................................................... 56
   Specifying the Realm in the URL ........................................................................ 56
   Authentication Parameters .................................................................................. 56
4. Authenticating (REST) ............................................................................................. 60
   Logging in to AM Using REST ............................................................................ 60
   Using the Session Token After Authentication ..................................................... 66
   Logging out of AM Using REST ........................................................................... 67
   Invalidating All Sessions for a Given User ........................................................... 67
5. Single Sign-On ........................................................................................................ 70
   About Realms and SSO ....................................................................................... 72
   About HTTP Cookies ........................................................................................... 72
   Implementing CDSSO .......................................................................................... 73
   Troubleshooting SSO ........................................................................................... 73
6. Social Authentication ............................................................................................... 75
   Configuring the Social Authentication Implementations Service ........................... 79
7. Suspended Authentication ....................................................................................... 81
8. MFA: Web Authentication (WebAuthn) ................................................................. 83
   Creating Trees for Web Authentication (WebAuthn) ............................................ 83
   Configuring Usernameless Authentication with ForgeRock Go ............................. 86
   Configuring WebAuthn Trust Anchors ................................................................. 91
9. MFA: Push Authentication ....................................................................................... 95
   Creating Trees for Push Authentication ............................................................... 96
   Creating Chains for Push Authentication ........................................................... 101
   Testing Push Authentication .............................................................................. 108
   Limitations When Using Passwordless Push Authentication ............................... 112
10. MFA: Open AuTHentication (OATH) ................................................................. 113
    Differences Among Authentication Modules That Support HOTP ....................... 113
    Creating Chains for One-Time Password Authentication .................................... 114
    Letting Users Opt Out of One-Time Password Authentication (OATH) ............ 119
11. Managing Devices for MFA ................................................................................... 123
    The ForgeRock Authenticator App ..................................................................... 123
    Recovering After Replacing a Lost Device .......................................................... 128
    Recovering After a Device Becomes Out of Sync .............................................. 129
    Resetting Registered Devices by using REST ..................................................... 129
12. Reference ............................................................................................................ 131
    Core Authentication Attributes .......................................................................... 131
Overview

This guide covers concepts, implementation procedures, and customization techniques for working with the authentication and single sign-on features of ForgeRock Access Management.

This guide is written for anyone using Access Management to manage authentication and implement single sign-on.

Quick Start

Configure AM for Authentication
Learn about AM’s authentication features and provide your users with different authentication mechanisms to log in to your applications.

Multi-Factor Authentication
Require that your users provide multiple forms of identification when logging in to services. For example, one-time passwords, push messages, or by using WebAuthn.

Single Sign-On
Enable single sign-on (SSO) so that your users can access multiple, independent services by logging in once with a single set of credentials.

Social Authentication
Allow your users to authenticate to your services by using third-party identity providers, such as Facebook, Google, and VKontakte.

About ForgeRock Identity Platform™ Software

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

Authentication is the act of confirming a user's identity, for example, by providing a set of credentials.

In access management, authentication is tightly coupled with authorization; usually, not only is it important to confirm that a user is who they say they are, but also to ensure that they can only access a subset of information.

Consider a user who wants to access an online shop. As the owner of the shop, you want to ensure the user identity is confirmed (since it is tied to their shipping and email addresses and payment information) and you also want to ensure that they can only access their own information.

With AM, you can deploy a ForgeRock Web Agent on the web server hosting the online shop. The agent redirects the user's request to an AM login page, where the user enters their credentials, such as username and password. AM determines who the user is, and whether the user has the right to access the protected page. AM then redirects the user back to the protected page with authorization credentials that can be verified by the agent. The agent allows the user authorized by AM to access the page.

In the same way, you can also use AM to protect physical devices connected on the Internet of things (IoT). For example, a delivery van tracking system could have its proxying gateway authenticate to a brokering system using an X.509 certificate to allow it to enable an HTTPS protocol and then connect to sensors in its delivery trucks. If the X.509 certificate is valid, the brokering system can monitor a van's fuel consumption, speed, mileage, and overall engine condition to maximize each van's operating efficiency.

AM supports the following features to implement authentication, authentication modules and chains and authentication nodes and trees.

Important

Authentication nodes and trees are replacing authentication modules and chains. We recommend that you implement nodes and trees when possible.

AM creates an authentication session to track the user's authentication progress through an authentication chain or tree. Once the user has authenticated, AM creates a session to manage the user's access to resources. To learn more about sessions, see the Sessions Guide.
About Multi-Factor Authentication

Multi-factor authentication (MFA) is an authentication technique that requires users to provide multiple forms of identification when logging in to AM.

Multi-factor authentication provides a more secure method for users to access their accounts with the help of a device. Note that the word device is used in this section to mean a piece of equipment that can display a one-time password or that supports push notifications using protocols supported by AM multi-factor authentication. Devices are most commonly mobile phones with authenticator apps that support the OATH protocol or push notifications, but could also include other equipment.

The following is an example scenario of multi-factor authentication in AM:

1. An AM administrator configures an authentication tree to capture the user's username and password and to create one-time passwords.
2. An end user authenticates to AM using that authentication tree.
3. AM prompts the user to enter the username and password—the first factor in multi-factor authentication.
4. If the user ID and password were correct, AM sends the user an email with a one-time password.
5. The user provides the one-time password to AM to successfully complete authentication—the second factor in multi-factor authentication.

AM supports the following multi-factor authentication protocols:

• Open AuTHentication (OATH), to enable one-time password authentication.
• Push Notifications, to receive push notifications in a device as part of the authentication process.
• Web Authentication (WebAuthn), to enable authentication using an authenticator device, such as a fingerprint scanner.
Chapter 2
Configuring AM for Authentication

AM provides the following features to authenticate users:

- **Authentication Nodes and Trees.** AM provides a number of authentication nodes to handle different modes of authenticating users. The nodes must be connected together in a tree to provide multiple authentication paths to users.

- **Authentication Modules and Chains.** AM provides a number of authentication modules to handle different modes of authenticating users. The modules also can be chained together to provide multiple authentication mechanisms, so that a user’s or entity’s credentials must be evaluated by one module before control passes to another module.

  **Important**
  
  Authentication nodes and trees are replacing authentication modules and chains. We recommend that you implement nodes and trees when possible.

AM leaves the authentication process flexible so that you can adapt how it works to your situation. Although the number of choices can seem daunting, once you understand the basic process you will see how AM allows you to protect access to a wide range of applications used in your organization.

Authentication happens at realm level in AM. Each realm has its own authentication configuration that is copied from the parent realm at creation time, which may save you some time if you are configuring subrealms.

The following table summarizes the high-level tasks required to configure authentication in a realm:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the Required Authentication Trees or Chains</td>
<td>• &quot;Authentication Nodes and Trees&quot;</td>
</tr>
<tr>
<td>You need to decide how your users are going to log in. For example, you may require your users to provide multiple credentials, or to log in using third-party identity providers, such as Facebook or Google.</td>
<td>• &quot;Authentication Modules and Chains&quot;</td>
</tr>
<tr>
<td>Configure the Realm Defaults for Authentication</td>
<td>• &quot;Configuring Realm Authentication Properties&quot;</td>
</tr>
</tbody>
</table>
## Task

**Configure the Success and Failure URLs for the Realm**

By default, AM redirects users to the console after successful authentication. No failure URL is defined by default.

**Configure an Identity Store in your Realm.**

The identity store you configure in the realm should contain those users that would log in to the realm.

## Resources

- "Configuring Success and Failure Redirection URLs"
- "Identity Stores" in the Setup Guide

## Authentication Nodes and Trees

Authentication trees (also referred to as Intelligent Authentication) provide fine-grained authentication by allowing multiple paths and decision points throughout the authentication flow. Use them to build complex authorization scenarios, while offering a streamlined login experience to users.

Authentication trees are made up of authentication nodes, which define actions taken during authentication. Each node performs a single task during authentication, for example, collecting a username or making a simple decision based on a cookie.

Nodes can have multiple outcomes rather than just success or failure; this allows you to create complex yet customer-friendly authentication experiences by linking nodes together, creating loops, branching the tree for different authentication scenarios, and nesting nodes within a tree:

*Example Authentication Tree*

To further control the authentication process, you can assign authentication levels to branches on a tree, with higher levels being used typically to allow access to more restricted resources.

Authentication trees differ in the following ways to traditional authentication chains:

- Authentication nodes are not yet available for all the functionality provided by authentication modules.
• Authentication trees cannot mix with authentication chains. Each authentication to AM can use either a tree or a chain, but not both together.

• The functionality derived from post-authentication plugins, used traditionally with authentication chains, is handled differently when using trees. For example:
  
  • Session property management is handled by individual nodes. See "Set Session Properties Node".
  
  • Calling out to third-party systems is handled by scripted nodes. See "Scripted Decision Node".
  
  • Registering events to make HTTP POST calls to a server is handled by webhooks. See "Configuring Authentication Webhooks". Note that post-authentication plugins do not get triggered when authenticating to a tree, only to a chain.

About Authentication Levels for Trees

When a user successfully authenticates, AM creates a session, which allows AM to manage the user's access to resources. The session is assigned an authentication level. The authentication level is often used as a measure of the strength of the authentication performed. For example, simple username and password may be assigned a low authentication level, whereas multi-factor with Push and webAuthn, a high one.

Authorization policies may require a particular authentication level to access protected resources. When an authenticated user tries to access a protected resource without satisfying the authentication level requirement, AM denies access to the resource and returns an advice indicating that the user needs to reauthenticate at the required authentication level to access the resource.

The web or Java agent or policy enforcement point can then send the user back to AM for session upgrade. For more information, see "Session Upgrade" in the Sessions Guide.

AM provides the following nodes to manage authentication levels:

• The Authentication Level Decision node, that checks that the current authentication level is equal or greater than the one specified in the node.

• The Modify Authentication Level node, that can raise or lower the authentication level.

Position these nodes to alter the authentication level depending on the route taken through the authentication tree.

About Account Lockout for Trees

It is recommended to limit the number of attempts a user can make at authenticating with credentials. Limiting the number of attempts helps to prevent password-guessing and brute-force attacks.

Authentication trees in AM have built-in support for account lockout, and provide nodes for checking the status of a user, and changing their status:
"Account Active Decision Node"

Use this node to determine if an account is marked as active, or inactive (locked).

"Account lockout Node"

Use this node to alter the user's status, to either active, or inactive (locked).

Note

When setting an account to active, the node will also reset the failed attempts and lockout duration counters.

In addition to the lockout-specific nodes above, the Success and Failure nodes include account lockout functionality, when lockout is enabled in a realm, as follows:

Success node:

- Checks the User Status property of the user profile, when reached, and fails the authentication with an error message, if the account is marked as Inactive:

  ![User Locked Out.]

  The error message is returned in the JSON response if authenticating to the tree by using REST:

  ```json
  {  
    "code":401,  
    "reason":"Unauthorized",  
    "message":"User Locked Out.",  
    "detail":  
      {  
        "failureUrl":"
      }
  }
  ```

  - Resets the failure count in the user profile, when reached, if the User Status property is set to Active.

Failure node:

- Checks the invalid attempts property of the user profile, and returns a warning message if the number of failed attempts is equal to or greater than the configured Warn User After N Failures value in the realm:

  ![Warning: You will be locked out after 1 more failure(s).]

  The error message is returned in the JSON response if authenticating to the tree by using REST:


- Increments the failure count in the user profile, when reached.

- Returns an error message if the account is marked as **Inactive**:

```
{
  "code":401,
  "reason":"Unauthorized",
  "message":"Warning: You will be locked out after 1 more failure(s).",
  "detail":
  {
    "failureUrl":"
  }
}
```

The error message is returned in the JSON response if authenticating to the tree by using REST:

```
{
  "code":401,
  "reason":"Unauthorized",
  "message":"User Locked Out.
  {
    "failureUrl":"
  }
}
```

For information on configuring account lockout in a realm, see "Configuring Account Lockout" in the **Security Guide**.

### Specifying IDM Identity Resources in Trees

When running AM as part of an integrated platform with IDM, trees configured to use the platform need to identify the type of identity resource or object the tree is working with. To do this, use the `identityResource` configuration property. If the property is not included in the tree configuration, it will default to `managed/user`.

To update `identityResource` on a tree, use the REST API to update the tree:
curl \
  --request PUT \
  --header 'Accept-API-Version: protocol=2.1,resource=1.0' \
  --header 'Accept: application/json' \
  --header 'If-None-Match: *' \
  --header 'Content-Type: application/json' \
  --header 'Cookie: <omitted for length>' \
  --data '{
    "entryNodeId":"e301438c-0bd0-429c-ab0c-66126501069a",
    "nodes":{},
    "staticNodes":{},
    "description":"Example tree description",
    "identityResource":"managed/newObjectType"
  }' \
  "https://default.iam.example.com/am/json/realms/root/realms/root/realm-config/authentication/authenticationtrees/trees/ExampleTree"

In the above example, the tree ExampleTree has no nodes added to it yet. It includes the identityResource property, set to use a managed object in IDM called newObjectType.

Since this is a PUT request, you need to include the entire tree as part of the request. For more information about using REST with AM, see "Introducing REST in AM" in the Getting Started with REST.

Configuring Authentication Trees

The following table summarizes the high-level tasks required to configure authentication trees:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design the Authentication Journey of your Users</td>
<td>• &quot;Authentication Nodes Configuration Reference&quot;, for a list of nodes delivered with AM.</td>
</tr>
<tr>
<td></td>
<td>• ForgeRock Marketplace website, for additional nodes certified by ForgeRock or our partners.</td>
</tr>
<tr>
<td></td>
<td>• &quot;About Multi-Factor Authentication&quot;, to understand how multi-factor authentication works with trees.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Social Authentication&quot;, to understand how social authentication works with trees.</td>
</tr>
</tbody>
</table>

Authentication trees are very flexible. For example, the same tree can branch for different use cases, or users can be forced to loop though branches until they are able to present the required credentials.

It is easy to create a massive tree that is difficult to understand, read, and maintain in the UI. For this reason, AM allows you to nest trees within trees.

The best way to tackle the design decision is to write down a list of required steps users would need to take to log in to your environment, and then check the list of nodes available in AM.

Tip

Evaluation installs of AM that use the embedded data store provide ready-made sample authentication trees to demonstrate how they can be put together.

These sample trees are not installed by default in instances of AM that use an external configuration store, or if you are
Configuring AM for Authentication

Configuring Authentication Trees

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>upgrading an existing instance of AM. To obtain a copy of the sample</td>
<td>• Authentication Node Development Guide</td>
</tr>
<tr>
<td>trees that you can import into your instance, see How do I access and</td>
<td>• &quot;Creating Post-Authentication Hooks for Trees&quot;</td>
</tr>
<tr>
<td>build the sample code provided for AM/OpenAM (All versions)? in the</td>
<td></td>
</tr>
<tr>
<td>ForgeRock Knowledge Base.</td>
<td></td>
</tr>
<tr>
<td>For information on importing the sample tree JSON files by</td>
<td></td>
</tr>
<tr>
<td>using Amster, see Importing Configuration Data in the Amster 7 User</td>
<td></td>
</tr>
<tr>
<td>Guide.</td>
<td></td>
</tr>
</tbody>
</table>

Decide if you Need Custom Authentication Nodes and Webhooks

If the nodes available in AM or in the ForgeRock Marketplace do not suit your needs, you can build your own nodes.

In the same way, you can create custom webhooks for nodes that need them.

Configure your Authentication Trees

Use the authentication tree designer to put together your trees quickly.

Configure Webhooks, if Required

If you have configured the Register Logout Webhook node, configure its webhook.

---

To Create an Authentication Tree

1. On the Realms page of the AM console, select the realm in which to create the authentication tree.

2. On the Realm Overview page, select Authentication in the left-hand menu, and then select Trees.

3. On the Trees page, select Create Tree. Enter a tree name, for example myAuthTree, and then select Create.

   The authentication tree designer is displayed, with the Start entry point connected to the Failure exit point.

   The authentication tree designer provides the following features on the toolbar:

   **Authentication Tree Designer Toolbar**

<table>
<thead>
<tr>
<th>Button</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>![/layout]</td>
<td>Lay out and align nodes according to the order they are connected.</td>
</tr>
<tr>
<td>![/fullscreen]</td>
<td>Toggle the designer window between normal and full screen layout.</td>
</tr>
<tr>
<td>![/delete]</td>
<td>Remove the selected node. Note that the Start entry point cannot be deleted.</td>
</tr>
</tbody>
</table>
4. Add a node to the tree by dragging the node from the Components panel on the left-hand side and dropping it into the designer area.

The list of authentication nodes is split into a number of categories, which you can expand and collapse by clicking the category title.

You can use the filter text field to restrict the list of authentication nodes, which will match on the nodes' name, and any tags applied to the node:

![Components panel]

5. (Optional) Configure the node properties by using the right-hand panel. For more information on the available properties for each node, see "Authentication Nodes Configuration Reference".

6. Connect the node to the tree as follows:

- Select and drag the output connector from an existing node and drop it onto the new node.
- Select and drag the output connector from the new node and drop it onto an existing node.

Nodes have one or more connectors, displayed as dots on the node. Unconnected connectors are colored red and must be connected to other nodes in the tree.

Tip

*Input* connectors appear on the left of the node, *output* connectors appear on the right.

A line is drawn between the connectors of connected nodes, and the connectors will no longer be red.
7. (Optional) Alter a connection by selecting and dragging the green connector in the connection and dropping it onto the new location.

8. Continue adding, connecting and removing nodes until the tree is complete, and then select Save.

9. Test your authentication tree by navigating to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=myAuthTree#login

Configuring Authentication Webhooks

This section covers creating webhooks, which are used to send HTTP POST calls to a server with contextual information about an authentication session when a predefined event occurs, for example, logging out.

Webhooks are used from within authentication trees, by the following nodes:

- Register Logout Webhook Node

To Create an Authentication Webhook

Perform the following steps to create an authentication webhook for use within an authentication tree:

1. Log in to the AM console as an administrator, for example, amAdmin.

2. Navigate to Realms > Realm Name > Authentication > Webhooks.
   - To create a new webhook, select Create Webhook, specify a Webhook Name, and then select Create.
   - To edit an existing webhook, select the name of the webhook.

A screen similar to the following appears:
Configure AM for Authentication

Configuring Authentication Webhooks

3. Complete the fields as required:

   **Url**
   
   Specifies the URL to which the HTTP POST is sent when the event occurs.

   **Body**
   
   Specifies the body of the HTTP POST. You can send different formats by also setting the correct Content-Type header in the **Header** property, for example:

   - **Form Data.** Enter the body value in the format `parameter=value&parameter2=value2`, and set a **Content-Type** header of `application/x-www-form-urlencoded`.
   
   - **JSON Data.** Enter the body value in the format `{"parameter":"value","parameter2":"value2"}`, and set a **Content-Type** header of `application/json`.

   **Headers**
   
   Specifies any HTTP headers to add to the POST.

   To add a header, enter the name of the header in the **Key** field, and the value, and then click the Add button (➕).

   To remove a header, select the Delete button (✖).

   Each of the fields in a webhook supports variables for retrieving values from the user's session after successfully authenticating. Specify a variable in the following format:
Any custom properties added to the session using the Set Session Properties Node can be accessed by using a variable, as well as the following session properties:

- AMCtxId
- amlbcokie
- authInstant
- AuthLevel
- CharSet
- clientType
- FullLoginURL
- Host
- HostName
- IndexType
- Locale
- Organization
- Principal
- Principals
- Service
- successURL
- sun.am.UniversalIdentifier
- UserID
- UserProfile
- UserToken
- webhooks

The following figure shows an example webhook, using variable substitutions:
Warning

Specifying a variable that is not present in the user's session places the literal variable text in to the HTTP POST, for example `user=${UserId}`, rather than `user=demo`.

Customizing Authentication Trees

Your deployment might require customizing standard authentication tree features.

For information on customizing authentication nodes, see Authentication Node Development Guide.

Creating Post-Authentication Hooks for Trees

This section explains how to create a hook used by a node within an authentication tree. These tree hooks can perform custom processing after an authentication tree has successfully completed and a session created.

AM includes the following authentication tree hooks:

CreatePersistentCookieJwt

Used by the SetPersistentCookieNode authentication node.
UpdatePersistentCookieJwt

Used by the PersistentCookieDecisionNode authentication node.

The Core Class of an Authentication Tree Hook

The following example shows the UpdatePersistentCookieTreehook class, as used by the Persistent Cookie Decision node:

```java
package org.forgerock.openam.auth.nodes.treehook;

import java.util.List;
import java.util.concurrent.TimeUnit;
import javax.inject.Inject;
import org.forgerock.guice.core.InjectorHolder;
import org.forgerock.http.protocol.Cookie;
import org.forgerock.http.protocol.Request;
import org.forgerock.http.protocol.Response;
import org.forgerock.openam.auth.node.api.TreeHook;
import org.forgerock.openam.auth.node.api.TreeHookException;
import org.forgerock.openam.auth.nodes.PersistentCookieDecisionNode;
import org.forgerock.openam.auth.nodes.jwt.InvalidPersistentJwtException;
import org.forgerock.openam.auth.nodes.jwt.PersistentJwtStringSupplier;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import com.google.inject.assistedinject.Assisted;

/**
 * A TreeHook for updating a persistent cookie.
 */
```
@TreeHook.Metadata(configClass = PersistentCookieDecisionNode.Config.class)
public class UpdatePersistentCookieTreeHook implements TreeHook {

    private final Request request;
    private final Response response;
    private final PersistentCookieDecisionNode.Config config;
    private final PersistentJwtStringSupplier persistentJwtStringSupplier;
    private final PersistentCookieResponseHandler persistentCookieResponseHandler;
    private final Logger logger = LoggerFactory.getLogger("amAuth");

    /**
     * The UpdatePersistentCookieTreeHook Constructor.
     *
     * @param request The request.
     * @param response The response.
     * @param config the config for updating the cookie.
     */
    @Inject
    public UpdatePersistentCookieTreeHook(@Assisted Request request, @Assisted Response response,
            @Assisted PersistentCookieDecisionNode.Config config) {
        this.request = request;
        this.response = response;
        this.config = config;
        this.persistentJwtStringSupplier = InjectorHolder.getInstance(PersistentJwtStringSupplier.class);
        this.persistentCookieResponseHandler = InjectorHolder.getInstance(PersistentCookieResponseHandler.class);
    }

    @Override
    public void accept() throws TreeHookException {
        logger.debug("UpdatePersistentCookieTreeHook.accept");
        String orgName = PersistentCookieResponseHandler.getOrgName(response);
        Cookie originalJwt = getJwtCookie(request, config.persistentCookieName());
        if (originalJwt != null) {
            String jwtString;
            try {
                jwtString = persistentJwtStringSupplier.getUpdatedJwt(originalJwt.getValue(), orgName,
                        String.valueOf(config.hmacSigningKey()), config.idleTimeout().to(TimeUnit.HOURS));
            } catch (InvalidPersistentJwtException e) {
                logger.error("Invalid jwt", e);
                throw new TreeHookException(e);
            }
            if (jwtString != null && !jwtString.isEmpty()) {
                persistentCookieResponseHandler.setCookieOnResponse(response, request,
                        config.persistentCookieName(), jwtString, originalJwt.getExpires(), config.useSecureCookie(),
                        config.useHttpOnlyCookie());
            }
        }
    }

    private Cookie getJwtCookie(Request request, String cookieName) {
        if (request.getCookies().containsKey(cookieName)) {
            List<Cookie> cookies = request.getCookies().get(cookieName);
            for (Cookie cookie : cookies) {
                if (cookie.getName().equals(cookieName)) {
                    return cookie;
                }
            }
        }
    }
}
Key:

1. The `@TreeHook.Metadata` annotation.

Before defining the core class, use a Java `@TreeHook.Metadata` annotation to specify the class the tree hook uses for its configuration. Use the `configClass` property to specify the configuration class of the node that will be using the tree hook.

2. The core class must implement the `TreeHook` interface. For more information, see the `TreeHook` interface in the AM 7.0.2 Public API Javadoc.

3. AM uses Google's Guice dependency injection framework for authentication nodes and tree hooks. Use the `@Inject` annotation to construct a new instance of the tree hook, specifying the configuration interface set up earlier and any other required parameters.

For more information, see the `Inject` annotation type and the `Assisted` annotation type in the Google Guice Javadoc.

4. Creating an `Accept` instance. The main logic of a tree hook is handled by the `Accept` function.

Authentication Modules and Chains

AM uses authentication modules to handle different ways of authenticating. Basically, each authentication module handles one way of obtaining and verifying credentials. You can chain different authentication modules together. In AM, this is called authentication chaining. Each authentication module can be configured to specify the continuation and failure semantics with one of the following four criteria: requisite, sufficient, required, or optional.

Authentication modules in a chain can assign a `pass` or `fail` flag to the authorization request. To successfully complete an authentication chain at least one pass flag must have been achieved, and there must be no fail flags.

Flags are assigned when completing a module as shown in the table below:

<p>| Authentication Criteria, Flags, and Continuation Semantics |
|---|---|---|---|
| <strong>Criteria</strong> | <strong>Fail</strong> | <strong>Pass</strong> | <strong>Example</strong> |
| Requisite | Assigns fail flag. | Assigns pass flag. | Active Directory, Data Store, and LDAP authentication modules are often set as requisite because of a subsequent requirement in the chain to identify the user. |
| | Expires chain. | Continues chain. | |</p>
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Fail</th>
<th>Pass</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient</td>
<td>Assigns no flag. Continues chain.</td>
<td>Assigns pass flag.</td>
<td>For example, the Device ID (Match) authentication module needs a user's ID before it can retrieve information about the user's devices.</td>
</tr>
<tr>
<td>Required</td>
<td>Assigns fail flag.</td>
<td>Assigns pass flag. Continues chain.</td>
<td>You could set Windows Desktop SSO as sufficient, so authenticated Windows users are let through, whereas web users must traverse another authentication module, such as one requiring a username and password. One exception is that if you pass a sufficient module after having failed a required module, you will continue through the chain and will not exit at that point. Consider using a requisite module instead of a required module in this situation.</td>
</tr>
<tr>
<td>Optional</td>
<td>Assigns no flag. Continues chain.</td>
<td>Assigns pass flag. Continues chain.</td>
<td>You could use an optional module to assign a higher authentication level if it passes. Consider a chain with a requisite Data Store module and an optional Certificate module. Users who only passed the Data Store module could be assigned a lower authentication level than users who passed both the Data Store and Certificate modules. The users with the higher authentication level could be granted access to more highly-secured resources.</td>
</tr>
</tbody>
</table>

**Tip**

In authentication chains with a single module, requisite and required are equivalent. For authentication chains with multiple modules, use required only when you want the authentication chain to continue evaluating modules even after the required criterion fails.

The AM authentication chain editor displays the flags that could be assigned by each module in the chain, and whether execution of the chain continues downwards through the chain or exits out, as shown below:
With AM, you can further set authentication levels per module, with higher levels being used typically to allow access to more restricted resources. The AM SPIs also let you develop your own authentication modules, and post authentication plugins. Client applications can specify the authentication level, module, user, and authentication service to use among those you have configured. As described later in this guide, you can use realms to organize which authentication process applies for different applications or different domains, perhaps managed by different people.
About Authentication Levels for Chains

When a user successfully authenticates, AM creates a session, which allows AM to manage the user's access to resources. The session is assigned an authentication level, which is calculated to be the highest authentication level of any authentication module that passed. If the user's session does not have the appropriate authentication level, then the user may need to reauthenticate again at a higher authentication level to access the requested resource.

The authentication level sets the level of security associated with a module. Typically, the strongest form of authentication is assigned the highest authentication level.

If an authentication chain contains requisite or required modules that were not executed due to the presence of a passing sufficient module in front of them, the session's authentication level is calculated to be whichever is greater: the highest authentication level of any authentication module that passed, or the highest authentication level of requisite or required modules that were not executed.

You can modify AM's default behavior, so that a session's authentication level is always the highest authentication level of any authentication module that passed, even if there are requisite or required modules in the authentication chain that were not executed.

To modify the default behavior, set the org.forgerock.openam.authLevel.excludeRequiredOrRequisite property to true under Deployment > Servers > Server Name > Advanced and restart the AM server.

Authorization policies may also require a particular authentication level to access protected resources. When an authenticated user tries to access a protected resource without satisfying the authentication level requirement, AM denies access to the resource and returns an advice indicating that the user needs to reauthenticate at the required authentication level to access the resource.

The web or Java agent or policy enforcement point can then send the user back to AM for session upgrade. For more information, see "Session Upgrade" in the Sessions Guide.

Configuring Authentication Chains

The following table summarizes the high-level tasks required to configure authentication chains:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design the Authentication Journey of your Users</td>
<td>• &quot;Authentication Modules Configuration Reference&quot;, for a list of modules delivered with AM.</td>
</tr>
<tr>
<td></td>
<td>• &quot;About Multi-Factor Authentication&quot;, to understand how multi-factor authentication works with chains.</td>
</tr>
<tr>
<td></td>
<td>• &quot;Social Authentication&quot;, to understand how social authentication works with chains.</td>
</tr>
</tbody>
</table>
### Configuring AM for Authentication

#### Configuring Authentication Chains

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decide if you Need Custom Authentication Modules, Server-Side Scripts, or Post-Authentication Plugins</td>
<td>&quot;Customizing Authentication Chains&quot;</td>
</tr>
<tr>
<td>Configure your Authentication Modules</td>
<td>&quot;To Configure Authentication Modules&quot;</td>
</tr>
<tr>
<td>Configure your Authentication Chains</td>
<td>&quot;To Create an Authentication Chain&quot;</td>
</tr>
<tr>
<td>Configure Post-Authentication Plugins</td>
<td>&quot;Implementing Post-Authentication Plugins&quot;</td>
</tr>
</tbody>
</table>

### To Configure Authentication Modules

The AM console provides two places where you can configure authentication modules:

- Under Configure > Authentication, you configure default properties for global authentication modules.
- Under Realms > Realm Name > Authentication v Modules, you configure modules for your realm.
- Configure the authentication modules required by your environment. The configuration of individual modules depend on its function. See the following links:
  - "MFA: Open AuTHentication (OATH)"
  - "MFA: Push Authentication"
  - "MFA: Web Authentication (WebAuthn)"
  - "Social Authentication"

For module reference information, see "Authentication Modules Configuration Reference".

### To Create an Authentication Chain

Once you have configured authentication modules and added the modules to the list of module instances, you can configure authentication chains. Authentication chains let you handle cases where alternate modules or credentials are needed. If you need modules in the chain to share user credentials, then set options for the module.

1. Go to Realms > Realm Name > Authentication > Chains.
2. On the Authentication Chains page, click Add Chain. Enter new chain name, and then click Create.

   The Edit Chain dialog appears. Click on Add a Module.

3. Select the authentication module in the drop-down list, and then assign appropriate criteria (Optional, Required, Requisite, Sufficient), as described in "Authentication Modules and Chains".

   Add as many modules as required.

4. (Optional) If you need modules in the chain to share user credentials, consider the following available options:

   + **Options to Share Credentials Among Modules**

     **iplanet-am-auth-store-shared-state-enabled**

     Set `iplanet-am-auth-store-shared-state-enabled=true` to store the credentials captured by this module in shared state. This enables subsequent modules in the chain to access the credentials captured by this module. The shared state is cleared when the user successfully authenticates, quits the chain, or logs out.

     Default: `true`

     **Note**

     OATH and OTP codes are never added to the shared state, and cannot be shared between other modules in the chain.

     **iplanet-am-auth-shared-state-enabled**

     Set `iplanet-am-auth-shared-state-enabled=true` to allow this module to access the credentials, such as user name and password, that have been stored in shared state by previous modules in the authentication chain.

     Default: `false`

     **iplanet-am-auth-shared-state-behavior-pattern**

     Set `iplanet-am-auth-shared-state-behavior-pattern=tryFirstPass` to try authenticating with the username and password stored in shared state. If authentication fails, AM displays the login screen of this module for the user to re-enter their credentials.

     Set `iplanet-am-auth-shared-state-behavior-pattern=useFirstPass` to prevent the user from entering the username and password twice during authentication. Typically, you set the property to `useFirstPass` for all modules in the chain except the first module. If authentication fails, then the module fails.
Default: tryFirstPass

Enter the key and its value, and then click Plus (+). When you finish entering the options, click OK.

+ Examples

For example, consider a chain with two modules sharing credentials according to the following settings: the first module in the chain has the option `iplanet-am-auth-store-shared-state-enabled=true`, and criteria REQUIRED.

**Authentication Chain First Module**

![Authentication Chain First Module](image)

The second module in the chain has options `iplanet-am-auth-shared-state-enabled=true`, `iplanet-am-auth-shared-state-behavior-pattern=useFirstPass` with criteria REQUIRED.
5. On the Settings tab, configure where AM redirects the user upon successful and failed authentication, and plug in your post-authentication processing classes as necessary.

   If you configure absolute URLs that are not in the same scheme, FQDN, and port as AM, you must also configure the Validation Service.

6. Click Save Changes.

   The following authentication sequence would occur: the user enters their credentials for the first module and successfully authenticates. The first module shares the credentials with the second module, successfully authenticating the user without prompting again for their credentials, unless the credentials for the first module do not successfully authenticate the user to the second module.

Implementing Post-Authentication Plugins

Post-authentication plugins (PAP) let you include custom processing at the end of the authentication process and when users log out of AM.
In the AM console, you add post-authentication plugins to an authentication chain. Navigate to Realms > Realm Name > Authentication > Chains > Auth Chain Name > Settings > Post Authentication Processing Class > Class Name.

See "Creating Post-Authentication Plugins for Chains" for more information about post authentication plugins.

**Standard Post-Authentication Plugins**

AM provides some post-authentication plugins as part of the standard product delivery.

**Class name: org.forgerock.openam.authentication.modules.adaptive.AdaptivePostAuthenticationPlugin**

The adaptive authentication plugin serves to save cookies and profile attributes after successful authentication.

Add it to your authentication chains that use the adaptive authentication module configured to save cookies and profile attributes.

**Class name: org.forgerock.openam.authentication.modules.common.JaspiAuthLoginModulePostAuthenticationPlugin**

The Java Authentication Service Provider Interface (JASPI) post authentication plugin initializes the underlying JASPI ServerAuth module.

JASPI defines a standard service provider interface (SPI) where developers can write message level authentication agents for Java containers on either the client side or the server side.

**Class name: org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin**

The OAuth 2.0 post-authentication plugin builds a global logout URL used by /oauth2c/OAuthLogout.jsp after successful OAuth 2.0 client authentication. This logs the resource owner out with the OAuth 2.0 provider when logging out of AM.

Before using this plugin, configure the OAuth 2.0 authentication module with the correct OAuth 2.0 Provider logout service URL, and set the Logout options to Log out or Prompt. This plugin cannot succeed unless those parameters are correctly set.

Sometimes OAuth 2.0 providers change their endpoints, including their logout URLs. When using a provider like Facebook, Google, or MSN, make sure you are aware when they change their endpoint locations so that you can change your client configuration accordingly.

**Class name: org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin**

The SAML v2.0 post-authentication plugin that gets activated for single logout. Supports HTTP-Redirect for logout-sending messages only.

Set the post-authentication processing class for the authentication chain that contains the SAML v2.0 authentication module.
Class name: org.forgerock.openam.authentication.modules.persistentcookie.PersistentCookieAuthModule

The Persistent Cookie Authentication Module provides logic for persistent cookie authentication in AM. It makes use of the JASPI JwtSession module to create and verify the persistent cookie.

Class name: com.sun.identity.authentication.spi.ReplayPasswd

Password replay post-authentication plugin class that uses a DES/ECB/NoPadding encryption algorithm. This class is deprecated in favor of the com.sun.identity.authentication.spi.JwtReplayPassword class.

The plugin encrypts the password captured by AM during the authentication process and stores it in a session property. IG or a web agent looks up the property, decrypts it, and replays the password into legacy applications.

To configure password replay for AM and IG, see the ForgeRock Identity Gateway Gateway Guide.

Class name: com.sun.identity.authentication.spi.JwtReplayPassword

Password replay post-authentication plugin class that uses a JWT-based AES A128CBC-HS256 encryption algorithm.

The plugin encrypts the password captured by AM during the authentication process and stores it in a session property. IG looks up the property, decrypts it, and replays the password into legacy applications.

Only IG 6 or later is supported.

To configure password replay for AM and IG, see the ForgeRock Identity Gateway Gateway Guide.

If necessary, you can also write your own custom post-authentication plugin as described in "Creating Post-Authentication Plugins for Chains".

Customizing Authentication Chains

Your deployment might require customizing standard authentication chain features. See the following sections for customization examples:

• Creating a Custom Authentication Module

• Using Server-side Authentication Scripts in Authentication Modules

• Creating Post-Authentication Plugins for Chains

1Only one password replay post-authentication plugin class can be active for a given AM deployment.
Creating a Custom Authentication Module

This section shows how to customize authentication with a sample custom authentication module. For deployments with particular requirements not met by existing AM authentication modules, determine whether you can adapt one of the built-in or extension modules for your needs. If not, build the functionality into a custom authentication module.

About the Sample Custom Authentication Module

The sample custom authentication module prompts for a user name and password to authenticate the user, and handles error conditions. The sample shows how you integrate an authentication module into AM such that you can configure the module through the AM console, and also localize the user interface.

For information on downloading and building AM sample source code, see How do I access and build the sample code provided for OpenAM 12.x, 13.x and AM (All versions)? in the Knowledge Base.

Get a local clone so that you can try the sample on your system. In the sources, you find the following files under the /path/to/openam-samples-external/custom-authentication-module directory:

- **pom.xml**
  Apache Maven project file for the module
  This file specifies how to build the sample authentication module, and also specifies its dependencies on AM components and on the Java Servlet API.

- **src/main/java/org/forgerock/openam/examples/SampleAuth.java**
  Core class for the sample authentication module
  This class is called by AM to initialize the module and to process authentication. See "The Sample Authentication Logic" for details.

- **src/main/java/org/forgerock/openam/examples/SampleAuthPrincipal.java**
  Class implementing java.security.Principal interface that defines how to map credentials to identities
  This class is used to process authentication. See "The Sample Auth Principal" for details.

- **src/main/resources/amAuthSampleAuth.properties**
  Properties file mapping UI strings to property values
  This file makes it easier to localize the UI. See "Sample Auth Properties" for details.

- **src/main/resources/amAuthSampleAuth.xml**
  Configuration file for the sample authentication service
This file is used when registering the authentication module with AM. See "The Sample Auth Service Configuration" for details.

src/main/resources/config/auth/default/SampleAuth.xml

Callback file for deprecated AM classic UI authentication pages

The sample authentication module does not include localized versions of this file. See "Sample Auth Callbacks" for details.

src/main/java/org/forgerock/openam/examples/SampleAuthPlugin.java
src/main/resources/META-INF/services/org.forgerock.openam.plugins.AmPlugin

These files serve to register the plugin with AM.

The Java class, SampleAuthPlugin, implements the org.forgerock.openam.plugins.AmPlugin interface. In the sample, this class registers the SampleAuth implementation, and the amAuthSampleAuth service schema for configuration.

The services file, org.forgerock.openam.plugins.AmPlugin, holds the fully qualified class name of the AmPlugin that registers the custom implementations. In this case, org.forgerock.openam.examples.SampleAuthPlugin.

For an explanation of service loading, see the ServiceLoader API specification.

Sample Auth Properties

AM uses a Java properties file per locale to retrieve the appropriate, localized strings for the authentication module.

The following is the Sample Authentication Module properties file, amAuthSampleAuth.properties.
Sample Auth Callbacks

AM callbacks XML files are used to build the deprecated classic UI to prompt the user for identity information needed to process the authentication. The document type for a callback XML file is described in WEB-INF/Auth_Module_Properties.dtd where AM is deployed.

The value of the moduleName property in the callbacks file must match your custom authentication module's class name. Observe that the module name SampleAuth, shown in the example below, matches the class name in "The Sample Authentication Logic" [31].

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!--
* The contents of this file are subject to the terms of the Common Development and
* Distribution License (the License). You may not use this file except in compliance with the
* License.
* *
* You can obtain a copy of the License at legal/CDDLv1.0.txt. See the License for the
* specific language governing permission and limitations under the License.
* *
* When distributing Covered Software, include this CDDL Header Notice in each file and include
* the License file at legal/CDDLv1.0.txt. If applicable, add the following below the CDDL
* Header, with the fields enclosed by brackets [] replaced by your own identifying
* information: "Portions copyright [year] [name of copyright owner]".
* *
* Copyright 2011-2017 ForgeRock AS. All Rights Reserved
* -->
<!DOCTYPE ModuleProperties PUBLIC "//iPlanet//Authentication Module Properties XML Interface 1.0 DTD//EN"
```
This file specifies three states.

1. The initial state (order="1") is used dynamically to replace the dummy strings shown between hashes (for example, #USERNAME#) by the substituteUIStrings() method in SampleAuth.java.

2. The next state (order="2") handles prompting the user for authentication information.

3. The last state (order="3") has the attribute error="true". If the authentication module state machine reaches this order then the authentication has failed. The NameCallback is not used and not displayed to user. AM requires that the callbacks array have at least one element. Otherwise AM does not permit header substitution.

The Sample Authentication Logic

An AM authentication module must extend the com.sun.identity.authentication.spi.AMLoginModule abstract class, and must implement the methods shown below.

Tip

The account lockout functionality in AM is triggered by counting invalid password exceptions, rather than invalid login exceptions.

To trigger account lockouts after repeated failed attempts, ensure your modules throw InvalidPasswordException exceptions instead of AuthLoginException exceptions when appropriate, as per the code below.

See the ForgeRock Access Management Java SDK API Specification for reference.
public void init(Subject subject, Map sharedState, Map options)

    // OpenAM calls the process() method when the user submits authentication
    // information. The process() method determines what happens next:
    // success, failure, or the next state specified by the order
    // attribute in the callbacks XML file.
    public int process(Callback[] callbacks, int state) throws LoginException

    // OpenAM expects the getPrincipal() method to return an implementation of
    // the java.security.Principal interface.
    public Principal getPrincipal()

AM does not reuse authentication module instances. This means that you can store information
specific to the authentication process in the instance.

The implementation, SampleAuth.java, is shown below:

package org.forgerock.openam.examples;
import java.security.Principal;
import java.util.Map;
import java.util.ResourceBundle;
import java.util.Set;
import javax.security.auth.Subject;
import javax.security.auth.callback.Callback;
import javax.security.auth.callback.NameCallback;
import javax.security.auth.callback.PasswordCallback;
import javax.security.auth.login.LoginException;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import com.sun.identity.authentication.spi.AMLoginModule;
import com.sun.identity.authentication.spi.AuthLoginException;
import com.sun.identity.authentication.util.ISAuthConstants;
import com.sun.identity.shared.datastruct.CollectionHelper;

/**
 * SampleAuth authentication module example.
 */

package org.forgerock.openam.examples;
* If you create your own module based on this example, you must modify all occurrences of "SampleAuth" in addition to changing the name of the class.
* Please refer to OpenAM documentation for further information.
* Feel free to look at the code for authentication modules delivered with OpenAM, as they implement this same API.
*/
public class SampleAuth extends AMLoginModule {
    // Name for the debug-log
    private final static String DEBUG_NAME = "SampleAuth";
    private final static Logger debug = LoggerFactory.getLogger(SampleAuth.class);

    // Name of the resource bundle
    private final static String amAuthSampleAuth = "amAuthSampleAuth";

    // User names for authentication logic
    private final static String USERNAME = "demo";
    private final static String PASSWORD = "Ch4ng31t";

    private final static String ERROR_1_USERNAME = "test1";
    private final static String ERROR_2_USERNAME = "test2";

    // Orders defined in the callbacks file
    private final static int STATE_BEGIN = 1;
    private final static int STATE_AUTH = 2;
    private final static int STATE_ERROR = 3;

    // Errors properties
    private final static String SAMPLE_AUTH_ERROR_1 = "sampleauth-error-1";
    private final static String SAMPLE_AUTH_ERROR_2 = "sampleauth-error-2";

    private Map<String, Set<String>> options;
    private ResourceBundle bundle;
    private Map<String, String> sharedState;

    public SampleAuth() {
        super();
    }

    /**
     * This method stores service attributes and localized properties for later use.
     * @param subject
     * @param sharedState
     * @param options
     */
    @Override
    public void init(Subject subject, Map sharedState, Map options) {
        debug.debug("SampleAuth::init");
        this.options = options;
        this.sharedState = sharedState;
        this.bundle = amCache.getResBundle(amAuthSampleAuth, getLoginLocale());
    }
@Override
public int process(Callback[] callbacks, int state) throws LoginException {
    debug.debug("SampleAuth::process state: {}", state);
    switch (state) {
    case STATE_BEGIN:
        // Initialize Callback list if used in chain with
        // iplanet-am-auth-shared-state-enabled=true
        setForceCallbacksRead(true);
        forceCallbacksInit();
        // No time wasted here - simply modify the UI and
        // proceed to next state
        substituteUIStrings();
        return STATE_AUTH;
    case STATE_AUTH:
        // Get data from callbacks. Refer to callbacks XML file.
        NameCallback nc = (NameCallback) callbacks[0];
        PasswordCallback pc = (PasswordCallback) callbacks[1];
        String username = nc.getName();
        String password = String.valueOf(pc.getPassword());
        // First errorstring is stored in "sampleauth-error-1" property.
        if (ERROR_1_USERNAME.equals(username)) {
            setErrorText(SAMPLE_AUTH_ERROR_1);
            return STATE_ERROR;
        }
        // Second errorstring is stored in "sampleauth-error-2" property.
        if (ERROR_2_USERNAME.equals(username)) {
            setErrorText(SAMPLE_AUTH_ERROR_2);
            return STATE_ERROR;
        }
        if (USERNAME.equals(username) && PASSWORD.equals(password)) {
            debug.debug("SampleAuth::process User '{}' authenticated with success.", username);
            return ISAuthConstants.LOGIN_SUCCEED;
        }
        throw new InvalidPasswordException("password is wrong", username);
    case STATE_ERROR:
        return STATE_ERROR;
    default:
        throw new AuthLoginException("invalid state");
    }
}

@Override
public Principal getPrincipal() {
    return new SampleAuthPrincipal(USERNAME);
}
private void setErrorText(String err) throws AuthLoginException {
    // Receive correct string from properties and substitute the
    // header in callbacks order 3.
    substituteHeader(STATE_ERROR, bundle.getString(err));
}

private void substituteUIStrings() throws AuthLoginException {
    // Get service specific attribute configured in OpenAM
    String ssa = CollectionHelper.getMapAttr(options, "specificAttribute");

    // Get property from bundle
    String new_hdr = ssa + " " +
    bundle.getString("sampleauth-ui-login-header");
    substituteHeader(STATE_AUTH, new_hdr);

    replaceCallback(STATE_AUTH, 0, new NameCallback(  
        bundle.getString("sampleauth-ui-username-prompt")));
    replaceCallback(STATE_AUTH, 1, new PasswordCallback(  
        bundle.getString("sampleauth-ui-password-prompt"), false));
}

The Sample Auth Principal

The implementation, SampleAuthPrincipal.java, is shown below:

/*
 * The contents of this file are subject to the terms of the Common Development and
 * Distribution License (the License). You may not use this file except in compliance with the
 * License.
 *
 * You can obtain a copy of the License at legal/CDDLv1.0.txt. See the License for the
 * specific language governing permission and limitations under the License.
 *
 * When distributing Covered Software, include this CDDL Header Notice in each file and include
 * the License file at legal/CDDLv1.0.txt. If applicable, add the following below the CDDL
 * Header, with the fields enclosed by brackets [] replaced by your own identifying
 * information: " Portions copyright [year] [name of copyright owner]."
 *
 * Copyright 2011-2017 ForgeRock AS. All Rights Reserved
 */

package org.forgerock.openam.examples;

import java.io.Serializable;
import java.security.Principal;

/**
 * SampleAuthPrincipal represents the user entity.
 */
public class SampleAuthPrincipal implements Principal, Serializable {
    private final static String COLON = " : ";

    private final String name;

    public SampleAuthPrincipal(String name) {
        if (name == null) {
            }
throw new NullPointerException("illegal null input");
}

this.name = name;

/**
 * Return the LDAP username for this <code>SampleAuthPrincipal</code>.
 * @return the LDAP username for this <code>SampleAuthPrincipal</code>
 */
@Override
public String getName() {
    return name;
}

/**
 * Return a string representation of this <code>SampleAuthPrincipal</code>.
 * @return a string representation of this <code>TestAuthModulePrincipal</code>.
 */
@Override
public String toString() {
    return new StringBuilder().append(this.getClass().getName()).append(COLON).append(name).toString();
}

/**
 * Compares the specified Object with this <code>SampleAuthPrincipal</code> for equality. Returns true if the
given object is also a <code>SampleAuthPrincipal</code> and the two <code>SampleAuthPrincipal</code> have
* the same username.
* @param o Object to be compared for equality with this <code>SampleAuthPrincipal</code>.
* @return true if the specified Object is equal equal to this <code>SampleAuthPrincipal</code>.
*/
@Override
public boolean equals(Object o) {
    if (o == null) {
        return false;
    }
    if (this == o) {
        return true;
    }
    if (!(o instanceof SampleAuthPrincipal)) {
        return false;
    }
    SampleAuthPrincipal that = (SampleAuthPrincipal) o;
    if (this.getName().equals(that.getName())) {
        return true;
    }
    return false;
}
The Sample Auth Service Configuration

AM requires that all authentication modules be configured by means of an AM service. At minimum, the service must include an authentication level attribute. Your module can access these configuration attributes in the options parameter passed to the init() method.

Some observations about the service configuration file follow in the list below.

• The document type for a service configuration file is described in WEB-INF/sms.dtd where AM is deployed.

• The service name is derived from the module name. The service name must have the following format:
  
  • It must start with either iPlanetAMAuth or sunAMAuth.

  • The module name must follow. The case of the module name must match the case of the class that implements the custom authentication module.

  • It must end with Service.

In the Sample Auth service configuration, the module name is SampleAuth and the service name is iPlanetAMAuthSampleAuthService.

• The service must have a localized description, retrieved from a properties file.

• The i18nFileName attribute in the service configuration holds the default (non-localized) base name of the Java properties file. The i18nKey attributes indicate properties keys to string values in the Java properties file.

• The authentication level attribute name must have the following format:
  
  • It must start with iplanet-am-auth-, sun-am-auth-, or forgerock-am-auth-.

  • The module name must follow, and must appear in lower case if the attribute name starts with iplanet-am-auth- or forgerock-am-auth-. If the attribute name starts with sun-am-auth-, it must exactly match the case of the module name as it appears in the service name.

  • It must end with -auth-level.
In the Sample Auth service configuration, the authentication level attribute name is `iplanet-am-auth-sampleauth-auth-level`.

- The Sample Auth service configuration includes an example `sampleauth-service-specific-attribute`, which can be configured through the AM console.

The service configuration file, `amAuthSampleAuth.xml`, is shown below. Save a local copy of this file, which you use when registering the module.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- The contents of this file are subject to the terms of the Common Development and Distribution License (the License). You may not use this file except in compliance with the License. -->
<!-- You can obtain a copy of the License at legal/ CDDLv1.0.txt. See the License for the specific language governing permission and limitations under the License. -->
<!-- When distributing Covered Software, include this CDDL Header Notice in each file and include the License file at legal/CDDLv1.0.txt. If applicable, add the following below the CDDL Header, with the fields enclosed by brackets [ ] replaced by your own identifying information: Portions copyright [year] [name of copyright owner]. -->
<!-- Copyright 2011-2020 ForgeRock AS. All Rights Reserved -->
<!DOCTYPE ServicesConfiguration PUBLIC "-//iPlanet//Service Management Services (SMS) 1.0 DTD//EN" "jar://com/sun/identity/sm/sms.dtd">
<ServicesConfiguration>
  <Service name="iPlanetAMAuthSampleAuthService" version="1.0">
    <Schema
      serviceHierarchy="/DSAMEConfig/authentication/iPlanetAMAuthSampleAuthService"
      i18nFileName="amAuthSampleAuth" revisionNumber="10"
      i18nKey="sampleauth-service-description" resourceName="sample">
      <Organization>
        <!-- Specify resourceName for a JSON-friendly property in the REST SMS -->
        <AttributeSchema name="iplanet-am-auth-sampleauth-auth-level" resourceName="authLevel" type="single" syntax="number_range" rangeStart="0" rangeEnd="2147483647"
          i18nKey="a500">
          <DefaultValues>
            <Value>1</Value>
          </DefaultValues>
        </AttributeSchema>
        <!-- No need for resourceName when the name is JSON-compatible -->
        <AttributeSchema name="specificAttribute" type="single" syntax="string" validator="no" i18nKey="a501" />
      </Organization>
      <!-- For Auth Modules, the parent Schema element specifies the REST SMS resourceName, and the nested SubSchema must have resourceName="USE-PARENT" -->
      <SubSchema name="serverconfig" inheritance="multiple" resourceName="USE-PARENT">
        <AttributeSchema name="iplanet-am-auth-sampleauth-auth-level" resourceName="authLevel" type="single" syntax="number_range" rangeStart="0" rangeEnd="2147483647"/>
      </SubSchema>
    </Schema>
  </Service>
</ServicesConfiguration>
```
Building and Installing the Sample Custom Auth Module

Build the module with Apache Maven, and install the module in AM.

For information on downloading and building AM sample source code, see How do I access and build the sample code provided for OpenAM 12.x, 13.x and AM (All versions)? in the Knowledge Base.

Installing the Module

Installing the sample authentication module consists of copying the .jar file to AM's WEB-INF/lib/ directory, registering the module with AM, and then restarting AM or the web application container where it runs.

1. Copy the sample authentication module .jar file to WEB-INF/lib/ where AM is deployed.

   $ cp target/custom*.jar /path/to/tomcat/webapps/openam/WEB-INF/lib/

2. Restart AM or the container in which it runs.

   For example if you deployed AM in Apache Tomcat, then you shut down Tomcat and start it again.

   $ /path/to/tomcat/bin/shutdown.sh
   $ /path/to/tomcat/bin/startup.sh
   $ tail -l /path/to/tomcat/logs/catalina.out
   INFO: Server startup in 14736 ms

Configuring & Testing the Sample Custom Auth Module

Authentication modules are registered as services with AM globally, and then set up for use in a particular realm. In this example, you set up the sample authentication module for use in the realm / (Top Level Realm).

Log in to the AM console as an administrator, such as amAdmin, and browse to Realms > Top Level Realm > Authentication > Modules. Click Add Module to create an instance of the Sample Authentication Module. Name the module Sample.
Click Create, and then configure the authentication module as appropriate.

Now that the module is configured, log out of the AM console.

Finally, try the module by specifying the Sample module. Browse to the login URL such as https://openam.example.com:8443/openam/XUI/?realm=/&module=Sample#login, and then authenticate with user name demo and password Ch4ng31t.
After authentication you are redirected to the end user page for the demo user. You can logout of the AM console, and then try to authenticate as the non-existent user test123 to see what the error handling looks like to the user.

Using Server-side Authentication Scripts in Authentication Modules

This section demonstrates how to use the default server-side authentication script. An authentication script can be called from a Scripted authentication module.

The default server-side authentication script only authenticates a subject when the current time on the AM server is between 09:00 and 17:00. The script also uses the logger and httpClient functionality provided in the scripting API.

To examine the contents of the default server-side authentication script in the AM console browse to Realms > Top Level Realm > Scripts, and then click Scripted Module - Server Side.

For general information about scripting in AM, see Getting Started with Scripting.

For information about APIs available for use when scripting authentication, see the following sections:

- "Accessing HTTP Services" in the Getting Started with Scripting
- "Debug Logging" in the Getting Started with Scripting
- "Scripted Module API Functionality"
Preparing AM To Use Server-side Authentication Scripts

AM requires a small amount of configuration before trying the example server-side authentication script. You must create an authentication module of the Scripted type, and then include it in an authentication chain, which can then be used when logging in to AM. You must also ensure the demo user has an associated postal address.

The procedures in this section are:

- "To Create a Scripted Authentication Module that Uses the Default Server-side Authentication Script"
- "To Create an Authentication Chain that Uses a Scripted Authentication Module"
- "To Add a Postal Address to the Demo User"

To Create a Scripted Authentication Module that Uses the Default Server-side Authentication Script

In this procedure, create a Scripted Authentication module, and link it to the default server-side authentication script.

1. Log in as an AM administrator, for example amAdmin.
2. Navigate to Realms > Top Level Realm > Authentication > Modules.
4. On the New Module page, enter a module name, such as myScriptedAuthModule, from the Type dropdown list, select Scripted Module, and then click Create.
5. On the module configuration page:
   a. Uncheck the Client-side Script Enabled checkbox.
   b. From the Server-side Script drop-down list, select Scripted Module - Server Side.
   c. Click Save Changes.

To Create an Authentication Chain that Uses a Scripted Authentication Module

In this procedure, create an authentication chain that uses a Data Store authentication module and the Scripted authentication module created in the previous procedure.

1. Log in as an AM administrator, for example amAdmin.
2. Navigate to Realms > Top Level Realm > Authentication > Chains.
3. On the Authentication Chains page, click Add Chain.

4. On the Add Chain page, enter a name, such as myScriptedChain, and then click Create.

5. On the Edit Chain tab, click Add a Module.

6. In the New Module dialog box:
   a. From the Select Module drop-down list, select DataStore.
   b. From the Select Criteria drop-down list, select Required.
   c. Click OK.

   **Note**
   The Data Store authentication module checks the user credentials, whereas the Scripted authentication module does not check credentials, but instead only checks that the authentication request is processed during working hours. Without the Data Store module, the username in the Scripted authentication module cannot be determined. Therefore, do not configure the Scripted authentication module (server-side script) as the first module in an authentication chain, because it needs a username.

7. On the Edit Chain tab, click Add Module.

8. In the New Module dialog box:
   a. From the Select Module drop-down list, select the Scripted Module from the previous procedure, for example myScriptedAuthModule.
   b. From the Select Criteria drop-down list, select Required.
   c. Click OK.

The resulting chain resembles the following:
9. On the Edit Chain tab, click Save Changes.

To Add a Postal Address to the Demo User

1. Log in as an AM administrator, for example amAdmin.
2. Navigate to Realms > Top Level Realm > Identities.
3. On the Identities tab, click the demo user.
4. In the Home Address field, enter a valid postal address, with lines separated by commas.
   For example:
5. Save your changes.

Trying the Default Server-side Authentication Script

This section shows how to log in using an authentication chain that contains a Scripted authentication module, which in turn uses the default server-side authentication script.

The default server-side authentication script gets the postal address of a user after they authenticate using a Data Store authentication module, and then makes an HTTP call to an external web service to determine the longitude and latitude of the address. Using these details, a second HTTP call is performed to get the local time at those coordinates. If that time is between two preset limits, authentication is allowed, and the user is given a session and redirected to the profile page.

To Log in Using a Chain Containing a Scripted Authentication Module

1. Log out of AM.

2. In a browser, navigate to the AM login URL, and specify the authentication chain created in the previous procedure as the value of the service parameter.

   For example:

   ```
   https://openam.example.com:8443/openam/XUI/?service=myScriptedChain#login
   ```

3. Log in as user demo with password Ch4ng31t.

   If login is successful, the user profile page appears. The script will also output messages, such as the following in the debug/Authentication log file:
Starting scripted authentication

amScript:02/27/2017 03:22:42:881 PM GMT: Thread[ScriptEvaluator-5,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
User: demo

amScript:02/27/2017 03:22:42:882 PM GMT: Thread[ScriptEvaluator-5,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
User address: ForgeRock Inc., 201 Mission St #2900, San Francisco, CA 94105, USA

amScript:02/27/2017 03:27:31:646 PM GMT: Thread[ScriptEvaluator-7,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
latitude:37.7914374 longitude:-122.3950694

amScript:02/27/2017 03:27:31:676 PM GMT: Thread[ScriptEvaluator-7,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
User REST Call. Status: [Status: 200 OK]

amScript:02/27/2017 03:27:31:676 PM GMT: Thread[ScriptEvaluator-7,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
Current time at the users location: 10

amScript:02/27/2017 03:27:31:676 PM GMT: Thread[ScriptEvaluator-7,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
Authentication allowed!

amLoginModule:02/27/2017 03:27:31:676 PM GMT: Thread[http-nio-8080-exec-4,5,main]:
TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
Login NEXT State : -1

amLoginModule:02/27/2017 03:27:31:676 PM GMT: Thread[http-nio-8080-exec-4,5,main]:
TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
SETTING Module name.... :myScriptedAuthModule

amAuth:02/27/2017 03:27:31:676 PM GMT: Thread[http-nio-8080-exec-4,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
Module name is .. myScriptedAuthModule

amAuth:02/27/2017 03:27:31:676 PM GMT: Thread[http-nio-8080-exec-4,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
successModuleSet is : [DataStore, myScriptedAuthModule]

amJAAS:02/27/2017 03:27:31:676 PM GMT: Thread[http-nio-8080-exec-4,5,main]: TransactionId[7635cd7c-ee97-4be6-8694-9e2be8642d56-8581]
login success

Tip
The default server-side authentication script outputs log messages at the message and error level.

AM does not log debug messages from scripts by default. You can configure AM to log such messages by setting the debug log level for the AmScript service. For details, see "Debug Logging" in the Maintenance Guide.

4. (Optional) To test that the script is being used as part of the login process, edit the script to alter the times when authentication is allowed:
   
a. Log out the demo user.

b. Log in as an AM administrator, for example amAdmin.

c. Navigate to Realms > Top Level Realm > Scripts > Scripted Module - Server Side.
d. In the script, swap the values for `START_TIME` and `END_TIME`, for example:

```javascript
var START_TIME = 17;
var END_TIME   = 9; //
```

e. Click Save.

f. Repeat steps 1, 2, and 3 above, logging into the module as the `demo` user as before. The authentication result will be the opposite of the previous result, as the allowed times have inverted.

Creating Post-Authentication Plugins for Chains

Post-authentication plugins (PAP) let you include custom processing at the following places in the authentication cycle:

- At the end of the authentication process, immediately before a user is authenticated
- When a user logs out of an AM session

A common use of post-authentication plugins is to set state information in the session object in conjunction with web or Java agents. The post-authentication plugin sets custom session properties, and then the web or Java agent injects the custom properties into the header sent to the protected application.

Two issues should be considered when writing a post-authentication plugin for an AM deployment that uses client-based sessions:

**Cookie size**

You can set an unlimited number of session properties in a post authentication plugin. When AM creates a client-based session, it writes the session properties into the session cookie, increasing the size of the cookie. Very large session cookies can exceed browser limitations. Therefore, when implementing a post-authentication plugin in a deployment with client-based sessions, be sure to monitor the session cookie size and verify that you have not exceeded browser cookie size limits.

For more information about client-based session cookies, see "Session Cookies and Session Security" in the Sessions Guide.

**Cookie security**

The AM administrator secures custom session properties in sessions residing in the CTS token store by using firewalls and other typical security techniques.

However, when using client-based sessions, custom session properties are written in cookies and reside on end users' systems. Cookies can be long-lasting and might represent a security issue if any session properties are of a sensitive nature. When developing a post authentication plugin for a deployment that uses client-based sessions, be sure that you are aware of the measures securing the session contained within the cookie.
For more information about client-based session cookie security, see "Configuring Client-Based Session Security" in the Security Guide.

This section explains how to create a post-authentication plugin.

Designing Your Post-Authentication Plugin

Your post-authentication plugin class implements the AMPostAuthProcessInterface interface, and in particular the following three methods.

```java
public void onLoginSuccess(
    Map requestParamsMap,
    HttpServletRequest request,
    HttpServletResponse response,
    SSOToken token
) throws AuthenticationException

public void onLoginFailure(
    Map requestParamsMap,
    HttpServletRequest request,
    HttpServletResponse response
) throws AuthenticationException

public void onLogout(
    HttpServletRequest request,
    HttpServletResponse response,
    SSOToken token
) throws AuthenticationException
```

AM calls the onLoginSuccess() and onLoginFailure() methods immediately before informing the user of login success or failure, respectively. AM calls the onLogout() method only when the user actively logs out, not when a user's session times out. See the ForgeRock Access Management Java SDK API Specification for reference.

These methods can perform whatever processing you require. Yet, know that AM calls your methods synchronously as part of the authentication process. Therefore, if your methods take a long time to complete, you will keep users waiting. Minimize the processing done in your post-authentication methods.

**Important**

Implementing a post-authentication processing plugin in the top level realm can have unexpected effects. AM invokes a post-authentication plugin when the plugin is configured in the top level realm, which will then run for all types of authentication during startup, including user logins and internal administrative logins. The best practice first and foremost is to configure end-users to only log into subrealms, while administrators only log into the top level realm. If you need to execute the post-authentication plugin for administrative logins, make sure that the plugin can also handle internal authentications.

An alternate solution is to configure the post-authentication plugin on a per authentication chain basis, which can be configured separately for user logins or internal administrative logins.

Post-authentication plugins must be stateless: they do not maintain state between login and logout. Store any information that you want to save between login and logout in a session property. AM
stores session properties in the CTS token store after login, and retrieves them from the token store as part of the logout process.

Building Your Sample Post-Authentication Plugin

The following example post-authentication plugin sets a session property during successful login, writing to its debug log if the operation fails.

```java
/*
 * The contents of this file are subject to the terms of the Common Development and
 * Distribution License (the License). You may not use this file except in compliance with the
 * License.
 *
 * You can obtain a copy of the License at legal/CDDLv1.0.txt. See the License for the
 * specific language governing permission and limitations under the License.
 *
 * When distributing Covered Software, include this CDDL Header Notice in each file and include
 * the License file at legal/CDDLv1.0.txt. If applicable, add the following below the CDDL
 * Header, with the fields enclosed by brackets [] replaced by your own identifying
 * information: " Portions copyright [year] [name of copyright owner]".
 *
 * Copyright 2011-2019 ForgeRock AS. All Rights Reserved
 */

package com.forgerock.openam.examples;

import java.util.Map;
import javax.servlet.http.HttpServletRequest;
import javax.servlet.http.HttpServletResponse;
import org.slf4j.Logger;
import org.slf4j.LoggerFactory;
import com.iplanet.sso.SSOException;
import com.iplanet.sso.SSOToken;
import com.sun.identity.authentication.spi.AMPostAuthProcessInterface;
import com.sun.identity.authentication.spi.AuthenticationException;

/**
 * Set a session property on successful authentication.
 * If authentication fails, log a debug message.
 */

public class SamplePAP implements AMPostAuthProcessInterface {
    private final static String PROP_NAME = "MyProperty";
    private final static String PROP_VALUE = "MyValue";
    private final static String DEBUG_FILE = "SamplePAP";

    private Logger debug = LoggerFactory.getLogger(SamplePAP.class);

    public void onLoginSuccess(
            Map requestParamsMap,
            HttpServletRequest request,
            HttpServletResponse response,
            SSOToken token
    ) throws AuthenticationException {
        try {
```
If you have not already done so, download and build the sample code.

For information on downloading and building AM sample source code, see How do I access and build the sample code provided for OpenAM 12.x, 13.x and AM (All versions)? in the Knowledge Base.

In the sources, you find the following files:

- `pom.xml`
  - Apache Maven project file for the module

  This file specifies how to build the sample post-authentication plugin, and also specifies its dependencies on AM components and on the Servlet API.

- `src/main/java/com/forgerock/openam/examples/SamplePAP.java`
  - Core class for the sample post-authentication plugin

Once built, copy the .jar to the `WEB-INF/lib` directory where you deployed AM.

```bash
$ cp target/*.jar /path/to/tomcat/webapps/openam/WEB-INF/lib/
```

Restart AM or the container in which it runs.

**Configuring Your Post-Authentication Plugin**

You can associate post-authentication plugins with realms or services (authentication chains). Where you configure the plugin depends on the scope to which the plugin should apply:

- Plugins configured at the realm level are executed when authenticating to any authentication chain in the realm, provided the authentication chain does not have an associated plugin.
Plugins configured at the service level are executed if that authentication chain is used for authentication. Any plugins configured at the realm level will not execute.

In the console, navigate to Realms > Realm Name > Authentication > Settings > Post Authentication Processing. In the Authentication Post Processing Classes list, add the sample plugin class, `com.forgerock.openam.examples.SamplePAP`, and then click Save.

Alternatively, you can configure sample plugin for the realm by using the `ssoadm` command.

```
$ ssoadm set-svc-attrs \
   --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org \n   --password-file /tmp/pwd.txt \n   --servicename iPlanetAMAuthService \n   --realm /myRealm \n   --attributevalues iplanet-am-auth-post-login-process-class= \n      com.forgerock.openam.examples.SamplePAP
```

Testing Your Post-Authentication Plugin

To test the sample post-authentication plugin, login successfully to AM in the scope where the plugin is configured. For example, if you configured your plugin for the realm, `/myRealm`, specify the realm in the login URL.

```
https://openam.example.com:8443/openam/XUI/?realm=/myRealm#login
```

Although you will not notice anywhere in the user interface that AM calls your plugin, a web or Java agent or custom client code could retrieve the session property that your plugin added to the user session.

Configuring Success and Failure Redirection URLs

AM determines the redirection URL based on authentication success or failure. During success, AM redirects the user to the URL specified in the `goto` parameter and, during failure, AM redirects the user to the URL specified in the `gotoOnFail` parameter.

AM provides a number of places where you can configure success or failure URLs:

+ **Successful Authentication URL Precedence, and Where to Configure Success URLs**

Upon a successful authentication, AM determines the redirection URL in the following order:

1. The URL set in the authentication chain or authentication tree.
   - To specify a URL in an authentication chain, in the AM console, set the Successful Login URL parameter by navigating to Realm Name > Authentication > Chains > chain > Settings.
• To specify a URL in an authentication tree, add a **Success URL Node** to the tree and specify the Success URL in the node properties.

2. The URL set in the `goto` login URL parameter. For example:

```
```

3. The URL set in the Success URL attribute in the user's profile.

   In the AM console, you can set the Success URL parameter by navigating to **Realm Name > Identities > identity**. In Success URL, enter a URL, and then click Save Changes.

   You can also specify the client type by entering `ClientType|URL` as the property value. If the client type is specified, it will have precedence over a regular URL in the user's profile.

4. The URL set in the Default Success Login URL attribute in the Top Level realm.

   You can set this property on the AM console by navigating to Configure > Authentication > Core Attributes > Post Authentication Processing.

   You can also specify the client type by entering `ClientType|URL` as the property value. If the client type is specified, it will have precedence over a Default Success Login URL in the Top Level realm.

---

**Failed Authentication URL Precedence, and Where to Configure Failure URLs**

Upon a failed authentication, AM determines the redirection URL in the following order:

1. The URL set in the authentication chain or authentication tree.

   • To specify a URL in an authentication chain, in the AM console, set the Failed Login URL parameter by navigating to **Realm Name > Authentication > Chains > chain > Settings**.

   • To specify a URL in an authentication tree, add a **Failure URL Node** to the tree and specify the Failure URL in the node properties.

2. The URL set in the `gotoOnFail` parameter. For example:

```
```

3. The URL set in the Failure URL attribute in the user's profile.

   In the AM console, you can set the Failure URL parameter by navigating to **Realm Name > Identities > identity**. Under Failure URL, enter a URL, and then click Save Changes.

   You can also specify the client type by entering `ClientType|URL` as the property value. If the client type is specified, it will have precedence over a regular URL in the user's profile.
4. The URL set in the Default Failure Login URL attribute in the Top Level realm.

You can set this property on the AM console by navigating to Configure > Authentication > Core Attributes > Post Authentication Processing.

You can also specify the client type by entering ClientType|URL as the property value. If the client type is specified, it will have precedence over a Default Failure Login URL in the Top Level realm.

URLs can be relative to AM's URL, or absolute.

By default, AM trusts all relative URLs and those absolute URLs that are in the same scheme, FQDN, and port as AM. This increases security against possible phishing attacks through open redirect.

To configure AM to trust other absolute URLs, add them to the Validation Service. If you do not, on login AM will redirect to the user profile or to the administrator console, and on logout to the default logout page in the UI instead.

+ Do I Need to Add my URL to the Validation Service?

Consider an example AM deployment configured in https://am.example.com:8443/am:

<table>
<thead>
<tr>
<th>URL</th>
<th>Needs to be configured in the Validation Service?</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://am.example.com:8080/am/XUI/#login">http://am.example.com:8080/am/XUI/#login</a></td>
<td>Yes, the scheme and port are different.</td>
</tr>
<tr>
<td><a href="https://am.example.com:443/am/XUI/#login">https://am.example.com:443/am/XUI/#login</a></td>
<td>Yes, the port is different.</td>
</tr>
<tr>
<td>/am/XUI/#login</td>
<td>No, the paths relative to the AM URL are trusted.</td>
</tr>
<tr>
<td><a href="https://mypage.example.com/app/logout.jsp">https://mypage.example.com/app/logout.jsp</a></td>
<td>Yes, the scheme, port, and FQDN are different.</td>
</tr>
</tbody>
</table>

To Configure the Validation Service

1. In the AM console, navigate to Realms > Realm Name > Services.

   Note that you can add an instance of the Validation Service on the Top Level Realm, too.

2. Click Add a Service.

3. From the Choose a service type drop-down list, select Validation Service.

4. In the Valid goto URL Resources field, enter one or more valid URL patterns to allow.

   For example, http://app.example.com:80/*?*
For information on pattern matching and wildcard rules, see Specifying Resource Patterns with Wildcards in the Authorization Guide.

+ **General Examples of URL Pattern Matching**


- A wildcard before "://" only matches up to "://"

  For example, `http://*:/*` matches `http://www.example.com/hello/world` and `https://www.example.com/hello`.

- A wildcard between "://" and ":" matches up to ":"

  For example, `http://*:85` matches `http://www.example.com:85`.

- A wildcard between ":" and "/" only matches up to the first "/"


- A wildcard after "/" matches anything, depending on whether it is single-level or a wildcard appropriately.

  For example, `https://www.example.com/*` matches `https://www.example.com:443/foo/bar/baz/me`

- If you do not use any wildcards, AM exactly matches the string, so `http://www.example.com` only matches `http://www.example.com`, but NOT `http://www.example.com/` (trailing slash).

  If you put the wildcard after the path, AM expects a path (even if it is blank), so `http://www.example.com/*` matches `http://www.example.com/` and `http://www.example.com/foo/bar/baz.html`, but NOT `http://www.example.com`.


5. Click Create to save your settings.

**Tip**

To validate a goto URL over REST, use the endpoint: `/json/users?_action=validateGoto`.
$ curl \
--request POST \
--header "Accept-API-Version: protocol=2.1,resource=3.0" \
--header "Content-Type: application/json" \
--header "iPlanetDirectoryPro: AQIC5...ACMDE.*" \
--data '{"goto":"http://www.example.com/"}' \
https://openam.example.com:8443/openam/json/users?_action=validateGoto
{
  "successURL":"http://www.example.com/
}

Configuring Realm Authentication Properties

In AM, users always authenticate to a realm. Every AM realm has a set of authentication properties that applies to all authentication performed to that realm. The settings are referred to as core authentication attributes.

To configure core authentication attributes for an entire AM deployment, navigate to Configure > Authentication in the AM console, and then click Core Attributes.

The Core Authentication Attributes Page
To override the global core authentication configuration in a realm, navigate to Realms > Realm Name > Authentication > Settings in the AM console. Note that when you configure core authentication attributes in a realm, the Global tab does not appear.

Use core authentication attributes to configure:

- The list of available authentication modules
- Which types of clients can authenticate with which modules
- Connection pools for access to directory servers
- Whether to retain objects used during authentication so they can be used at logout
- Defaults for configuring authentication in a particular realm

For detailed information about the core configuration attributes, see "Core Authentication Attributes".
Chapter 3
Authenticating (Browser)

When using AM's extended user interface (XUI), the base URL to authenticate to points to /XUI/#login under the deployment URL, such as https://openam.example.com:8443/openam/XUI/#login.

The base URL to log out is similar, for example, https://openam.example.com:8443/openam/XUI/#logout/.

When authenticating using a browser, you can send AM a realm and also different authentication parameters that would help you customize the user's experience.

Specifying the Realm in the URL

When making a request to the UI, specify the realm or realm alias as the value of a realm parameter in the query string, or the DNS alias in the domain component of the URL. If you do not use a realm alias, then you must specify the entire hierarchy of the realm, starting at the Top Level Realm. For example https://openam.example.com:8443/openam/XUI/?realm=/customers/europe#login/.

The following table demonstrates additional examples:

<table>
<thead>
<tr>
<th>Description</th>
<th>Example URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full path of the realm as a parameter of XUI</td>
<td><a href="https://openam.example.com:8443/openam/XUI/?realm=/customers/europe#login">https://openam.example.com:8443/openam/XUI/?realm=/customers/europe#login</a></td>
</tr>
<tr>
<td>Realm alias of the realm as a parameter of XUI</td>
<td><a href="https://openam.example.com:8443/openam/XUI/?realm=myrealm#login">https://openam.example.com:8443/openam/XUI/?realm=myrealm#login</a></td>
</tr>
<tr>
<td>DNS Alias of the realm as the fully qualified host name in the URL</td>
<td><a href="http://myRealm.example.com:8080/openam/XUI/#login">http://myRealm.example.com:8080/openam/XUI/#login</a></td>
</tr>
</tbody>
</table>

The DNS alias is overridden by any use of either the full path or a realm alias as a query string parameter.

Authentication Parameters

AM accepts the following parameters in the query string. With the exception of IDToken parameters, use no more than one occurrence of each.
arg=newsession

Request that AM end the user's current session and start a new session.

authlevel

Request that AM authenticate the user using a module with at least the specified authentication level that you have configured.

As this parameter determines authentication module selection, do not use it with module, service, or user.

ForceAuth

If ForceAuth=true, request that AM force the user to authenticate even if they already have a valid session. On successful authentication, AM does one of the following:

• (Authentication trees only) AM issues new session tokens to users reauthenticating to meet higher security requirements.

Users reauthenticating to meet the same security requirements are not issued a new token. AM updates the existing session token with the new authentication information, if required.

• (Authentication chains only) AM does not issue new session tokens on reauthentication, regardless of the security level they are authenticating to. Instead, it updates the session token with the new authentication information, if required.

goto

On successful authentication, or successful logout, request that AM redirect the user to the specified location. Values must be URL-encoded. See "Configuring Success and Failure Redirection URLs" for more information.

gotoOnFail

On authentication failure, request that AM redirect the user to the specified location. Values must be URL-encoded. See "Configuring Success and Failure Redirection URLs" for more information.

IDToken1, IDToken2, ..., IDTokenN

Pass the specified credentials as IDToken parameters in the URL. The IDToken credentials map to the fields in the login page for the authentication module, such as IDToken1 as user ID and IDToken2 as password for basic user name, password authentication. The order depends on the callbacks in login page for the module; IDTokenN represents the Nth callback of the login page.

locale

Request that AM display the user interface in the specified, supported locale. Locale can also be set in the user's profile, in the HTTP header from her browser, configured in AM, and so on.
module

Request that AM use the authentication module instance as configured for the realm where the user is authenticating.

As this parameter determines authentication module selection, do not use it with authlevel, service, or user.

realm

Request that AM authenticate the user to the specified realm.

resource

Set this parameter to true to request resource-based authentication.

For resource-based authentication, also set the resourceURL parameter.

resourceURL

Set this parameter to the URL of the resource for resource-based authentication.

Resource-based authentication applies when an authorization policy has an environment setting of type Authentication by Module Chain or Authentication by Module Instance. When the specified resource URL matches a policy resource, AM finds the chain or module configured in the policy environment settings. AM then uses the specified chain or module to perform authentication.

For example, if you configure a policy with the resource https://www.example.com:443/index.html and the environment Authentication by Module Chain: DataStore, then the following login URL causes AM to use the DataStore chain to authenticate the user:

```
```

On successful authentication, AM redirects the user-agent to https://www.example.com/.

As shown in the example, when setting the resourceURL parameter, also set resource=true.

service

Request that AM authenticate the user with the specified authentication chain.

As this parameter determines authentication module selection, do not use it with authlevel, module, or user.

user

Request that the user, specified by their AM universal ID, authenticates according to the chain specified by the User Authentication Configuration property in their user profile. You can configure this property for a user under Realms > Realm Name > Identities > UserName.
In order for the User Authentication Configuration property to appear in user profiles, the `iplanet-am-user-service` object class must contain the `iplanet-am-user-auth-config` attribute in the identity repository schema. The default identity repository schemas provided with AM include this object class and attribute. See "Preparing Identity Repositories" in the Installation Guide for information about identity repository schema.

As this parameter determines authentication module selection, do not use it with `authlevel`, `module`, or `service`.

Example UI Login URLs

Use any of the options listed in "Authentication Parameters" as URL parameters. Note that URL parameters must appear before any occurrences of the pound or hash character (`#`). The following are example URLs with parameters:

<table>
<thead>
<tr>
<th>Description</th>
<th>Example URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log in to the top level realm, requesting that AM display the user interface in German.</td>
<td><code>https://openam.example.com:8443/openam/XUI/?realm=/&amp;locale=de#login</code></td>
</tr>
<tr>
<td>Log in to the <code>myRealm</code> subrealm whose parent is the Top Level Realm, requesting that AM display the user interface in German.</td>
<td><code>https://openam.example.com:8443/openam/XUI/?realm=/myRealm&amp;locale=de#login</code></td>
</tr>
<tr>
<td>Log in to the <code>myRealm</code> subrealm whose parent is the Top Level Realm using the <code>HOTPChain</code> authentication chain, requesting that AM display the user interface in German.</td>
<td><code>https://openam.example.com:8443/openam/XUI/?realm=/myRealm&amp;locale=de&amp;service=HOTPChain#login</code></td>
</tr>
</tbody>
</table>
Chapter 4
Authenticating (REST)

AM provides the `/json/authenticate` endpoint for authentication, and the `/json/sessions` endpoint for managing sessions and logging out.

The following table summarizes authentication operations you can perform using REST:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authenticate to AM</td>
<td>See &quot;Logging in to AM Using REST&quot;</td>
</tr>
<tr>
<td>Authentication to AM means logging in to a specific realm and receiving a session token from AM. Add parameters to the authentication request to provide AM with more information about how you want to authenticate.</td>
<td></td>
</tr>
<tr>
<td>Use the Session Token</td>
<td>See &quot;Using the Session Token After Authentication&quot;</td>
</tr>
<tr>
<td>AM provides you with a session token after authenticating to a realm. Use this token in subsequent calls to AM. For example, when using REST calls to create, modify, or delete configuration objects.</td>
<td></td>
</tr>
<tr>
<td>Log Out of AM</td>
<td>See &quot;Logging out of AM Using REST&quot;</td>
</tr>
<tr>
<td>Log out your users by sending a <code>logout</code> action to the <code>/json/sessions</code> endpoint.</td>
<td></td>
</tr>
<tr>
<td>Invalidate Sessions</td>
<td>See &quot;Invalidating All Sessions for a Given User&quot;</td>
</tr>
<tr>
<td>Obtain all the sessions for a given user and invalidate them to ensure they are logged out of AM.</td>
<td></td>
</tr>
</tbody>
</table>

Logging in to AM Using REST

To authenticate to AM using REST, make an HTTP POST request to the `json/authenticate` endpoint. You must specify the entire hierarchy of the realm, starting at the Top Level Realm. Prefix each realm in the hierarchy with the `realms/` keyword. For example, `/realms/root/realms/customers/realms/europe`. 
Authenticating (REST)
Logging in to AM Using REST

AM uses the default authentication service configured for the realm. You can override the default by specifying authentication services and other options in the REST request.

AM provides both simple authentication methods, such as providing user name and password, and complex authentication journeys that may involve a tree with inner tree evaluation and/or multi-factor authentication.

For authentication journeys where providing a user name and password is enough, you can log in to AM using a `curl` command similar to the following:

```
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "X-OpenAM-Username: demo" \
--header "X-OpenAM-Password: Ch4ng31t" \n--header "Accept-API-Version: resource=2.0, protocol=1.0" \n'https://openam.example.com:8443/openam/json/realms/root/authenticate'
{
  "tokenId": "AQIC5w...NTcy*",
  "successUrl": "/openam/console",
  "realm": "/"
}
```

The user name and password are sent in headers. This zero page login mechanism works only for name/password authentication.

Note that the POST body is empty; otherwise, AM interprets the body as a continuation of an existing authentication attempt, one that uses a supported callback mechanism. AM implements callback mechanisms to support complex authentication journeys, such as those where the user needs to be redirected to a third party or interact with a device as part of multi-factor authentication.

After a successful authentication, AM returns a `tokenId` object that applications can present as a cookie value for other operations that require authentication. This object is known as the session token. For more information about how applications can use the session token, see "Using the Session Token After Authentication".

When a client makes a call to the `/json/authenticate` endpoint appending a valid SSO token, AM returns the `tokenId` field empty when `HttpOnly` cookies are enabled. For example:

```
{
  "tokenId": "",
  "successUrl": "/openam/console",
  "realm": "/"
}
```
Tip

You can request AM to authenticate a user without providing them a session by using the noSession parameter. For more information, see "Authenticate Endpoint Parameters".

Using UTF-8 User Names

To use UTF-8 user names and passwords in calls to the /json/authenticate endpoint, base64-encode the string, and then wrap the string as described in RFC 2047:

```
encoded-word = "=?" charset "?" encoding "?" encoded-text "?="
```

For example, to authenticate using a UTF-8 username, such as dēmō, perform the following steps:

1. Encode the string in base64 format: yZfdq8mxw7g=.
3. Use the result in the X-OpenAM-Username header passed to the authentication endpoint as follows:

   ```
   $ curl 
   --request POST 
   --header "Content-Type: application/json" 
   --header "X-OpenAM-Username: =?UTF-8?B?yZfdq8mxw7g=?=" 
   --header "X-OpenAM-Password: Ch4ng31t" 
   --header "Accept-API-Version: resource=2.0, protocol=1.0" 
   'https://openam.example.com:8443/openam/json/realms/root/authenticate' 
   { 
   "tokenId": "AQIC5w...NTcy*", 
   "successUrl": "/openam/console", 
   "realm": "/"
   }
   ```

Authenticating to Specific Authentication Services

You can provide AM with additional information about how you are authenticating. For example, you can specify the authentication tree you want to use, or request from AM a list of the authentication services that would satisfy a particular authentication condition.

The following example shows how to specify the ldapService chain by using the authIndexType and authIndexValue query string parameters:

```
$ curl 
--request POST 
--header "X-OpenAM-Username: demo" 
--header "X-OpenAM-Password: Ch4ng31t" 
--header 'Accept-API-Version: resource=2.0, protocol=1.0' 
'https://openam.example.com:8443/openam/json/realms/root/authenticate?authIndexType=service&authIndexValue=ldapService'
```

You can exchange the ldapService chain with any other chain or tree.
For more information about using the `authIndexType` parameter to authenticate to specific services, see "Authenticate Endpoint Parameters".

Returning Callback Information to AM

The `/json/authenticate` endpoint supports callback mechanisms to perform complex authentication journeys. Whenever AM needs to return or request information, it will return a JSON object with the authentication step, the authentication identifier, and the related callbacks.

The following types of callbacks are available:

- **Read-only callbacks.** AM uses read-only callbacks to provide information to the user, such as text messages or the amount of time that the user needs to wait before continuing their authentication journey.

- **Interactive callbacks.** AM uses interactive callbacks to ask the user for information. For example, to request their user name and password, or to request that the user chooses between different options.

- **Backchannel callbacks.** AM uses backchannel callbacks when it needs to access additional information from the user's request. For example, when it requires a particular header or a certificate.

Read-only and interactive callbacks have an array of `output` elements suitable for displaying to the end user. The JSON returned in interactive callbacks also contains an array of `input` elements, which must be completed and returned to AM. For example:

```json
"output": [
  {
    "name": "prompt",
    "value": " User Name: "
  },

  "input": [
    {
      "name": "IDToken1",
      "value": ""
    }
  ]
]
```

The value of some interactive callbacks can be returned as headers, such as the `X-OpenAM-Username` and `X-OpenAM-Password` headers, but most of them must be returned in JSON as a response to the request.

Depending on how complex the authentication journey is, AM may return several callbacks sequentially. Each must be completed and returned to AM until authentication is successful.

The following example shows a request for authentication, and AM's response of the `NameCallback` and `PasswordCallback` callbacks:
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "Accept-API-Version: resource=2.0, protocol=1.0" \
'https://openam.example.com:8443/openam/json/realms/root/authenticate'

```json
{
    "authId": "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJvdGsiOiJ...", ①
    "template": "", ②
    "stage": "DataStore1", ③
    "callbacks": [
        {
            "type": "NameCallback", ④
            "output": [ ⑤
                {
                    "name": "prompt",
                    "value": " User Name: ">
                },
            ],
            "input": [ ⑥
                {
                    "name": "IDToken1",
                    "value": ""
                }
            ]
        },
        {
            "type": "PasswordCallback", ④
            "output": [ ⑤
                {
                    "name": "prompt",
                    "value": " Password: ">
                },
            ],
            "input": [ ⑥
                {
                    "name": "IDToken2",
                    "value": ""
                }
            ]
        }
    ]
}
```

**Key:**

① The JWT that uniquely identifies the authentication context to AM.
② A template to customize the look of the authentication module, if exists. For more information, see How do I customize the Login page? in the ForgeRock Knowledge Base.
③ The authentication module stage where the authentication journey is at the moment.
④ The type of callback. It must be one the "Supported Callbacks".
⑤ The information AM offers about this callback. Usually, this information would be displayed to the user in the UI.
The information AM is requesting. The user must fill the "value": "" object with the required information.

To respond to a callback, send back the whole JSON object with the missing values filled. The following example shows how to respond to the NameCallback and PasswordCallback callbacks, with the demo and Ch4ng31t values filled:

```
$ curl \
  --request POST \
  --header "Content-Type: application/json" \
  --header "Accept-API-Version: resource=2.0, protocol=1.0" \
  --data ' {
    "authId" : "eyJ0eXAiOiJKV1QiLCJhbGciOiJIUzI1NiJ9.eyJvdGsiOiJ...",
    "template": "",
    "stage": "DataStore1",
    "callbacks": [ 
      { 
        "type": "NameCallback",
        "output": [
          { 
            "name": "prompt",
            "value": " User Name: "
          } 
        ],
        "input": [
          { 
            "name": "IDToken1",
            "value": "demo"
          } 
        ] 
      }, 
      { 
        "type": "PasswordCallback",
        "output": [
          { 
            "name": "prompt",
            "value": " Password: "
          } 
        ],
        "input": [
          { 
            "name": "IDToken2",
            "value": "Ch4ng31t"
          } 
        ] 
      } 
    ] }
  }' \\
  'https://openam.example.com:8443/openam/json/realms/root/authenticate'

{ 
  "tokenId": "AQIC5wM2...U3MTE4NA..*",
  "successUrl": "/openam/console",
  "realm": "/"
}
```

On complex authentication journeys, AM may send several callbacks sequentially. Each must be completed and returned to AM until authentication is successful.
For more information about the callbacks AM may return, see "Supported Callbacks".

Using the Session Token After Authentication

After a successful authentication, AM returns a `tokenId` object that applications can present as a cookie value for other operations that require authentication. This object is a session token—a representation of the exchange of information and credentials between AM and the user or identity.

The type of `tokenId` returned varies depending on where AM stores the sessions for the realm to which the user authenticates:

- If CTS-based sessions are enabled, the `tokenId` object is a reference to the session state stored in the CTS token store.
- If client-based sessions are enabled, the `tokenId` object is the session state for that particular user or identity.

Developers should be aware that the size of the `tokenId` for client-based sessions—2000 bytes or greater—is considerably longer than for CTS-based sessions—approximately 100 bytes. For more information about session tokens, see "Session Cookies and Session Security" in the Sessions Guide.

The following is a common scenario when accessing AM by using REST API calls:

- First, call the `/json/authenticate` endpoint to log a user in to AM. This REST API call returns a `tokenId` value, which is used in subsequent REST API calls to identify the user:

  ```
  curl \
  --request POST \
  --header "Content-Type: application/json" \
  --header "X-OpenAM-Username: demo" \
  --header "X-OpenAM-Password: Ch4ng31t" \
  --header "Accept-API-Version: resource=2.0, protocol=1.0" \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate' \
  
  
  "tokenId":"AQIC5wM...TU3OQ*", 
  "successUrl":"/openam/console", 
  "realm":"/
  
  }
  ``

  The returned `tokenId` is known as a session token (also referred to as an SSO token). REST API calls made after successful authentication to AM must present the session token in the HTTP header as proof of authentication.

- Next, call one or more additional REST APIs on behalf of the logged-in user. Each REST API call passes the user's `tokenId` back to AM in the HTTP header as proof of previous authentication.

  The following is a partial example of a `curl` command that inserts the token ID returned from a prior successful AM authentication attempt into the HTTP header:
Observe that the session token is inserted into a header field named `iPlanetDirectoryPro`. This header field name must correspond to the name of the AM session cookie—by default, `iPlanetDirectoryPro`. You can find the cookie name in the AM console by navigating to Deployment > Servers > Server Name > Security > Cookie, in the Cookie Name field of the AM console.

Once a user has authenticated, it is not necessary to insert login credentials in the HTTP header in subsequent REST API calls. Note the absence of `X-OpenAM-Username` and `X-OpenAM-Password` headers in the preceding example.

Users are required to have appropriate privileges in order to access AM functionality using the REST API. For example, users who lack administrative privileges cannot create AM realms. For more information on the AM privilege model, see "Delegating Privileges" in the Security Guide.

Finally, call the REST API to log the user out of AM as described in "Authenticating (REST)". As with other REST API calls made after a user has authenticated, the REST API call to log out of AM requires the user's `tokenId` in the HTTP header.

Logging out of AM Using REST

Authenticated users can log out with the token cookie value and an HTTP POST to `/json/sessions/?_action=logout`:

```bash
$ curl \
  --request POST \
  --header "iPlanetDirectoryPro: AQIC5w...NTcy*" \
  --header "Accept-API-Version: resource=3.1, protocol=1.0" \
  https://openam.example.com:8443/openam/json/realms/root/sessions/?_action=logout
{
  "result":"Successfully logged out"
}
```

Invalidating All Sessions for a Given User

To log out all sessions for a given user, first obtain a list of session handles of their active sessions, by performing an HTTP GET to the `/json/sessions/` endpoint, using the SSO token of an administrative user, such as `amAdmin` as the value of the `iPlanetDirectoryPro` header. You must also specify a `queryFilter` parameter.
The queryFilter parameter requires the name of the user, and the realm to search. For example, to obtain a list of session handles for a user named demo in the Top Level Realm, the query filter value would be:

```
username eq "demo" and realm eq "/"
```

**Note**

The query filter value must be URL encoded when sent over HTTP.

For more information on query filter parameters, see "Query" in the Getting Started with REST.

In the following example, there are two active sessions:

```bash
$ curl \
--request GET \
--header "iPlanetDirectoryPro: AQICS...NzEz*" \
--header "Accept-API-Version: resource=3.1, protocol=1.0" \
https://openam.example.com:8443/openam/json/realms/root/sessions?_queryFilter=username%20eq%20%22demo%22%20and%20realm%20eq%20%22%2F%22
{
    "result": [
        {
            "_rev": "652365455",
            "username": "demo",
            "universalId": "id=demo,ou=user,dc=openam,dc=forgerock,dc=org",
            "realm": "/myrealm",
            "sessionHandle": "shandle:cmvShY1....AA.*",
            "latestAccessTime": "2019-10-03T09:36:53.041Z",
            "maxIdleExpirationTime": "2019-10-03T10:06:53Z",
            "maxSessionExpirationTime": "2019-10-03T11:36:53Z",
        }
    ],
    "resultCount": 1,
    "pagedResultsCookie": null,
    "totalPagedResultsPolicy": "NONE",
    "totalPagedResults": -1,
    "remainingPagedResults": -1
}
```

To log out all sessions for the specific user, perform an HTTP POST to the `/json/sessions/` endpoint, using the SSO token of an administrative user, such as amAdmin as the value of the iPlanetDirectoryPro header. You must also specify the logoutByHandle action, and include an array of the session handles to invalidate in the POST body, in a property named sessionHandles, as shown below:
Invalidating All Sessions for a Given User

```bash
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "iPlanetDirectoryPro: AQICS...NzEz*" \
--header "Accept-API-Version: resource=3.1, protocol=1.0" \
--data '{
   "sessionHandles": [
      "shandle:SJ80.*AA....JT.*",
      "shandle:H4CV.*DV....FM.*"
   ]
}' https://openam.example.com:8443/openam/json/realms/root/sessions/?_action=logoutByHandle
{
   "result": {
      "shandle:SJ80.*AA....JT.*": true,
      "shandle:H4CV.*DV....FM.*": true
   }
}
```
Chapter 5
Single Sign-On

Single sign-on (SSO) lets users who have authenticated to AM access multiple independent services from a single login session by storing user sessions as HTTP cookies. Cross-domain single sign-on (CDSSO) is an AM-specific capability that provides SSO inside the same organization within a single domain or across domains. For example, CDSSO allows your AM servers in the DNS domain .internal.net to provide authentication and authorization to web and Java agents from the .internal.net domain and other DNS domains, such as .example.net.

Since CDSSO removes the constraint of configuring SSO depending on the DNS domain, it simplifies the deployment of SSO in your environment.

When implementing CDSSO, take into account the following points:

• For SSO across multiple organizations or when integrating with other access management software, use AM’s federation capabilities, such as OAuth 2.0 or SAML v2.0.

• Web Agents and Java Agents both support CDSSO.

  AM also supports CDSSO with IG version 6 or later. For more information, see Single Sign-On and Cross-Domain Single Sign-On in the ForgeRock Identity Gateway Gateway Guide.

• CDSSO supports CTS-based and client-based sessions. For more information about session state impact on CDSSO, see Impact of Storage Location for Sessions in the Sessions Guide.

Web Agents and Java Agents wrap the SSO session token inside an OpenID Connect (OIDC) JSON Web Token (JWT). During the CDSSO flow, the agents create cookies for the different domains specified in the agent profile, and the oauth2/authorize endpoint authorizes the different cookie domains as required.

The following diagram illustrates the CDSSO flow for Web Agents and Java Agents:

---

1 If you are unfamiliar with HTTP cookies, see “About HTTP Cookies” for more information.
Web and Java Agents CDSSO Flow

**AM Web Agents and Java Agents CDSSO Flow**

**ForgeRock Access Management**

**Browser**

1. Browse to protected resource.
   - No SSO token for resource domain yet

```
[Java Agent]
2. Set an amFilterCDSSORequest cookie and redirect...
   - The amFilterCDSSORequest cookie holds information consumed when processing the form submitted in 15
```

```
[Web Agent]
3. Redirect...
   - ...to oauth2/authorize endpoint.
```

```
5. If browser presents SSO token, request SSO token validation
```

**Block not executed when Browser requests a resource in the second domain**

```
7. Redirect...
8. ...to AM for authentication
9. Authentication page
10. Submit credentials
11. Set valid SSO token with AM domain name and redirect...
12. ...to oauth2/authorize endpoint
```

```
13. Request SSO token validation
14. SSO token is valid.
15. Send self-submitting form with OIDC token having embedded restricted SSO token
```

```
[Java Agent]
16. Form POSTs automatically to an agent endpoint that consumes the response
   - Sets cookie domain to FQDN of resource and validates OIDC token
   - Redirect, with request to delete the amFilterCDSSORequest cookie...
   - ...to protected resource
```

```
[Web Agent]
19. Form POSTs automatically to protected resource
   - Policy agent intercepts and validates OIDC token
```

```
20. Request SSO token validation
21. Response for SSO token validation
22. Request policy decision
23. Response for policy decision
24. Allow access and return resource, or deny access and return HTTP 403
```

Browser

Agent

- `oauth2/authorize` Endpoint

Policy, Session Services

Authentication Service
About Realms and SSO

When changing authentication realms, a subject leaves the current SSO realm. The new SSO realm might apply to different applications, and use a different authentication process. For AM, logging in to a new realm means logging out of the current realm.

When a user interactively changes realms through the AM console, AM offers the option of logging out of the current realm to log in to the new realm, or choosing to remain logged in to the current realm.

The result depends on the user's choice:

- If the user cancels the change at this point, the user remains logged in to the current realm, and is not logged in to the new realm.
- If the user chooses to log in to the new realm, AM first logs the user out of the current realm, and then prompts the user to log in to the new realm.

About HTTP Cookies

To understand how SSO works, you need to understand some key elements of the HTTP cookie, as described in RFC 6525, HTTP State Management Mechanism.

Within an HTTP cookie, you can store a single custom name=value pair, such as sessionid=value. Other properties within a cookie are as follows:

**Domain**

Normally set to the full URL that was used to access the configurator. To work with multiple subdomains, the Domain should be set to a URL like Domain=server.example.net. This is also known as the cookie domain.

**Path**

The directory in the URL to which the cookie applies. If the Path=/openam, the cookie applies to the /openam subdirectory of the URL, and lower level directories, including openam/XUI.

**Secure**

If the Secure name is included, the cookie can be transferred only over HTTPS. When a request is made over HTTP, the cookie is not made available to the application.

For more information, see "Configuring Secure Session Cookies" in the Security Guide.

**HttpOnly**

When the HttpOnly flag is included, that cookie will not be accessible through JavaScript. According to RFC 6265, the noted flag "instructs the user agent to omit the cookie when providing access to cookies via 'non-HTTP' APIs (for example, a web browser API that exposes cookies to scripts)."

For more information, see "Configuring HttpOnly Session Cookies" in the Security Guide.

Expires

The lifetime of a cookie can be limited, with an Expires name configured with a time, based on UTC (GMT).

**Warning**

Do not take a shortcut with a top-level domain. Web browser clients today are designed to ignore cookies set to top-level domains including com, net, and co.uk. In addition, a cookie with a value like Domain= appl.example.net will not work for similar subdomains, such as app2.example.net.

Implementing CDSSO

CDSSO provides SSO capabilities for AM servers and web or Java agents within a single domain or across domains in the same organization.

CDSSO is the only mode of operation of Web Agents and Java Agents and, therefore, no additional configuration is required to make it work. You must, however, protect the session cookie against hijacking. For more information, see "Enabling Restricted Tokens for CDSSO Session Cookies" in the Security Guide.

**Tip**

IG also supports CDSSO with AM. For more information, see the ForgeRock Identity Gateway Gateway Guide.

Troubleshooting SSO

In general, problems with single sign-on relate to some sort of mismatch of domain names. For example, a cookie that is configured on a third-level domain, such as sso.example.net will not work with an application on a similar domain, such as app.example.net. The following list describes scenarios that may lead to similar problems:

- **When a cookie domain does not match a domain for the protected application.**

  Assume the application is configured on a domain named example.org. That application will not receive an SSO token configured on the example.net domain.

- **When a third-level domain is used for the SSO token.**

  If an SSO token is configured on sso.example.net, an application on app.example.net does not receive the corresponding session token. In this case, the solution is to configure the SSO token on example.net.
• When the **Cookie Security** or the **CDSSO Secure Enable** properties are configured in the agent profile with a regular HTTP application.

If you need encrypted communications for an application protected by AM, use the **Cookie Security** or the **CDSSO Secure Enable** properties and make sure the application is accessible over HTTPS.

• When the path listed in the cookie does not match the path for the application.

Perhaps the cookie is configured with a `/helloworld` path; that will not match an application that might be configured with a `/hellomars` path. In that case, the application will not receive the cookie.

• When an inappropriate name is used for the cookie domain

As noted earlier, client browsers are configured to ignore first-level domains, such as `com` and `net` as well as functional equivalents, such as `co.uk` and `co.jp`.

• When working with different browsers

The `name=value` pairs described earlier may not apply to all browsers. The requirements for an HTTP cookie sent to an IE browser may differ from the requirements for other standard browsers, such as Firefox and Chrome. Based on anecdotal reports, IE does not recognize domain names that start with a number. In addition, IE reportedly refuses cookies that include the underscore `_` character in the FQDN.

• When a client-based session cookie exceeds the maximum size permitted by the browser

As described in "**Session Cookies and Session Security**" in the **Sessions Guide**, the default size of the `iPlanetDirectoryPro` cookie is approximately 2,000 bytes. When you customize AM sessions by adding attributes, the cookie size grows. Browsers allow cookie sizes between 4,000 and 5,200 bytes, depending on the browser. AM single sign-on does not support a cookie size that exceeds the maximum cookie size allowed by the browser.
Chapter 6
Social Authentication

AM supports delegated authentication through third-party identity providers, such as Facebook, Google, and VKontakte. The following table summarizes the social authentication providers and standards that AM 7 supports:

<table>
<thead>
<tr>
<th>Provider/Standard</th>
<th>Authentication Node?</th>
<th>Authentication Module?</th>
</tr>
</thead>
<tbody>
<tr>
<td>OpenID Connect 1.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>OAuth 2.0</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Facebook</td>
<td>Yes</td>
<td>Yes ^a</td>
</tr>
<tr>
<td>Google</td>
<td>Yes</td>
<td>Yes ^a</td>
</tr>
<tr>
<td>Instagram</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft</td>
<td>Yes b</td>
<td>Yes c</td>
</tr>
<tr>
<td>VKontakte</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WeChat</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>WeChat Mobile</td>
<td>No</td>
<td>Yes</td>
</tr>
</tbody>
</table>

^a Configure a Social Auth OpenID authentication module.
^b Configure an OAuth 2.0 authentication node.
^c Configure a Social Auth OAuth2 authentication module.

Configuring Social Authentication

Configuring social authentication is a three-step process:

1. Obtain a client ID and client secret from the social provider, as well as their implementation details.

Some modules and nodes are pre-configured for specific providers because of their implementation of OAuth 2.0/OpenId Connect, while you need the details for other providers, as shown in the preceding table.

+ How/Where do I Obtain a Client ID or the Implementation Details?

To obtain a Client ID and Client Secret, register an application with the third party provider. For example:
Facebook

Facebook App Quickstart

Google

Google Developers Console

Note
You must enable the Google+ API in order to authenticate with Google. To enable the Google+ API, login to the Google Developers Console, select your project, navigate to APIs and auth > APIs, and then set the status of the Google+ API to ON.

VKontakte

VKontakte Developers - My apps

If you need to use the generic OAuth 2.0 or OpenID Connect modules, you need at least, the following details from your provider:

- Does it need an OAuth 2.0 or an OpenID Connect client?
- What is the URL of their authentication endpoint?
- What is the URL of their access token endpoint?
- What is the URL of their user profile service?
- Which scopes you need to request from them?

2. Configure a chain or tree that contains the module or node relevant for your social provider. See the preceding table for links to more information about each of them.

For general information about configuring modules and chains, and nodes and trees, see "Authentication Modules and Chains" and "Authentication Nodes and Trees".

Optionally, you can also integrate social authentication modules with IDM. See "To Integrate Social Authentication with Identity Management".

3. Configure the Social Authentication Implementation service to add social provider logos to the login page, if required. For example:

+ Login Screen With Social Authentication Logos
See "Configuring the Social Authentication Implementations Service".

Note
To allow AM to contact internet services through a proxy, see "Settings for Configuring a JVM Proxy" in the Installation Guide.

To Integrate Social Authentication with Identity Management

After configuring the relevant node or module, perform the following additional steps to configure AM to work with an IDM deployment:

1. (Optional) (Google only) Navigate to the configuration of the node or module:
   • Go to Realms > Realm Name > Authentication > Modules, and click on the name of the module. For example, GoogleSocialAuthentication.
   • Go to Realms > Realm Name > Authentication > Trees, and click on the name of the tree that has the social node. For example, GoogleSocialTree.
Modify the configuration of the node or module as follows:

a. Add `sub=iplanet-am-user-alias-list` to the Account Mapper Configuration property.

   The `iplanet-am-user-alias-list` property defines one or more aliases for mapping a user's multiple profiles.

b. Add `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|iplanet-am-user-alias-list|google-` to the Attribute Mapper property.

c. Add `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|iplanet-am-user-alias-list|google-` to the Attribute Mapper property.

2. (Optional) (Google only) Navigate to the configuration of the node or module:

   • Go to Realms > Realm Name > Authentication > Modules, and click on the name of the module. For example, `GoogleSocialAuthentication`.

   • Go to Realms > Realm Name > Authentication > Trees, and click on the name of the tree that has the social node. For example, `GoogleSocialTree`.

3. (Optional) (Facebook only) Navigate to the configuration of the node or module:

   • Realms > Realm Name > Authentication > Modules, and click on the name of the module For example, `FacebookSocialAuthentication`.

   • Go to Realms > Realm Name > Authentication > Trees, and click on the name of the tree that has the social node. For example, `FacebookSocialTree`.

Modify the configuration of the node or module as follows:

a. Add `id=iplanet-am-user-alias-list` to the Account Mapper Configuration property.

   The `iplanet-am-user-alias-list` property defines one or more aliases for mapping a user's multiple profiles.

b. Add `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|iplanet-am-user-alias-list|facebook-` to the Attribute Mapper property.

4. Enable the Create account if it does not exist property.

5. Save your changes.
Configuring the Social Authentication Implementations Service

You can add logos to the login page to allow users to authenticate using configured social authentication providers.

To Configure the Social Authentication Implementations Service

Perform the following steps to add a logo for the authentication provider to the AM login screen:

1. Go to Realms > Realm Name > Services, and perform one of the following actions:
   - If the Social Authentication Implementations Service exists, click on it.
   - If the Social Authentication Implementations Service does not exist, add it as a service.

   The social authentication implementations page appears.

2. In the Display Names section, enter a Map Key, enter the text to display as ALT text on the logo in the Corresponding Map Value field, and then click Add.

   For example, add Facebook as the key, and Authenticate with Facebook as the text.

   Note
   AM uses the value in the Map Key fields throughout the configuration to tie the various implementation settings to each other. The value is case-sensitive.

3. In the Authentication Chains section, re-enter the Map Key used in the previous step, and click Add.

   Now, select the relevant authentication tree or chain from the drop-down list.

4. In the Icons section, re-enter the Map Key used in the previous steps, enter the path to a logo image to be used on the login screen in the Corresponding Map Value list, and then click Add.

5. In the Enabled Implementations field, re-enter the Map Key used in the previous steps.

   Tip
   Removing a Map Key from the Enabled Implementations list removes the associated logo from the login screen. There is no need to delete the Display Name, Authentication Chain or Icon configuration to remove the logo from the login screen.

6. Review your configuration, and save your changes.
An icon now appears on the AM login screen, allowing users to authenticate with the third party authentication provider.
Chapter 7
Suspended Authentication

Suspended authentication lets you save a user's progress through an authentication tree, and later resume from the same point.

Any input provided during authentication is saved when the authentication tree is suspended, and restored when the authentication tree is resumed. This lets the authentication tree continue after closing the browser, using a different browser, or even on a different device.

When suspending an authentication tree, you provide the user with a URL they must visit to resume their authentication. That URL contains a unique identifier for retrieving the saved progress, and can only be used once. These URLs are sometimes referred to as *magic links*.

The following nodes support suspended authentication:

- "Email Suspend Node"

Typical use cases include passwordless authentication, and email verification during progressive profile completion.

The following example lets a user authenticate if they have forgotten their username:

After obtaining the user's email address in the "Attribute Collector Node", the example tree attempts to identify the user. Then, the tree attempts to email the user, and suspends itself.
Note that both the *True* and *False* outcomes are mapped into the "Email Suspend Node", to reduce potential data leakage. If the username is found, it is included in the email sent to the user, along with the link to use to resume the authentication tree.

When the user follows the link, the authentication tree resumes at the "Inner Tree Evaluator Node", which lets the user authenticate with their recovered username and credentials.

### Configuring Suspended Authentication

You can configure the length of time an authentication session can last for in AM, so that resources can be freed up from incomplete authentications. You can also configure the length of time that a tree can be suspended.

You should set this value to the minimum reasonable time required to complete the authentication. For example, if you are sending an email, 10 minutes might be reasonable. The time allowed for suspending authentication must be the same or less than the maximum duration for the tree.

To configure these timeouts, in the AM administration console, go to Configure > Authentication > Core Attributes > Trees. For more information about the properties, see Trees.

### Adding Suspended Authentication to Custom Nodes

You can enable suspended authentication in your custom nodes. For more information, see "The Action Interface" in the *Authentication Node Development Guide*. 
Chapter 8
MFA: Web Authentication (WebAuthn)

Web Authentication allows users to authenticate by using an authenticator device, for example the fingerprint scanner on their laptop or phone.

Communication with the authentication devices is handled by the user's browser. AM requests that the browser activates authenticators with certain criteria; for example it must be built-in to the platform rather than a roaming USB device, and/or that it must verify the identity of the user, rather than simply that a user is present.

To use WebAuthn with AM, users must first register their authenticators. If recovery codes are enabled, users must also make a copy of their codes.

Registration involves the selected authenticator creating, or minting, a key pair. The public key of the pair is returned to AM and stored in the user's profile. The private key is stored securely, either in the authenticator itself, or in the platform managing the authenticators. The private key does not leave the client at any time.

When authenticating by using WebAuthn, the authenticator locks some data using the stored private key, which is sent to AM to verify using the public key stored in the user's profile. If the data is verified as being from the correct device, and passes any attestation checks, the authentication is considered successful.

AM supports web authentication in the following user agents and platform minimum versions:

<table>
<thead>
<tr>
<th>User Agent</th>
<th>Platform</th>
<th>Version</th>
<th>Supported?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Desktop</td>
<td>70</td>
<td>✔</td>
</tr>
<tr>
<td></td>
<td>Android</td>
<td>70</td>
<td>✔</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>Desktop</td>
<td>18</td>
<td>✔</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Desktop</td>
<td>60</td>
<td>✔</td>
</tr>
</tbody>
</table>

Creating Trees for Web Authentication (WebAuthn)

This section explains how to create an authentication tree to authenticate users by using a WebAuthn device, and allow them to register a device if they have not already done so.
If the user has already registered a WebAuthn device, they only need to enter their username, and then perform the authorization gesture with their registered device to access their profile.

If the user does not have a registered device, they are prompted for their password, and must be verified by the Data Store Decision Node before registering a new WebAuthn device. Once completed, they must authenticate with the new device before gaining access to their profile page.

To Create a Tree for WebAuthn Registration and Authentication

This procedure assumes the following:

- The WebAuthn Profile Encryption Service is configured.

This service specifies the attribute in which to store information about registered WebAuthn devices, and whether to encrypt that information.

For detailed information about the available properties, see "WebAuthn Profile Encryption Service" in the Reference.

To create a multi-factor authentication tree for WebAuthn authentication, and registration if required, perform the following steps:

Note

The tree created in this procedure is an example, and does not provide user-friendly features, such as allowing retries of the users' password.

1. Log in to the AM console as an AM administrator, for example, amAdmin.

2. Select the realm that will contain the authentication tree.

3. Create the authentication tree as follows:

   a. Select Authentication > Trees, and then click Create Tree.

      The New Tree page appears.

   b. Specify a name of your choosing, for example, myWebAuthnTree, and then click Create.

      The authentication tree designer is displayed, with the Start entry point connected to the Failure exit point.

      You can add nodes to the authentication tree by dragging the node from the Components panel on the left-hand side and dropping it into the designer area.

   c. Add the following nodes to the authentication tree:

      - Username Collector Node
4. Test your WebAuthn authentication and registration tree as follows:

a. Logout of AM, and then navigate to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=myWebAuthnTree#login

**Important**
You must connect over HTTPS in order to use Web Authentication.

A login screen prompting you to enter your user ID appears.

b. Enter the username of an existing account in the specified realm. For example, enter demo.

c. (Optional) If the demo user does not have a registered device:

i. When asked for the user's password, enter the default Ch4ng31t.
ii. At the following screen, register a WebAuthn authenticator by performing an authorization gesture, for example press the button on a connected Yubikey.

The WebAuthn Registration node waiting for an authenticator.

Note
The user's browser may present a consent pop-up to allow access to the authenticators available on the client. When consent has been granted, the browser activates the relevant authenticators, ready for registration.

If the device registration is successful, the user is redirected to the new node in the tree in order to authenticate with the newly registered device.

d. When prompted, authenticate to AM by performing an authorization gesture with a registered device.

If the authorization is verified, the user's profile page is displayed.

• Click the Dashboard link to see a list of the registered WebAuthn authenticators, and to rename or delete them. The default name for a new device is New Security Key.

Configuring Usernameless Authentication with ForgeRock Go

With ForgeRock Go, you can create a secure and seamless login experience by authenticating with any credential on the user’s device that supports FIDO2 WebAuthn.
You can also extend passwordless authentication to include usernameless authentication with popular authenticators that support resident keys; for example, Windows Hello (biometric authenticators).

To use usernameless authentication, you must register an authenticator that supports resident keys to the user's profile, and enable the option to associate a certificate on the device with the user's username.

Once registered, that device can be used to authenticate the user without them having to provide their credentials; they just have to select the appropriate entry to use from the list their device provides.

To Configure Usernameless Authentication with ForgeRock Go

To Configure Usernameless Authentication with ForgeRock Go, create a Web Authentication registration tree to associate a device that supports resident keys with a user. The registration tree is similar to that described in "Creating Trees for Web Authentication (WebAuthn)".

Create a second tree that lets users authenticate to AM without entering their username or password, by using Forgerock Go.

Note

The trees in this procedure are examples, and do not provide user-friendly features, such as allowing retries, or redirecting to further help on failures.

1. Log in to the AM console as an AM administrator, for example, amAdmin.
2. Select the realm that will contain the ForgeRock Go registration tree.
3. Create the registration tree as follows:
   a. Select Authentication > Trees, and then click Create Tree.
      The New Tree page appears.
   b. Specify a name of your choosing, for example, fr-go-reg, and then click Create.
      The authentication tree designer is displayed, with the Start entry point connected to the Failure exit point.
      You can add nodes to the authentication tree by dragging the node from the Components panel on the left side and dropping it into the designer area.
   c. Add the following nodes to the authentication tree:
      • Username Collector Node
      • Password Collector Node
      • Data Store Decision Node
d. Connect the nodes as demonstrated in the following figure:

Tip
You can use JavaScript similar to the following in the Scripted Decision node to create a suitable display name:

```javascript
var username = sharedState.get("username");
var displayName = ";

var fullName = idRepository.getAttribute(username, "CN").iterator().next();
var email = idRepository.getAttribute(username, "mail").iterator().next();

if(fullName){
    displayName += fullName;
}

if(email){
    displayName += ' (' + email + ');
}

sharedState.put("displayName", displayName.toString());
outcome = "continue";
```

If you place a display name value into shared state, enter the variable name into the Shared state attribute for display name property in the WebAuthn Registration node.

e. In the WebAuthn Registration node properties, ensure Username to device is enabled.

f. Save your changes.

4. Create an authentication tree for ForgeRock Go, and specify a name of your choosing; for example, fr-go-auth.
a. Add a WebAuthn Authentication Node to the authentication tree.

b. Connect the nodes as demonstrated in the following figure:

![Diagram of authentication tree]

c. In the WebAuthn Authentication node properties, ensure Username from device is enabled.

d. Save your changes.

5. You are now ready to register a device, and authenticate by using ForgeRock Go.

Proceed to "Registering and Authenticating with ForgeRock Go".

Registering and Authenticating with ForgeRock Go

Follow these steps to register a device for use with usernameless authentication, and then authenticate without having to provide your username or password.

1. To register a device for use with ForgeRock Go:

a. Log out of AM, and then navigate to your ForgeRock Go registration tree, with a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=fr-go-reg#login

   **Important**
   
   You must connect over HTTPS in order to use Web Authentication.

   A login screen prompting you to enter your credentials appears.

b. Enter the username and password of an existing account in the specified realm. For example, enter demo, and the password Ch4ng31t, and then click Log In.

c. If you are authenticating from a FIDO2-enabled device, a dialog will display asking you to choose the method to verify your identity; for example, a USB security key, or built-in biometric sensor.

   Select the option you want to associate with the user.

d. Perform the authorization gesture of the chosen option when asked to do so. For example, scan your fingerprint with TouchID, or press the button on your USB security key.
If successful, you are taken to the profile page for the user.

e. (Optional) The new device appears on the Dashboard page, as New Security Key.

   Give a suitable name to the device; for example, *Apple Mac TouchID*, by clicking the context icon (﴿), and selecting Settings.

2. To use a device to authenticate without username or password by using ForgeRock Go:

   a. Log out of AM, and then navigate to your ForgeRock Go authentication tree, with a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=fr-go-auth#login

   **Important**

   You must connect over HTTPS in order to use Web Authentication.

   b. Perform the authorization gesture of the chosen option when asked to do so. For example, scan your fingerprint with TouchID, or press the button on your USB security key.

   If successful, a list of the accounts associated with the authentication device displays:

   ![Account List](image)

   Select an account to sign in

   Demo User (demo.user@example.com)
   demo

   Note that in this example the user's full name and email address appear, which were gathered by the Scripted Decision node from the user's profile during registration.

   c. Select the account that you want to sign in.

   If successful, you are taken to the profile page for the user, without having to enter username or password credentials!
Configuring WebAuthn Trust Anchors

AM 7 adds support for a new CA attestation type, whereby the attestation data received from a device can be verified as authentic by using the relevant CA certificates.

If the trust chains defined by the CA certificates have CRL or OCSP entries, AM is also able to check for revocation.

To Configure WebAuthn Trust Anchors

To configure trust anchors in AM, you should obtain the CA-issued certificate chains for the devices you intend to verify, and make them available to AM in a secret store.

When the relevant certificate chains are in place, configure the "WebAuthn Registration Node" with the alias of the secret store, and set Preferred mode of attestation to either DIRECT or INDIRECT.

Perform the following steps to enable trust anchors and achieve CA attestation for trusted devices:

1. Obtain the CA-issued certificate chains for the devices you want to verify.

   You may need to consult the device manufacturer to obtain the certificate chains.

2. Import the certificate chains into a keystore:

   ```
   $ keytool -import \
   -file /Downloads/vendor-a-ca.crt \
   -alias "vendor-a-devices" \
   -storetype JCEKS \
   -storepass changeit \
   -keystore /path/to/openam/security/keystores/webauthnTrustStore.jceks
   ```

   The command above imports a hypothetical trust chain from "Vendor A" into a secret store named `webauthnTrustStore.jceks`, located in the default AM path for keystores, `/path/to/openam/security/keystores`.

   If their keystore does not exist, the command creates it and sets the store password to `changeit`; otherwise it adds the specified certificate to the secret store.

3. Repeat the previous step until the `webauthnTrustStore.jceks` secret store contains all of the CA-issued certificate chains for the devices you want to verify.

4. Ensure that the password to access the new `webauthnTrustStore.jceks` secret store is available to your AM instance; for example, by encrypting the password and adding the result to a new file named `webauthnStorepass`, in `/path/to/openam/security/secrets/encrypted`.

   For more information, see "File System Secret Volumes Secret Stores" in the Security Guide.

5. In the AM console, go to the realm containing the web authentication registration tree that will attempt CA-level attestation, navigate to Authentication > Trees, and click your registration tree.
6. Select the WebAuthn Registration Node, and in the properties pane:

   a. Set the Preferred mode of attestation property to **DIRECT** or **INDIRECT**.

   b. Set the Trust Store alias property to a string that will identify both the name of the trust store, and will be the suffix of the secret ID used for mappings; for example, `webauthnTrustStore`.

   c. (Optional) If you want to act upon the attestation type achieved when registering a device; for example, using a script, then you should enable the Store data in transient state property.

      When this is enabled, the WebAuthn Registration Node stores the level of attestation achieved in a variable named `webauthnAttestationType`, in the transient state of the tree.

      **Tip**

      Use code similar to the following JavaScript to read the value of `webauthnAttestationType`:

      ```javascript
      var attestationLevel = transientState.get("webauthnAttestationType");
      ```

   d. Save your changes.

      For more information on the available properties, see "WebAuthn Registration Node".

7. Navigate back to the realm page, select Secret Stores, and then click Add Secret Store.

8. In Secret Store ID, enter the alias you specified in the registration node earlier; for example, `webauthnTrustStore`.

   Select the store type, specify the path to the store, and then click Create.
9. Set the Store password secret ID to the name of the file you created earlier with the encrypted value of the store password in; for example, `webauthnStorepass`.

Save your changes.


11. In Secret ID, select the ID that begins with `am.authentication.nodes.webauthn.truststore`, and has the alias you specified earlier as the suffix. For example, `am.authentication.nodes.webauthn.truststore.webauthnTrustStore`.

12. Enter the alias of the certificate chains you want to use for verification, and then click Add.

Repeat this step to add all the aliases of certificate chains you want to use for CA-level attestation:
13. Save your changes.

Your registration tree is now ready to verify the attestation data against the list of configured certificate chains.
Chapter 9
MFA: Push Authentication

You can use push notifications as part of the authentication process in AM.

To receive push notifications when authenticating, end users must register an Android or iOS device with AM. The registered device can then be used as an additional factor when authenticating to AM. AM can send the device a push notification, which can be accepted by the ForgeRock Authenticator app. In the app, the user can allow or deny the request that generated the push notification and return the response to AM.

Overview of Push Authentication

The following steps occur when AM receives an authentication request and is configured for multi-factor authentication using push notifications:

1. The user must provide credentials to enable AM to locate the user in the identity store and determine if they have a registered mobile device.

2. AM prompts the user to register a mobile device if they have not done so already. Registering a device associates metadata about the device essential for enabling push notifications with the user's profile in the identity store.

   For more information, see "Managing Devices for MFA".

3. Once the details of the registered device are obtained, AM creates a push message specific to the registered device. The message has a unique ID, which AM stores in anticipation of a response from the registered device.
A pending record using the same message ID is also written to the CTS store, providing redundancy should an individual server go offline during the authentication process.

4. AM sends the push message to the registered device.

AM uses cloud-based push notification services to deliver the messages to the devices. Depending on the registered device, AM uses either Apple Push Notification Services (APNS) or Google Cloud Messaging (GCM) to deliver the push notification.

AM begins to poll the CTS for an accepted response from the registered device.

5. The user responds to the notification on the registered device, which will open the ForgeRock Authenticator app. In the ForgeRock Authenticator app, the user approves the authentication request with either a swipe, or by using a fingerprint or face recognition on supported hardware.

For more information, see "Testing Push Authentication".

The app returns the response to the AM site.

6. AM verifies the message is from the correct registered phone and has not been tampered with, and marks the pending record as accepted if valid.

AM detects the accepted record and redirects the user to their profile page, completing the authentication.

The following table summarizes the tasks you need to perform to implement Push authentication in your environment:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure Authentication Tree or Chains</td>
<td>• &quot;Creating Trees for Push Authentication&quot;</td>
</tr>
<tr>
<td></td>
<td>• &quot;Creating Chains for Push Authentication&quot;</td>
</tr>
<tr>
<td>Depending on your environment, choose whether to configure Push authentication on trees or chains.</td>
<td></td>
</tr>
<tr>
<td>ForgeRock recommends that you implement authentication trees.</td>
<td></td>
</tr>
<tr>
<td>If you are planning to implement passwordless push authentication, see also &quot;Limitations When Using Passwordless Push Authentication&quot;.</td>
<td></td>
</tr>
<tr>
<td>Test Push Authentication</td>
<td>• &quot;Testing Push Authentication&quot;</td>
</tr>
<tr>
<td>After configuring AM, download the ForgeRock Authenticator app and test your configuration.</td>
<td></td>
</tr>
</tbody>
</table>

Creating Trees for Push Authentication

Push authentication uses the authentication trees to receive push notifications and to perform the actual authentication itself.
Authentication trees can be used for passwordless authentication using push notifications. When configured for passwordless authentication, the authentication flow asks the user to enter their user ID but not their password. A push notification is then sent to their registered device to complete the authentication by using the ForgeRock Authenticator app.

Before implementing passwordless push authentication, consider the "Limitations When Using Passwordless Push Authentication".

To Create a Tree for Push Authentication

The procedure assumes the following:

• Users will provide user IDs and passwords as the first step of multi-factor authentication.

• This procedure assumes users have registered using an authentication chain. At this time, authentication trees do not support registering devices. For more information, see in "To Create a Chain for Push Authentication".

• A push notification will be sent to the device as a second factor to complete authentication.

• The following services are configured:

  **ForgeRock Authenticator (Push) Service**
  Specifies the attribute in which to store information about the registered Push device, and whether to encrypt the data.

  For detailed information about the available properties, see "ForgeRock Authenticator (Push) Service" in the Reference.

  **Push Notification Service**
  Configures how AM sends push notifications to registered devices, including endpoints, and access credentials.

  For information on provisioning the credentials required by the Push Notification Service, see How To Configure Service Credentials (Push Auth, Docker) in Backstage in the ForgeRock Knowledge Base.

  For detailed information about the available properties, see "Push Notification Service" in the Reference.

To create a multi-factor authentication tree, perform the following steps:

1. Log in to the AM console as an AM administrator, for example amAdmin.

2. Select the realm that will contain the authentication tree.

3. Create the authentication tree as follows:
a. Select Authentication > Trees, and then click Create Tree.

The New Tree page appears.

b. Specify a name of your choosing, for example myPushAuthTree, and then click Create.

The authentication tree designer is displayed, with the Start entry point connected to the Failure exit point.

You can add nodes to the authentication tree by dragging the node from the Components panel on the left-hand side and dropping it into the designer area.

c. Add the following nodes to the authentication tree:

- Username Collector Node
- Password Collector Node
- Push Sender Node
- Push Result Verifier Node
- Polling Wait Node
- Success Node

d. Connect the nodes as demonstrated in the following figure:

![Authentication Tree Diagram]

 e. Save your changes.

4. Test your authentication tree as follows:

a. Logout of AM, and then navigate to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=myPushAuthTree#login

A login screen prompting you to enter your user ID and password appears.

b. Follow the procedure described in "Testing Push Authentication" to verify that you can use the ForgeRock Authenticator app to perform multi-factor authentication. If the authentication
To Create a Tree for Passwordless Authentication

The procedure assumes the following:

• Users will provide only their user IDs as the first step of multi-factor authentication.

• This procedure assumes users have registered using an authentication chain. At this time, authentication trees do not support registering devices. For more information, see "To Create a Chain for Push Authentication".

• A push notification will be sent to the device as a second factor to complete authentication, without the need to enter the user's password.

• The following services are configured:

  **ForgeRock Authenticator (Push) Service**

  Specifies the attribute in which to store information about the registered Push device, and whether to encrypt the data.

  For detailed information about the available properties, see "ForgeRock Authenticator (Push) Service" in the Reference.

  **Push Notification Service**

  Configures how AM sends push notifications to registered devices, including endpoints, and access credentials.

  For information on provisioning the credentials required by the Push Notification Service, see How To Configure Service Credentials (Push Auth, Docker) in Backstage in the ForgeRock Knowledge Base.

  For detailed information about the available properties, see "Push Notification Service" in the Reference.

To create a multi-factor authentication tree for passwordless authentication, perform the following steps:

1. Log in to the AM console as an AM administrator, for example amAdmin.
2. Select the realm that will contain the authentication tree.
3. Create the authentication tree as follows:
   a. Select Authentication > Trees, and then click Create Tree.

   The New Tree page appears.
b. Specify a name of your choosing, for example `myPasswordlessAuthTree`, and then click Create. The authentication tree designer is displayed, with the Start entry point connected to the Failure exit point.

You can add nodes to the authentication tree by dragging the node from the Components panel on the left-hand side and dropping it into the designer area.

c. Add the following nodes to the authentication tree:
   - Username Collector Node
   - Push Sender Node
   - Push Result Verifier Node
   - Polling Wait Node
   - Success Node

d. Connect the nodes as demonstrated in the following figure:

![Authentication Tree Diagram]

<table>
<thead>
<tr>
<th>Start</th>
<th>Username Collector</th>
<th>Push Sender</th>
<th>Push Result Verifier</th>
<th>Polling Wait</th>
<th>Success</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

You can see the connections between the nodes in the diagram.

e. Save your changes.

4. Test your authentication tree as follows:

a. Logout of AM, and then navigate to a URL similar to the following: `https://openam.example.com:8443/openam/XUI/?realm=/&service=myPasswordlessAuthTree/#login`

A login screen prompting you to enter your user ID appears.

b. Follow the procedure described in "Testing Push Authentication" to verify that you can use the ForgeRock Authenticator app to perform multi-factor authentication. If the authentication tree is correctly configured, authentication is successful and AM displays the user profile page, without having to enter a password.
Creating Chains for Push Authentication

Push authentication uses two separate authentication modules:

- A module to register a device to receive push notifications called *ForgeRock Authenticator (Push) Registration*.

- A module to perform the actual authentication itself, called *ForgeRock Authenticator (Push)*.

You can insert both modules into a single chain to register devices and then authenticate with push notifications. See "To Create a Chain for Push Authentication".

The ForgeRock Authenticator (Push) module can also be used for passwordless authentication using push notifications. If the module is placed at the start of a chain, it will ask the user to enter their user ID, but not their password. A push notification is then sent to their registered device to complete the authentication by using the ForgeRock Authenticator app.

Before implementing passwordless push authentication, consider the "Limitations When Using Passwordless Push Authentication".

**To Create a Chain for Push Authentication**

The procedure assumes the following:

- Users will provide user IDs and passwords as the first step of multi-factor authentication.

- If the user does not have a device registered to receive push notifications, they will be asked to register a device. After successfully registering a device for push, authentication will proceed to the next step.

- A push notification will be sent to the device as a second factor to complete authentication.

- The following services are configured:

  **ForgeRock Authenticator (Push) Service**

  Specifies the attribute in which to store information about the registered Push device, and whether to encrypt the data.

  For detailed information about the available properties, see "ForgeRock Authenticator (Push) Service" in the Reference.

  **Push Notification Service**

  Configures how AM sends push notifications to registered devices, including endpoints, and access credentials.

  For information on provisioning the credentials required by the Push Notification Service, see How To Configure Service Credentials (Push Auth, Docker) in Backstage in the ForgeRock Knowledge Base.
For detailed information about the available properties, see "Push Notification Service" in the Reference.

To create a multi-factor authentication chain that uses the ForgeRock Authenticator (Push) Registration and ForgeRock Authenticator (Push) modules, perform the following steps:

1. Log in to the AM console as an AM administrator, for example `amAdmin`.
2. Select the realm that will contain the authentication chain.
3. Create a ForgeRock Authenticator (Push) Registration authentication module as follows:
   a. Select Authentication > Modules, and then click Add Module.
      
      The New Module page appears.
   b. Fill in fields in the New Module page as follows:
      
      • Name: Specify a module name of your choosing, for example `push-reg`.
      • Type: Select ForgeRock Authenticator (Push) Registration.
   c. Click Create.
      
      A page that lets you configure the authentication module appears.
   d. Configure the module to meet your organization's requirements.
      
      For more information about the authentication module's configuration settings, see "ForgeRock Authenticator (Push) Registration Authentication Module".

4. Create a ForgeRock Authenticator (Push) authentication module as follows:
   a. Select Authentication > Modules, and then click Add Module.
      
      The New Module page appears.
   b. Fill in fields in the New Module page as follows:
      
      • Name: Specify a module name of your choosing, for example `push-authn`.
      • Type: Select ForgeRock Authenticator (Push).
   c. Click Create.
      
      A page that lets you configure the authentication module appears.
   d. Configure the module to meet your organization's requirements.
      
      For more information about the authentication module's configuration settings, see "ForgeRock Authenticator (Push) Authentication Module".
5. Create the authentication chain as follows:
   a. Select Authentication > Chains, and then click Add Chain.
      The Add Chain page appears.
   b. Specify a name of your choosing, for example `myPushAuthChain`, and then click Create.
      A page appears with the Edit Chain tab selected.
   c. Add the Data Store authentication module to the authentication chain as follows:
      i. Click Add a Module.
         The New Module dialog box appears.
      ii. Fill in the New Module dialog box, specifying the Data Store authentication module. For this example, specify the `Requisite` flag.
      iii. Click OK.
         The graphic showing your authentication chain now includes a Data Store authentication module.
   d. Add the ForgeRock Authenticator (Push) Registration authentication module to the authentication chain as follows:
      i. Click Add a Module.
         The New Module dialog box appears.
      ii. Fill in the New Module dialog box, specifying the ForgeRock Authenticator (Push) Registration authentication module that you just created. For this example, specify the `Requisite` flag.
      iii. Click OK.
         The graphic showing your authentication chain now includes a Data Store, and a ForgeRock Authenticator (Push) Registration authentication module.
   e. Add the ForgeRock Authenticator (Push) authentication module to the authentication chain as follows:
      i. Click Add a Module.
         The New Module dialog box appears.
      ii. Fill in the New Module dialog box, specifying the ForgeRock Authenticator (Push) authentication module that you created. For this example, specify the `Required` flag.
iii. Click OK.

The graphic showing your authentication chain now includes a Data Store, a ForgeRock Authenticator (Push) Registration, and a ForgeRock Authenticator (Push) authentication module.

f. Save your changes.

6. Test your authentication chain as follows:

a. Logout of AM, and then navigate to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=myPushAuthChain#login
A login screen prompting you to enter your user ID and password appears.

b. Follow the procedure described in "Testing Push Authentication" to verify that you can use the ForgeRock Authenticator app to perform multi-factor authentication. If the chain is correctly configured, authentication is successful and AM displays the user profile page.

**To Create a Chain for Push Registration and Passwordless Authentication**

The procedure assumes the following:

- Users will provide only their user IDs as the first step of multi-factor authentication.

- The user already has a device registered for receiving push notifications. For details of an authentication chain which can register a device for push notifications, see "To Create a Chain for Push Authentication".

- A push notification will be sent to the device as a second factor, to complete authentication without the need to enter a password.

- The following services are configured:

  **ForgeRock Authenticator (Push) Service**

  Specifies the attribute in which to store information about the registered Push device, and whether to encrypt the data.

  For detailed information about the available properties, see "ForgeRock Authenticator (Push) Service" in the Reference.

  **Push Notification Service**

  Configures how AM sends push notifications to registered devices, including endpoints, and access credentials.

  For information on provisioning the credentials required by the Push Notification Service, see How To Configure Service Credentials (Push Auth, Docker) in Backstage in the ForgeRock Knowledge Base.

  For detailed information about the available properties, see "Push Notification Service" in the Reference.

To create a multi-factor authentication chain that uses the ForgeRock Authenticator (Push) module for passwordless authentication, perform the following steps:

1. Log in to the AM console as an AM administrator, for example amAdmin.

2. Select the realm that will contain the authentication chain.

3. Create the authentication chain as follows:
a. Select Authentication > Chains, and then click Add Chain.

The Add Chain page appears.

b. Specify a name of your choosing, for example *myPasswordlessAuthChain*, and then click Create.

A page appears with the Edit Chain tab selected.

c. Add the ForgeRock Authenticator (Push) authentication module to the authentication chain as follows:

i. Click Add a Module.

The New Module dialog box appears.

ii. Fill in the New Module dialog box, specifying the ForgeRock Authenticator (Push) authentication module that you created. For this example, specify the *Requisite* flag.

iii. Click OK.

The graphic showing your authentication chain now includes a ForgeRock Authenticator (Push) authentication module.
d. Save your changes.

4. Test your authentication chain as follows:
   a. Logout of AM, and then navigate to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/#login/&service=myPasswordlessAuthChain

   A login screen prompting you to enter your user ID appears.

   b. Follow the procedure described in "Testing Push Authentication" to verify that you can use the ForgeRock Authenticator app to perform multi-factor authentication. If the chain is correctly configured, authentication is successful and AM displays the user profile page, without having to enter a password.
Testing Push Authentication

AM presents you with a page for entering only your user ID, or user ID and password. After you provide those credentials, AM verifies them. If your credentials are valid and the account has a device registered for push notifications, AM sends a push notification to the registered device.

Note

The device needs access to the Internet to receive push notifications, and the AM server must be able to receive responses from the device.

Receiving Push Notifications

On your registered device, you will receive a push notification from AM. Depending on the state of the phone and the ForgeRock Authenticator app, respond to the notification as follows:

• If the phone is locked, the notification may appear similar to the following:

Slide the notification across the screen, then unlock the phone. The ForgeRock Authenticator app will automatically open and display the push notification authentication screen.

• If the phone is not locked, and the ForgeRock Authenticator app is not open, the notification may appear similar to the following:
Tap the notification. The ForgeRock Authenticator app will automatically open and display the push notification authentication screen.

- If the phone is not locked, and the ForgeRock Authenticator app is open, the app will open the push notification authentication screen automatically.

**Approving Requests**

On the push notification authentication screen, approve the request using one of the following methods:

- Slide the switch with a checkmark on horizontally to the right.
• If the registered device supports Touch ID, and fingerprints have been provided, you can approve the request by using a registered fingerprint.
Tip

If the registered device supports face recognition and you have set up facial recognition, you can approve the request by glancing at your device.

AM will display the user's profile page.

Denying Requests

Deny the request by tapping the cancel icon in the top-right of the screen or, if Touch ID or face recognition are enabled, tap the Cancel button.

After a timeout has passed, AM will report that authentication has failed.
Limitations When Using Passwordless Push Authentication

When authenticating to a passwordless push authentication tree or chain, the user will be asked to enter their user ID, but not their password. A push notification is then sent to their registered device to complete the authentication by using the ForgeRock Authenticator app.

You should be aware of the following potential limitations before deciding to implement passwordless push authentication:

• Unsolicited push messages could be sent to a user's registered device by anyone who knew or was able to guess their user ID.

• If a malicious user attempted to authenticate by using push at the same time as a legitimate user, the legitimate user might unintentionally approve the malicious attempt. This is because push notifications only contain the username and issuer in the text, and it is not easy to determine which notification relates to which authentication attempt.

Consider using push notifications as part of a multi-factor authentication, and not on their own.

Note

If you do not approve or deny the request on the registered device, the AM Push Authentication page will timeout and the authentication will fail. The timeout can be configured in the ForgeRock Authenticator (Push) authentication module settings or in the Push Sender node.
Chapter 10
MFA: Open AuTHentication (OATH)

The ForgeRock Authenticator (OATH) module supports HMAC one-time password (HOTP) and time-based one-time password (TOTP) authentication as defined in the OATH standard protocols for HOTP (RFC 4226) and TOTP (RFC 6238). Both HOTP and TOTP authentication require an OATH-compliant device that can provide the password.

HOTP authentication generates the one-time password every time the user requests a new password on their device. The device tracks the number of times the user requests a new one-time password with a counter. The one-time password displays for a period of time you designate in the setup, so the user may be further in the counter on their device than on their account.

AM will resynchronize the counter when the user finally logs in. To accommodate this, you set the number of passwords a user can generate before their device cannot be resynchronized. For example, if you set the number of HOTP Window Size to 50 and someone presses the button 30 times on the user's device to generate a new password, the counter in AM will review the passwords until it reaches the one-time password entered by the user. If someone presses the button 51 times, you will need to reset the counter to match the number on the device's counter before the user can login to AM. HOTP authentication does not check earlier passwords, so if the user attempts to reset the counter on their device, they will not be able to login until you reset the counter in AM to match their device. For more information, see "Resetting Registered Devices by using REST".

TOTP authentication constantly generates a new one-time password based on a time interval you specify. The device tracks the last several passwords generated and the current password. The TOTP Time Steps setting configures the number of passwords tracked. The Last Login Time setting monitors the time when a user logs in to make sure that user is not logged in several times within the present time period. The TOTP Time-Step Interval should not be so long as to lock users out, with a recommended time of 30 seconds.

Differences Among Authentication Modules That Support HOTP

The ForgeRock Authenticator (OATH), OATH, and HOTP authentication modules let you configure authentication that prompts users to enter HMAC one-time passwords. It is important that administrators understand the differences among these authentication modules:

• The ForgeRock Authenticator (OATH) and OATH authentication modules accept one-time passwords generated by the end user's device, while the HOTP authentication module generates passwords and sends them to users by e-mail or SMS.
• All three of the authentication modules support HOTP passwords. The ForgeRock Authenticator (OATH) and OATH authentication modules also support TOTP passwords.

• The ForgeRock Authenticator (OATH) and OATH authentication modules require users to register their devices, and store the device registration details in the user profile. The HOTP authentication module requires the presence of mobile phone numbers and/or e-mail addresses in user profiles.

• The ForgeRock Authenticator (OATH) authentication module can encrypt stored device registration details.

Before deciding on an implementation strategy, assess your requirements against the following capabilities in AM:

### Comparing the ForgeRock Authenticator (OATH) to the HOTP Authentication Module

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Available With the ForgeRock Authenticator (OATH) Authentication Module?</th>
<th>Available With the HOTP Authentication Module?</th>
</tr>
</thead>
<tbody>
<tr>
<td>End users can authenticate using a HOTP password</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>AM can generate a HOTP password and send it to end users in a text message or an e-mail</td>
<td>✗</td>
<td>✓</td>
</tr>
<tr>
<td>End users can register a mobile phone with AM, and an authenticator app on the phone can generate a HOTP or TOTP password that AM accepts as proof of authentication</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>End users can authenticate with a TOTP password</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>End users can opt out of providing a one-time password</td>
<td>✓</td>
<td>✗</td>
</tr>
<tr>
<td>End users can authenticate using XUI</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

### Creating Chains for One-Time Password Authentication

This section covers one-time password authentication.

**To Create a Chain for One-Time Password Authentication**

The procedure assumes the following:

• Users will provide user IDs and passwords as the first step of multi-factor authentication.

• An existing Data Store authentication module will collect and verify user IDs and passwords.

• All authentication modules in the chain will use the Requisite flag setting. See "Authentication Modules and Chains" for details about authentication module flag settings.
• Users can opt out of one-time password authentication.

• The ForgeRock Authenticator (OATH) Service is configured.

This service specifies the attribute in which to store information about the registered OATH device, and whether to encrypt that information. It also specifies the attribute used to indicate if a user has opted out of one-time passwords.

For detailed information about the available properties, see "ForgeRock Authenticator (OATH) Service" in the Reference.

To create a multi-factor authentication chain that uses the ForgeRock Authenticator (OATH) module, perform the following steps:

1. Log in to the AM console as an AM administrator, for example amAdmin.

2. Select the realm that will contain the authentication chain.

3. You can allow users to opt out of using OATH-based one-time passwords as follows:
   a. Select Authentication > Settings > General.
   b. Make sure that the Two Factor Authentication Mandatory is not enabled.

   See General for details about this configuration setting.

For information about how letting users skip multi-factor authentication impacts the behavior of authentication chains, see "Letting Users Opt Out of One-Time Password Authentication (OATH)".

4. Create a ForgeRock Authenticator (OATH) authentication module as follows:
   a. Select Authentication > Modules, and then click Add Module.

   The New Module page appears.

   b. Fill in fields in the New Module page as follows:
      • Name: Specify a module name of your choosing.
      • Type: Select ForgeRock Authenticator (OATH).

   c. Click Create.

   A page that lets you configure the authentication module appears.

   d. Configure the ForgeRock Authenticator authentication module to meet your organization's requirements.

   For more information about the authentication module's configuration settings, see "ForgeRock Authenticator (OATH) Authentication Module".

5. Create the authentication chain as follows:
a. Select Authentication > Chains, and then click Add Chain.
   
   The Add Chain page appears.

b. Specify a name of your choosing, for example myOATHAuthChain, and then click Create.
   
   A page appears with the Edit Chain tab selected.

c. Click Add a Module. Fill in fields in the New Module dialog box as follows:
   
   • Select Module: Select the existing Data Store module to use in this chain.

   • Select Criteria: Select a flag setting for the module in the authentication chain. For this example, specify the Requisite flag.

   See "Authentication Modules and Chains" for information about authentication module flag settings.

d. Click OK.
   
   A graphic showing an authentication chain with a single Data Store module appears on the page.

e. Add the ForgeRock Authenticator (OATH) authentication module to the authentication chain as follows:
   
   i. Click Add a Module.

   The New Module dialog box appears.

   ii. Fill in the New Module dialog box, specifying the ForgeRock Authenticator (OATH) authentication module that you just created. For this example, specify the Requisite flag.

   iii. Click OK.

   The graphic showing your authentication chain now includes the Data Store and ForgeRock Authenticator (OATH) authentication module.
f. Save your changes.

6. Test your authentication chain as follows:

a. Log out of AM, and then navigate to a URL similar to the following: https://openam.example.com:8443/openam/XUI/?realm=/&service=myOATHAuthChain#login

A login screen prompting you to enter your user ID and password appears.

b. Follow the procedure described in "To Perform Authentication using a One-Time Password" to verify that you can use the ForgeRock Authenticator app to perform multi-factor
authentication. If the chain is correctly configured, authentication is successful and AM displays the user profile page.

**To Perform Authentication using a One-Time Password**

This example uses the authentication chain as created in "Creating Chains for One-Time Password Authentication".

Because the first module in the authentication chain is a Data Store module, AM presents you with a page for entering your user ID and password. After you provide those credentials, AM verifies them. If your credentials are valid, AM proceeds to the ForgeRock Authenticator (OATH) authentication module.

On the ForgeRock Authenticator (OATH) screen, follow these steps to complete one-time password authentication:

1. On your registered device, open the ForgeRock Authenticator app, and then tap the account matching the user ID you entered earlier. The registered authentication methods for that account are displayed:

   ![Registered Authenticator App](image)

2. In the One-time Password section, click the refresh icon. A one-time password is displayed:
3. On the ForgeRock Authenticator (OATH) page in AM, enter the one-time password that the authenticator app generated on your phone, and then click Submit:

![One-time password input screen]

AM will display the user's profile page.

**Letting Users Opt Out of One-Time Password Authentication (OATH)**

Letting users opt out of providing one-time passwords when they perform multi-factor authentication is an important implementation decision. The Two Factor Authentication Mandatory setting under Realms > Realm Name > Authentication > Settings > General configures whether users can opt out.

When the Two Factor Authentication Mandatory setting is enabled, users must provide a one-time password every time they authenticate to a chain that includes a ForgeRock Authenticator (OATH) authentication module. When the setting is disabled, the user can optionally skip one-time passwords.
By default, AM lets users opt out of providing one-time passwords. Users authenticating with one-time passwords for the first time are prompted with a screen that lets them opt out of providing one-time passwords.

With the Two Factor Authentication Mandatory setting enabled, the user experience differs from the default behavior. AM does not provide an option to skip multi-factor authentication during the initial attempt at multi-factor authentication:

When configuring an authentication chain that implements one-time passwords, you need to be aware that a user's decision to opt out affects the authentication process. When a user who has opted out of providing one-time passwords authenticates to a chain that includes a ForgeRock Authenticator (OATH) authentication module, that module always passes authentication.

Consider the example authentication chain in "Creating Chains for One-Time Password Authentication". The first authentication module is a Data Store module and the second authentication module is a ForgeRock Authenticator (OATH) module. Both authentication modules have the Requisite flag setting.

A user who has opted out of providing one-time passwords might experience the following sequence of events when authenticating to the chain:

1. The Data Store authentication module prompts the user to provide a user ID and password.
2. The user provides a valid user ID and password.
3. Data Store authentication passes, and authentication proceeds to the next module in the chain—the ForgeRock Authenticator (OATH) module.
4. The ForgeRock Authenticator (OATH) authentication module determines that the user has opted out of providing one-time passwords.
5. ForgeRock Authenticator (OATH) authentication passes. Because it is the last authentication module in the chain, AM considers authentication to have completed successfully.
Contrast the preceding sequence of events to the experience of a user who has not opted out of providing one-time passwords, or who is required to provide one-time passwords, while authenticating to the same chain:

1. The Data Store authentication module prompts the user to provide a user ID and password.
2. The user provides a valid user ID and password.
3. Data Store authentication passes, and authentication proceeds to the next module in the chain—the ForgeRock Authenticator (OATH) module.
4. The ForgeRock Authenticator (OATH) authentication module determines that the user has not opted out of providing one-time passwords, and prompts the user for a one-time password.
5. The user obtains a one-time password from the authenticator app on their mobile phone.
6. If the one-time password is valid, ForgeRock Authenticator (OATH) authentication passes. Because it is the last authentication module in the chain, AM considers authentication to have completed successfully. However, if the one-time password is not valid, ForgeRock Authenticator (OATH) authentication fails, and AM considers authentication to have failed.

Opting Out of One-Time Password Authentication (OATH)

Unless the AM administrator has made one-time password authentication mandatory, users can choose to opt out of using one-time passwords by clicking the Skip This Step button on the ForgeRock Authenticator (OATH) screen. ¹ This button appears:

- When users are prompted to register their mobile devices during their initial login from a new device.
- Every time users are prompted by the ForgeRock Authenticator (OATH) authentication module to enter one-time passwords.

Users who decide to opt out of using one-time passwords are not prompted to enter one-time passwords when authenticating to AM.

The decision to opt out of using one-time passwords in AM is revocable: users who have decided to opt out of using one-time passwords can reverse their decisions, so that one-time password authentication is once again required.

End users should follow these steps to opt out or opt in to using one-time passwords:

**To Opt out or Opt in to Using One-Time Passwords**

1. Log in to AM.

¹For information about making the usage of one-time passwords mandatory in AM, see “Letting Users Opt Out of One-Time Password Authentication (OATH)”.


2. Select Dashboard from the top navigation bar.

3. In the Authentication Devices section of the Dashboard page, click the context menu button for the chosen device, and then click Settings:

![Dashboard](image)

4. Enable or disable the multi-factor authentication option:

![OATH Device Default Settings](image)

5. Click Save.
Chapter 11
Managing Devices for MFA

Multi-factor authentication requires you to register a device, which is used as an additional factor when you log in to AM.

The following table summarizes different tasks related to devices used for multi-factor authentication:

<table>
<thead>
<tr>
<th>Task</th>
<th>Resources</th>
</tr>
</thead>
</table>
| Learn About the ForgeRock Authenticator | • "The ForgeRock Authenticator App"
| Download the ForgeRock Authenticator app, which supports push authentication notifications and one-time passwords, and register it in AM. |
| Recovering User Accounts    | • "Recovering After Replacing a Lost Device"
| Learn how to recover a user account when the user has lost their registered device, or when their device has become out of sync with AM. |
| Reset Registered Devices    | • "ReSETTING Registered Devices by using REST" |
| In some scenarios, for example, when users are not able to access their recovery codes, you may need to reset their registered devices to allow them to register again. |

The ForgeRock Authenticator App

The ForgeRock Authenticator app supports push authentication notifications and one-time passwords.

Download and install the ForgeRock Authenticator app on your phone, so that you can perform multi-factor authentication. The app is available for both Android and iOS devices, and is free to download.

• Download: Google Play  • Download: App Store
Tip

For access to the source code for sample mobile applications, see How do I access and build the sample code provided for AM/OpenAM (All versions)? in the ForgeRock Knowledge Base.

Registering the ForgeRock Authenticator for Multi-Factor Authentication

Registering the ForgeRock Authenticator app enables it to be used as an additional factor when logging in to AM.

The ForgeRock Authenticator app supports registration of multiple accounts and multiple different authentication methods in each account, such as push notifications and one-time passwords.

For information on registering Web Authentication (WebAuthn) devices with AM, see "Creating Trees for Web Authentication (WebAuthn)".

ForgeRock Authenticator registration only needs to be completed the first time an authentication method is used with an identity provider. Use of a different authentication method may require that registration with the identity provider is repeated for that additional method.

The ForgeRock Authenticator needs access to the internet to register to receive push notifications. Registering for one-time password authentication does not require a connection to the internet.

To Register the ForgeRock Authenticator for Multi-Factor Authentication

1. When visiting a protected resource without having any registered devices for multi-factor authentication, AM requires that you register a device.

To register your mobile phone with AM, click Register Device. A screen with a QR code appears:
2. Start the ForgeRock Authenticator app on the device to register, and then click the plus icon:

   The screen on the device changes to an interface similar to your camera app.

3. Point the camera at the QR code on the AM page and the ForgeRock Authenticator app will acquire the QR code and read the data encoded within.

   If you are logging in to AM on the registered device and cannot scan the screen, click the button labelled On a mobile device?. The ForgeRock Authenticator app will request permission to launch. If allowed, the information required to register the device will be transferred to the ForgeRock Authenticator app directly, without the need to scan the QR code.
4. Once registered, the app displays the registered accounts and the authentication methods they support, for example one-time passwords (a timer icon) or push notifications (a bell icon):

5. When registering a device, you MUST make a copy of the recovery codes associated with that device.

   Depending on the device type you registered, perform one of the following steps:
   
   - If you registered an OATH device:
     a. Click the Login Using Verification Code button.
        
        You will be asked to enter a verification code.
     
     b. In the ForgeRock Authenticator app, click the newly registered account, and then click the Refresh button to generate a new one-time password.
c. Enter the one-time password into the web page, and then click Submit.

d. On the recovery codes page, make a copy of the displayed recovery codes and store them safely. The codes will never be displayed again.

When you have safely stored the recovery codes for your newly registered OATH device, click the Continue button.

• If you registered a push device:
  • On the recovery codes page, make a copy of the displayed recovery codes and store them safely. The codes will never be displayed again.
When you have safely stored the recovery codes for your newly registered push device, click the Continue button.

Your device is now registered. You will able to use it to perform multi-factor authentication.

Recovering After Replacing a Lost Device

If you register a device with AM and then lose it, you must authenticate to AM using a recovery code, delete the lost device, and then register the new device. Perform the following steps:

To Register a New Device After Losing a Registered Device

1. Log in to AM. If push authentication is enabled, enter your user ID, click Log In, and then click Use Emergency Code. If one-time passwords are enabled, when prompted to enter a verification code, instead enter one of your recovery codes.

   Because recovery codes are valid for a single use only, make a note to yourself not to attempt to reuse this code.
If you did not save the recovery codes for the lost device, contact your administrator to remove the registered device from your AM user profile.

2. Select Dashboard from the top-level menu.

3. Locate the entry for your phone in the Authentication Devices section, click the context menu button, and then click Delete.

4. If you have not already done so, install the ForgeRock Authenticator app on your new phone. See "The ForgeRock Authenticator App".

5. Register your new device. See "Registering the ForgeRock Authenticator for Multi-Factor Authentication".

Users who do not save recovery codes or who run out of recovery codes and cannot authenticate to AM without a verification code require administrative support to reset their device profiles. See "Resetting Registered Devices by using REST" for more information.

Recovering After a Device Becomes Out of Sync

If you repeatedly enter valid one-time passwords that appear to be valid passwords, but AM rejects the passwords as unauthorized, it is likely that your device has become out of sync with AM.

When a registered device becomes out of sync with AM, you must authenticate to AM using a recovery code, delete your device, and then re-register your device. You can do so by performing the steps in "To Register a New Device After Losing a Registered Device".

Users who do not save recovery codes or who run out of recovery codes and cannot authenticate to AM without a verification code require administrative support to reset their device profiles. See "Resetting Registered Devices by using REST" for more information.

Resetting Registered Devices by using REST

As described in "Recovering After Replacing a Lost Device", a user who has lost a mobile phone registered with AM can register a replacement device by authenticating using a recovery code, deleting their existing device, and then re-registering a new device.

Additional support is required for users who lose mobile phones but did not save their recovery codes when they initially registered the phone, and for users who have used up all their recovery codes.

AM provides a REST API to reset a device profile by deleting information about a user's registered device. Either the user or an administrator can call the REST API to reset a device profile. Device profile reset can be implemented as follows:

- Administrators provide authenticated users with a self-service page that calls the REST API to let the users reset their own device profiles.
Administrators can call the REST API themselves to reset users' device profiles.

Administrators can call the REST API themselves to reset a device when the HOTP counter exceeds the HOTP threshold window and requires a reset.

**Note**
The reset action deletes the OATH device profile, which by default has a limit of one profile per device, and sets the Select to Enable Skip option to its default value of Not Set.

**Reset OATH Devices**

To reset a user's OATH device profile, perform an HTTP POST to the `/users/user/devices/2fa/oath?_action=reset` endpoint.

When making a REST API call, specify the realm in the path component of the endpoint. You must specify the entire hierarchy of the realm, starting at the Top Level Realm. Prefix each realm in the hierarchy with the `realms/` keyword. For example `/realms/root/realms/customers/realms/europe`.

The following example resets the OATH devices of a user named `myUser` in a subrealm of the Top Level Realm called `mySubrealm`:

```bash
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "Accept-API-Version: resource=1.0" \
--header "iplanetDirectoryPro: AQIC5w...2NzEz*" \
--data '{}' \
{
    "result":true
}
```

**Reset Push Devices**

To reset push devices over REST, perform an HTTP POST to the `/users/user/devices/push?_action=reset` endpoint as follows:

```bash
$ curl \
--request POST \
--header "Content-Type: application/json" \
--header "Accept-API-Version: resource=1.0" \
--header "iplanetDirectoryPro: AQIC5w...2NzEz*" \
--data '{}' \
{
    "result":true
}
```
Chapter 12
Reference

This reference section covers settings and the scripting API relating to authentication in AM. For global services and global authentication reference, see Reference.

• "Core Authentication Attributes"
• "Supported Callbacks"
• "Authenticate Endpoint Parameters"
• "Authentication Nodes Configuration Reference"
• "Scripted Decision Node API Functionality"
• "Authentication Module Properties"
• "Authentication Modules Configuration Reference"
• "Scripted Module API Functionality"

Core Authentication Attributes

Every AM realm has a set of authentication properties that applies to all authentication performed to that realm. The settings are referred to as core authentication attributes.

To configure core authentication attributes for an entire AM deployment, navigate to Configure > Authentication in the AM console, and then click Core Attributes.

To override the global core authentication configuration in a realm, navigate to Realms > Realm Name > Authentication > Settings in the AM console. Note that when you configure core authentication attributes in a realm, the Global Attributes tab does not appear.

amster service name: Authentication

ssoadm service name: iPlanetAMAAuthService

+ Global Attributes

The following properties are available under the Global Attributes tab:
Pluggable Authentication Module Classes

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

For more information about custom authentication modules, see "Creating a Custom Authentication Module".

amster attribute: authenticators

ssoadm attribute: iplanet-am-auth-authenticators

LDAP Connection Pool Size

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

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

This attribute is for LDAP and Membership authentication modules only.

amster attribute: ldapConnectionPoolSize

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

Default LDAP Connection Pool Size

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

Format is `minimum:maximum`.

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

This attribute is for LDAP and Membership authentication modules only.

amster attribute: ldapConnectionPoolDefaultSize

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

Remote Auth Security

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

amster attribute: remoteAuthSecurityEnabled

ssoadm attribute: sunRemoteAuthSecurityEnabled
Keep Post Process Objects for Logout Processing

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

Enabling this setting increases the memory usage of AM.

amster attribute: keepPostProcessInstances
ssoadm attribute: sunAMAuthKeepPostProcessInstances

+ Core

The following properties are available under the Core tab:

Administrator Authentication Configuration

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

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

Organization Authentication Configuration

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

amster attribute: orgConfig
ssoadm attribute: iplanet-am-auth-org-config

+ User Profile

The following properties are available under the User Profile tab:

User Profile

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

true. Dynamic.

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

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

ignore. Ignored.

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

**Warning**

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

false. Required.

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

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

User Profile Dynamic Creation Default Roles

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

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

This functionality is deprecated in the Release Notes.

**amster** attribute: defaultRole

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

Alias Search Attribute Name

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

**amster** attribute: aliasAttributeName

**ssoadm** attribute: iplanet-am-auth-alias-attr-name
Note

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

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

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

---

**Account Lockout**

The following properties are available under the Account Lockout tab:

**Login Failure Lockout Mode**

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

**amster** attribute: `loginFailureLockoutMode`

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

**Login Failure Lockout Count**

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

**amster** attribute: `loginFailureCount`

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

**Login Failure Lockout Interval**

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

Specifies one or more email addresses to which notification is sent if a user lockout occurs. Separate multiple addresses with spaces, and append `|locale|charset` to addresses for recipients in non-English locales.

amster attribute: `lockoutEmailAddress`

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

Warn User After N Failures

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

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

Login Failure Lockout Duration

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

amster attribute: `lockoutDuration`

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

Lockout Duration Multiplier

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

amster attribute: `lockoutDurationMultiplier`

ssoadm attribute: `sunLockoutDurationMultiplier`

Lockout Attribute Name

Defines the LDAP attribute used for physical lockout. The default attribute is `inetuserstatus`, although the field in the AM console is empty. The Lockout Attribute Value field must also contain an appropriate value.
amster attribute: lockoutAttributeName
ssoadm attribute: iplanet-am-auth-lockout-attribute-name

Lockout Attribute Value

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

amster attribute: lockoutAttributeValue
ssoadm attribute: iplanet-am-auth-lockout-attribute-value

Invalid Attempts Data Attribute Name

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

amster attribute: invalidAttemptsDataAttributeName
ssoadm attribute: sunAMAuthInvalidAttemptsDataAttrName

Store Invalid Attempts in Data Store

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

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

amster attribute: storeInvalidAttemptsInDataStore
ssoadm attribute: sunStoreInvalidAttemptsInDS

+ General

The following properties are available under the General tab:

Default Authentication Locale

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

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

Identity Types

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

Agent

Searches for identities under your agents.

agentgroup

Searches for identities according to your established agent group.

agentonly

Searches for identities only under your agents.

Group

Searches for identities according to your established groups.

User

Searches for identities according to your users.

Default: Agent and User.

amster attribute: identityType

ssoadm attribute: sunAMIdentityType

Pluggable User Status Event Classes

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

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

amster attribute: userStatusCallbackPlugins

ssoadm attribute: sunAMUserStatusCallbackPlugins

Use Client-Based Sessions

When enabled, AM assigns client-based sessions to users authenticating to this realm. Otherwise, AM users authenticating to this realm are assigned CTS-based sessions.
For more information about sessions, see "Introducing Sessions" in the Sessions Guide.

**amster attribute:** statelessSessionsEnabled

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

### Two Factor Authentication Mandatory

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

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

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

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

**Note**

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

**amster attribute:** twoFactorRequired

**ssoadm attribute:** forgerockTwoFactorAuthMandatory

### External Login Page URL

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

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

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

**amster attribute:** externalLoginPageUrl
**ssoadm attribute:** `externalLoginPageUrl`

**Default Authentication Level**

Specifies the default authentication level for authentication modules.

- **amster attribute:** `defaultAuthLevel`
- **ssoadm attribute:** `iplanet-am-auth-default-auth-level`

**Trees**

The following properties are available under the Trees tab:

**Authentication session state management scheme**

Specifies the location where AM stores authentication sessions.

Possible values are:

- **CTS.** AM stores authentication sessions in the CTS token store.
- **JWT.** AM sends the authentication session to the client as a JWT.
- **In-Memory.** AM stores authentication sessions in its memory.

For more information on authentication session storage locations, and the requirements for each, see "Introducing Sessions" in the Sessions Guide.

Default: **JWT** (new installations), **In-Memory** (after upgrade)

- **amster attribute:** `authenticationSessionsStateManagement`
- **ssoadm attribute:** `openam-auth-authentication-sessions-state-management-scheme`

**Max duration (minutes)**

Specifies the maximum allowed duration of an authentication session, including any time spent in the suspended state, in minutes.

Values from 1 to 2147483647 are allowed.

Default: 5

- **amster attribute:** `authenticationSessionsMaxDuration`
- **ssoadm attribute:** `openam-auth-authentication-sessions-max-duration`

**Suspended authentication duration (minutes)**

Specifies the length of time an authentication session can be suspended, in minutes.
Suspending an authentication session allows time for out-of-band authentication methods, such as responding to emailed codes or performing an action on an additional device. The value must be less than or equal to the total time allowed for an authentication session, specified in the `Max duration (minutes)` property.

Values from 1 to 2147483647 are allowed.

Default: 5

**ssoadm** attribute: `suspendedAuthenticationTimeout`

**Enable whitelisting**

When enabled, AM whitelists authentication sessions to protect them against replay attacks.

Default: Disabled

**amster** attribute: `authenticationSessionsWhitelist`

**ssoadm** attribute: `openam-auth-authentication-sessions-whitelist`

+ Security

The following properties are available under the Security tab:

**Module Based Authentication**

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

ForgeRock recommends disabling module-based authentication in production environments.

**amster** attribute: `moduleBasedAuthEnabled`

**ssoadm** attribute: `sunEnableModuleBasedAuth`

**Persistent Cookie Encryption Certificate Alias**

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

Default: test

**amster** attribute: `keyAlias`

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

**Zero Page Login**

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

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

AM always allows HTTP POST requests for zero page login.

Default: false (disabled)

amster attribute: zeroPageLoginEnabled

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

Zero Page Login Referer Whitelist

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

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

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

amster attribute: zeroPageLoginReferrerWhiteList

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

Zero Page Login Allowed Without Referer?

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

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

amster attribute: zeroPageLoginAllowedWithoutReferrer

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

Organization Authentication Signing Secret

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

When modifying this value, ensure the new shared secret is Base-64 encoded and at least 128 bits in length.
amster attribute: sharedSecret
ssoadm attribute: iplanet-am-auth-hmac-signing-shared-secret

+ Post Authentication Processing

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

**Default Success Login URL**

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

amster attribute: loginSuccessUrl
ssoadm attribute: iplanet-am-auth-login-success-url

**Default Failure Login URL**

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

amster attribute: loginFailureUrl
ssoadm attribute: iplanet-am-auth-login-failure-url

**Authentication Post Processing Classes**

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

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

For information on creating post-authentication plugins, see "Creating Post-Authentication Plugins for Chains".

amster attribute: loginPostProcessClass
ssoadm attribute: iplanet-am-auth-post-login-process-class

**Generate UserID Mode**

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

**amster** attribute: `usernameGeneratorEnabled`

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

### Pluggable User Name Generator Class

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

**amster** attribute: `usernameGeneratorClass`

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

### User Attribute Mapping to Session Attribute

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

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

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

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

**amster** attribute: `userAttributeSessionMapping`

**ssoadm** attribute: `sunAMUserAttributesSessionMapping`

---

### Supported Callbacks

The following types of callbacks are available:
Interactive Callbacks

AM returns the following callbacks to request information from the user:

ChoiceCallback

Used to display a list of choices and retrieve the selected choice. To indicate that the user selected the first choice, return a value of 0 to AM. For the second choice, return a value of 1, and so forth.

+ Example

```json
"callbacks": [
  {
    "type": "ChoiceCallback",
    "output": [
      {
        "name": "prompt",
        "value": "Choose one"
      },
      {
        "name": "choices",
        "value": [
          "Choice A",
          "Choice B",
          "Choice C"
        ]
      },
      {
        "name": "defaultChoice",
        "value": 2
      }
    ],
    "input": [
      {
        "name": "IDToken1",
        "value": 0
      }
    ]
  }
]
```

Class to import: `javax.security.auth.callback.ChoiceCallback`
ConfirmationCallback

Used to ask for a boolean-style confirmation, such as yes/no or true/false, and retrieve the response. Also can present a "Cancel" option. To indicate that the user selected the first choice, return a value of 0 to AM. For the second choice, return a value of 1, and so forth.

+ Example

```
"callbacks": [
    {
        "type": "ConfirmationCallback",
        "output": [
            {
                "name": "prompt",
                "value": ""
            },
            {
                "name": "messageType",
                "value": 0
            },
            {
                "name": "options",
                "value": [
                    "Submit",
                    "Start Over",
                    "Cancel"
                ]
            },
            {
                "name": "optionType",
                "value": -1
            },
            {
                "name": "defaultOption",
                "value": 1
            }
        ],
        "input": [
            {
                "name": "IDToken2",
                "value": 0
            }
        ]
    }
]
```

Class to import: `javax.security.auth.callback.ConfirmationCallback`

DeviceProfileCallback

Used to request information about the device being used to authenticate.

**Important**

The AM XUI user interface does not support this callback.
Support for this callback is provided by:
• The ForgeRock SDKs.
• The Login UI component of the Platform UI.

The callback may request metadata and/or location information about the device by setting the relevant value to true in the JSON:

+ **Example**

```
"callbacks": [
    
    { 
        "type": "DeviceProfileCallback", 
        "output": [ 
            
            { 
                "name": "metadata", 
                "value": true 
            },
            
            { 
                "name": "location", 
                "value": true 
            },
            
            { 
                "name": "message", 
                "value": "Collecting....." 
            } 
        ],
    
        "input": [ 
            
            { 
                "name": "IDToken1", 
                "value": "" 
            }
        ] 
    } 
]
```

The callback also contains the message entry, with optional text to display to the user while collecting the information.

The ForgeRock SDKs gather and return the requested information in a JSON object, as well as the following elements:

**identifier**

A unique identifier string that can be used to later match the device.

**alias**

A friendly name for the device, often derived from the make and model.

The response you should return in the callback should include information resembling the following:
+ Example Callback Response

```json
{
  "identifier": "aec3fe784...o3Xjiizy9b9=",
  "alias": "Pixel 3 XL",
  "metadata": {
    "platform": {
      "platform": "Android",
      "version": 28,
      "device": "generic_x86_arm",
      "deviceName": "AOSP on IA Emulator",
      "model": "AOSP on IA Emulator",
      "brand": "google",
      "locale": "en US",
      "timeZone": "America/Vancouver",
      "jailBreakScore": 1
    },
    "hardware": {
      "hardware": "ranchu",
      "manufacturer": "Google",
      "storage": 774,
      "memory": 1494,
      "cpu": 4,
      "display": {
        "width": 1440,
        "height": 2621,
        "orientation": 1
      },
      "camera": {
        "numberOfCameras": 2
      }
    },
    "browser": {
      "agent": "Dalvik/2.1.0 (Linux; U; Android 9; AOSP on IA Emulator Build/PSR1.180720.117)"
    },
    "bluetooth": {
      "supported": false
    },
    "network": {
      "connected": true
    },
    "telephony": {
      "networkCountryIso": "us",
      "carrierName": "Android"
    },
    "location": {
      "latitude": 51.431534,
      "Longitude": -121.522353
    }
  }
}
```

The JSON should be escaped and returned in the `input/IDToken1` property of the response.
As with all interactive callbacks, you should also return the authId value. See "Returning Callback Information to AM".

**NameCallback**

Used to retrieve a data string which can be entered by the user. Usually used for collecting user names.

+ **Example**

```
"callbacks": [
  {
    "type": "NameCallback",
    "output": [
      {
        "name": "prompt",
        "value": "User Name"
      }
    ],
    "input": [
      {
        "name": "IDToken1",
        "value": ""
      }
    ]
  }
]
```

Class to import: `javax.security.auth.callback.NameCallback`

**PasswordCallback**

Used to retrieve a password value.

+ **Example**
"callbacks": [
    {
        "type": "PasswordCallback",
        "output": [
            {
                "name": "prompt",
                "value": "Password"
            }
        ],
        "input": [
            {
                "name": "IDToken1",
                "value": ""
            }
        ]
    }
]

Class to import: `javax.security.auth.callback.PasswordCallback`

TextInputCallback

Used to retrieve text input from the end user.

+ Example

```
"callbacks": [
    {
        "type": "TextInputCallback",
        "output": [
            {
                "name": "prompt",
                "value": "User Name"
            }
        ],
        "input": [
            {
                "name": "IDToken1",
                "value": ""
            }
        ]
    }
]
```

Class to import: `javax.security.auth.callback.TextInputCallback`

Read-only Callbacks

AM uses the following callbacks to return information to the client or to show information to the user:
HiddenValueCallback

Used to return form values that are not visually rendered to the end user.

+ Example

```
"callbacks": [
    {
      "type": "HiddenValueCallback",
      "output": [ 
        {
          "name": "value",
          "value": "6186c911-b3be-4dbc-8192-bdf251392072"
        },
        {
          "name": "id",
          "value": "jwt"
        }
      ],
      "input": [ 
        {
          "name": "IDToken1",
          "value": "jwt"
        }
      ]
    }
]
```

Class to import: `com.sun.identity.authentication.callbacks.HiddenValueCallback`

MetadataCallback

Used to inject key-value meta data into the authentication process. For example:

+ Example

```
"callbacks": [
    {
      "type": "MetadataCallback",
      "output": [ 
        {
          "name": "data",
          "value": {
            "myParameter": "MyValue"
          }
        }
      ]
    }
]
```

Class to import: `com.sun.identity.authentication.spi.MetadataCallback`
PollingWaitCallback

Tells the user the amount of time to wait before responding to the callback.

+ Example

```json
"callbacks": [
    {
        "type":"PollingWaitCallback",
        "output": [
            {
                "name":"waitTime",
                "value":"8000"
            },
            {
                "name":"message",
                "value":"Waiting for response..."
            }
        ]
    }
]
```

Class to import: `org.forgerock.openam.authentication.callbacks.PollingWaitCallback`

RedirectCallback

Used to redirect the user's browser or user-agent.

+ Example

```json
"callbacks": [
    {
        "type":"RedirectCallback",
        "output": [
            {
                "name":"redirectUrl",
                "value":"https://accounts.google.com/o/oauth2/v2/auth?nonce..."
            },
            {
                "name":"redirectMethod",
                "value":"GET"
            },
            {
                "name":"trackingCookie",
                "value":true
            }
        ]
    }
]
```

Class to import: `com.sun.identity.authentication.spi.RedirectCallback`
SuspensionTextOutputCallback

Used to display a message to the end user after their authentication tree is suspended.

Example

```
"callbacks": [
  {
    "type": "SuspensionTextOutputCallback",
    "output": [
      {
        "name": "message",
        "value": "An email has been sent to your inbox."
      },
      {
        "name": "messageType",
        "value": "0"
      }
    ]
  }
]
```

Class to import: `org.forgerock.openam.auth.node.api.SuspensionTextOutputCallback`

TextOutputCallback

Used to display a message to the end user.

Example

```
"callbacks": [
  {
    "type": "TextOutputCallback",
    "output": [
      {
        "name": "message",
        "value": "Default message"
      },
      {
        "name": "messageType",
        "value": "0"
      }
    ]
  }
]
```

Class to import: `javax.security.auth.callback.TextOutputCallback`

Backchannel Callbacks

AM uses backchannel callbacks when it needs to recover additional information from the user's request. For example, when it requires a particular header or a certificate.
HttpCallback

Used to access user credentials sent in the Authorization header. For example:

Authorization: Basic bXlDbGllbnQ6Zm9yZ2Vyb2Nr

Class to import: com.sun.identity.authentication.spi.HttpCallback

LanguageCallback

Used to retrieve the locale for localizing text presented to the end user. The locale is sent in the request as a header.

Class to import: javax.security.auth.callback.LanguageCallback

ScriptTextOutputCallback

Used to insert a script into the page presented to the end user. The script can, for example, collect data about the user's environment.

Class to import: com.sun.identity.authentication.callbacks.ScriptTextOutputCallback

X509CertificateCallback

Used to retrieve the content of an x.509 certificate, for example, from a header.

Class to import: com.sun.identity.authentication.spi.X509CertificateCallback

Authenticate Endpoint Parameters

To authenticate to AM using REST, make an HTTP POST request to the json/authenticate endpoint. You must specify the entire hierarchy of the realm, starting at the Top Level Realm. Prefix each realm in the hierarchy with the realms/ keyword. For example, /realms/root/realms/customers/realms/europe.

The following list describes the json/authenticate endpoint supported parameters:

authIndexType

Specifies the type of authentication the user will perform. Always use in conjunction with the authIndexValue parameter to provide additional information about the way the user is authenticating.

If not specified, AM authenticates the user against the default authentication service configured for the realm.

The authIndexType parameter supports the following types:

• composite_advice

  Specifies that the value of the authIndexValue parameter is a URL-encoded composite advice string.
Use `composite_advice` when you want to give AM hints of which authentication services to use when logging in a user. For example, use an authentication service that provides an authentication level of 10 or higher:

```
$ curl -X GET \
--header "Content-Type: application/json" \
--header 'Accept-API-Version: resource=2.0, protocol=1.0' \
--data-urlencode 'authIndexType=composite_advice' \
--data-urlencode 'authIndexValue=<Advices>\n<AttributeValuePair>\n<Attribute name="AuthLevelConditionAdvice"/>\n<Value>10</Value>\n</AttributeValuePair>\n</Advices>' \
'https://openam.example.com:8443/openam/json/realms/root/authenticate'
```

Note that the previous `curl` command URL-encodes the XML values, and the `-G` parameter appends them as query string parameters to the URL.

Possible options for advices are:

- **TransactionConditionAdvice.** Requires the unique ID of a transaction token. For example:

  ```
  <Advices>
  <AttributeValuePair>
    <Attribute name="TransactionConditionAdvice"/>\n    <Value>9dae2c80-fe7a-4a36-b57b-4fb1271b8687</Value>
  </AttributeValuePair>
  </Advices>
  
  For more information, see "Transactional Authorization" in the Authorization Guide.
  
  - **AuthenticateToServiceConditionAdvice.** Requires the name of an authentication chain or tree. For example:

    ```
    <Advices>
    <AttributeValuePair>
      <Attribute name="AuthenticateToServiceConditionAdvice"/>\n      <Value>myExampleTree</Value>
    </AttributeValuePair>
    </Advices>
    
    - **AuthSchemeConditionAdvice.** Requires the name of an authentication module. For example:

      ```
      <Advices>
      <AttributeValuePair>
        <Attribute name="AuthSchemeConditionAdvice"/>\n        <Value>DataStoreModule</Value>
      </AttributeValuePair>
      </Advices>
      
      - **AuthenticateToRealmConditionAdvice.** Requires the name of a realm. For example:
• **AuthLevelConditionAdvice.** Requires an authentication level. For example:

```xml
<Advices>
  <AttributeValuePair>
    <Attribute name="AuthLevelConditionAdvice"/>
    <Value>10</Value>
  </AttributeValuePair>
</Advices>
```

• **AuthenticateToTreeConditionAdvice.** Requires the name of an authentication tree. For example:

```xml
<Advices>
  <AttributeValuePair>
    <Attribute name="AuthenticateToTreeConditionAdvice"/>
    <Value>PersistentCookieTree</Value>
  </AttributeValuePair>
</Advices>
```

You can specify multiple advice conditions and combine them. For example:

```xml
<Advices>
  <AttributeValuePair>
    <Attribute name="AuthenticateToServiceConditionAdvice"/>
    <Value>ldapService</Value>
  </AttributeValuePair>
  <AttributeValuePair>
    <Attribute name="AuthenticateToServiceConditionAdvice"/>
    <Value>Example</Value>
  </AttributeValuePair>
  <AttributeValuePair>
    <Attribute name="AuthLevelConditionAdvice"/>
    <Value>10</Value>
  </AttributeValuePair>
</Advices>
```

• **level**

Specifies that the value of the `authIndexValue` parameter is the minimum authentication level an authentication service must satisfy to log in the user.

For example, to log into AM using an authentication service that provides a minimum authentication level of 10, you could use the following:

```
$ curl \
  --request POST \
  --header 'Accept-API-Version: resource=2.0, protocol=1.0' \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate?authIndexType=level&authIndexValue=10'
```
• **module**

  Specifies that the value of the `authIndexValue` parameter is the name of the authentication module AM must use to log in the user.

  For example, to log into AM using the built-in **DataStore** authentication module, you could use the following:

  ```bash
  $ curl \
  --request POST \
  --header 'Accept-API-Version: resource=2.0, protocol=1.0' \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate?authIndexType=module&authIndexValue=DataStore'
  ```

  You should disable module-based authentication for security reasons. For more information, see "Securing Realms" in the Security Guide

• **resource**

  Specifies that the value of the `authIndexValue` parameter is a URL protected by an AM policy.

  For example, to log into AM using a policy matching the `http://www.example.com` resource, you could use the following:

  ```bash
  $ curl \
  --request POST \
  --header 'Accept-API-Version: resource=2.0, protocol=1.0' \
  ```

  Note that the resource must be URL-encoded. Authentication will fail if no policy matches the resource.

• **service**

  Specifies that the value of the `authIndexValue` parameter is the name of an authentication tree or authentication chain AM must use to log in the user.

  For example, to log in to AM using the built-in **ldapService** authentication chain, you could use the following:

  ```bash
  $ curl \
  --request POST \
  --header 'Accept-API-Version: resource=2.0, protocol=1.0' \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate?authIndexType=service&authIndexValue=ldapService'
  ```

• **user**

  Specifies that the value of the `authIndexValue` parameter is a valid user ID. AM will then authenticate the user against the chain configured in the User Authentication Configuration field of that user's profile.
For example, for the user `demo` to log into AM using the chain specified in their user profile, you could use the following:

```bash
$ curl \
  --request POST \
  --header 'Accept-API-Version: resource=2.0, protocol=1.0' \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate?
  authIndexType=user&authIndexValue=demo'
```

Authentication will fail if the User Authentication Configuration field is empty for the user.

If several authentication services that satisfy the authentication requirements are available, AM presents them as a choice callback to the user. Return the required callbacks to AM to authenticate.

Required: No.

**authIndexValue**

Specifies the value of the `authIndexType` parameter.

Required: Yes, when using the `authIndexType` parameter.

**noSession**

When set to `true`, specifies that AM should not return a session when authenticating a user. For example:

```bash
$ curl \
  --request POST \
  --header "Content-Type: application/json" \
  --header "Accept-API-Version: resource=2.0, protocol=1.0" \
  --header "X-OpenAM-Username: demo" \
  --header "X-OpenAM-Password: Ch4ng31t" \
  'https://openam.example.com:8443/openam/json/realms/root/authenticate?noSession=true'

{
  "message":"Authentication Successful",
  "successUrl":"/openam/console",
  "realm":"/"
}
```

Required: No.

**Authentication Nodes Configuration Reference**

This section covers the configuration of the authentication nodes that are built into AM.
Basic Authentication Nodes

Use the following nodes for basic authentication tasks, such as collecting usernames and passwords:

Data Store Decision Node

The Data Store Decision authentication node verifies that the username and password values exist in the data store configured in the realm.

For example, the username and password could be obtained by a combination of the Username Collector and Password Collector nodes, or the Zero Page Login Collector node.

Tree evaluation continues along the True path if the credentials are located in the configured data store. Otherwise, the tree evaluation continues along the False path.

Note

Unlike the "LDAP Decision Node", which supports LDAP Behera Password Policies, the data store decision node does not have separate outcomes for accounts that are locked or their password has expired.

Properties:

This node has no configurable properties.

Kerberos Node

The Kerberos authentication node enables desktop single sign-on such that a user who has already authenticated with a Kerberos Key Distribution Center can authenticate to AM without having to provide the login information again.

To achieve this, the user presents a Kerberos token to AM through the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol.

End users may need to set up Integrated Windows Authentication in Internet Explorer or Microsoft Edge to benefit from single sign-on when logged on to a Windows desktop.

Tree evaluation continues along the True path if Windows Desktop SSO is successful. Otherwise, the tree evaluation continues along the False path.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Principal</strong></td>
<td>Specifies the Kerberos principal for authentication in the format <code>HTTP/AM-DOMAIN@AD-DOMAIN</code>, where <code>AM-DOMAIN</code> corresponds to the host and domain names of the AM instance, and <code>AD-DOMAIN</code> is the domain name of the Kerberos realm (the FQDN of the Active Directory domain). <code>AD-DOMAIN</code> can differ from the domain name for AM.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>In multi-instance AM deployments, configure AM-DOMAIN as the FQDN or IP address of the load balancer in front of the AM instances.</td>
</tr>
<tr>
<td></td>
<td>For example, HTTP/AM-LB.example.com@KERBEROSREALMINTERNAL.COM.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the KB article How do I set up the WDSSO authentication module in AM in a load-balanced environment?.</td>
</tr>
<tr>
<td>Key Tab File Path</td>
<td>Specifies the full, absolute path of the keytab file for the specified Service Principal.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong></td>
</tr>
<tr>
<td></td>
<td>You generate the keytab file using the Windows ktpass utility; for example:</td>
</tr>
<tr>
<td></td>
<td>C:&gt; ktpass -out fileName.keytab -princ HTTP/openam.example.com@AD_DOMAIN.COM -pass +rdnPass -maxPass 256 -mapuser <a href="mailto:amKerberos@frdpcloud.com">amKerberos@frdpcloud.com</a> -crypto AES256-SHA1 -ptype KRB5_NT_PRINCIPAL -kvno 0</td>
</tr>
<tr>
<td>Kerberos Realm</td>
<td>Specifies the name of the Kerberos (Active Directory) realm used for authentication.</td>
</tr>
<tr>
<td></td>
<td>Must be specified in all caps.</td>
</tr>
<tr>
<td>Kerberos Server Name</td>
<td>Specifies the fully qualified domain name, or IP address of the Kerberos (Active Directory) server.</td>
</tr>
<tr>
<td>Trusted Kerberos realms</td>
<td>Specifies a list of trusted Kerberos realms for user Kerberos tickets. If realms are configured, then Kerberos tickets are only accepted if the realm part of the user principal name of the user's Kerberos ticket matches a realm from the list.</td>
</tr>
<tr>
<td></td>
<td>Each trusted Kerberos realm must be specified in all caps.</td>
</tr>
<tr>
<td>Return Principal with Domain Name</td>
<td>When enabled, AM returns the fully qualified name of the authenticated user rather than just the username.</td>
</tr>
<tr>
<td>Lookup User In Realm</td>
<td>Validates the user against the configured data stores. If the user from the Kerberos token is not found, tree evaluation continues along the False path.</td>
</tr>
<tr>
<td></td>
<td>This search uses the Alias Search Attribute Name from the core realm attributes. See User Profile for more information about this property.</td>
</tr>
<tr>
<td>Is Initiator</td>
<td>When enabled (true), specifies that the node is using initiator credentials, which is the default.</td>
</tr>
<tr>
<td></td>
<td>When disabled (false), specifies that the node is using acceptor credentials.</td>
</tr>
</tbody>
</table>

**Example:**

This flow will attempt to authenticate the user, by using Windows Desktop SSO. If unsuccessful, AM will request the username and password for login. Meter nodes are used to track metrics for the various paths through the tree.
LDAP Decision Node

The LDAP Decision authentication node verifies that the provided username and password values exist in a specified LDAP user data store, and whether they are expired or locked out.

For example, the username and password could be obtained by a combination of the Username Collector and Password Collector nodes, or by using the Zero Page Login Collector node.

Tree evaluation continues along the True outcome path if the credentials are located in the specified LDAP user data store. If the profile associated with the username and password is locked, or the password has expired, tree evaluation continues along the respective Locked or Expired outcome paths. If the user needs to change their password on first login, but cancels the password change form, tree evaluation continues along the Cancelled outcome path.

If the credentials are not found, the tree evaluation continues along the False outcome path.

Properties:
Primary LDAP Server

Specify one or more primary directory servers. Specify each directory server in the following format: `host:port`.

For example, `directory_services.example.com:389`.

Secondary LDAP Server

Specify one or more secondary directory servers. Specify each directory server in the following format: `host:port`.

Secondary servers are used when none of the primary servers are available.

For example, `directory_services_backup.example.com:389`.

DN to Start User Search

Specify the DN from which to start the user search. More specific DNs, such as `ou=sales,dc=example,dc=com`, result in better search performance.
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Bind User DN, Bind User Password</strong></td>
<td>Specifies the credentials used to bind to the LDAP user data store.</td>
</tr>
<tr>
<td><strong>Attribute Used to Retrieve User Profile</strong></td>
<td>Specifies the attribute used to retrieve the profile of a user from the directory server. The user search will have already happened, as specified by the Attributes Used to Search for a User to be Authenticated and User Search Filter properties.</td>
</tr>
<tr>
<td><strong>Attributes Used to Search for a User to be Authenticated</strong></td>
<td>Specifies the attributes used to match an entry in the directory server to the credentials provided by the user. The default value of <code>uid</code> will form the following search filter of <code>uid=user</code>. Specifying multiple values such as <code>uid</code> and <code>cn</code> causes the node to create a search filter of `(</td>
</tr>
<tr>
<td><strong>User Search Filter</strong></td>
<td>Specifies an additional filter to append to user searches. For example, searching for <code>mail</code> and specifying a User Search Filter of <code>(objectClass=inetOrgPerson)</code>, causes AM to use <code>(&amp;(mail=address)(objectClass=inetOrgPerson))</code> as the resulting search filter, where <code>address</code> is the mail address provided by the user.</td>
</tr>
<tr>
<td><strong>Search Scope</strong></td>
<td>Specifies the extent of searching for users in the directory server. Scope <code>OBJECT</code> means search only the entry specified as the DN to Start User Search, whereas <code>ONELEVEL</code> means search only the entries that are directly children of that object. <code>SUBTREE</code> means search the entry specified and every entry under it. Default: <code>SUBTREE</code></td>
</tr>
<tr>
<td><strong>LDAP Connection Mode</strong></td>
<td>Specifies whether to use SSL or StartTLS to connect to the LDAP user data store. AM must be able to trust the certificates used. Possible values: <code>LDAP</code>, <code>LDAPS</code>, and <code>StartTLS</code> Default: LDAP</td>
</tr>
<tr>
<td><strong>Return User DN to DataStore</strong></td>
<td>When enabled, the node returns the DN rather than the User ID. From the DN value, AM uses the RDN to search for the user profile. For example, if a returned DN value is <code>uid=demo,ou=people,dc=openam,dc=example,dc=org</code>, AM uses <code>uid=demo</code> to search the data store. Default: Enabled</td>
</tr>
</tbody>
</table>
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Creation Attributes</td>
<td>This list lets you map (external) attribute names from the LDAP directory server to (internal) attribute names used by AM.</td>
</tr>
<tr>
<td>Minimum Password Length</td>
<td>Specifies the minimum acceptable password length.</td>
</tr>
<tr>
<td>Default: 8</td>
<td></td>
</tr>
<tr>
<td>LDAP Behera Password Policy Support</td>
<td>When enabled, support interoperability with servers that implement the Internet-Draft, Password Policy for LDAP Directories.</td>
</tr>
<tr>
<td>Default: Enabled</td>
<td></td>
</tr>
<tr>
<td>Trust All Server Certificates</td>
<td>When enabled, blindly trust server certificates, including self-signed test certificates.</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td></td>
</tr>
<tr>
<td>LDAP Connection Heartbeat Interval</td>
<td>Specifies how often AM should send a heartbeat request to the directory server to ensure that the connection does not remain idle.</td>
</tr>
<tr>
<td>Some network administrators configure firewalls and load balancers to drop connections that are idle for too long. You can turn this off by setting the value to 0 or to a negative number. Set the units for the interval in the LDAP Connection Heartbeat Time Unit property.</td>
<td></td>
</tr>
<tr>
<td>Default: 10</td>
<td></td>
</tr>
<tr>
<td>LDAP Connection Heartbeat Time Unit</td>
<td>Specifies the time unit corresponding to LDAP Connection Heartbeat Interval.</td>
</tr>
<tr>
<td>Default: Seconds</td>
<td></td>
</tr>
<tr>
<td>LDAP Operations Timeout</td>
<td>Defines the timeout in milliseconds that AM should wait for a response from the directory server.</td>
</tr>
<tr>
<td>Default: 0 (means no timeout)</td>
<td></td>
</tr>
</tbody>
</table>

### Password Collector Node

The Password Collector authentication node prompts the user to enter their password. The captured password is transient, persisting only until the authentication flow reaches the next node requiring user interaction.

Tree evaluation continues along the single outcome path after capturing the password.

![Password Collector](PasswordCollector.png)

**Properties:**

This node has no configurable properties.
Username Collector Node

The Username Collector authentication node prompts the user to enter their username. Tree evaluation continues along the single outcome path after capturing the username.

Properties:

This node has no configurable properties.

Zero Page Login Collector Node

The Zero Page Login Collector authentication node checks whether selected headers are provided in the incoming authentication request, and if so, uses their value as the provided username and password.

Tree evaluation continues along the Has Credentials outcome path if the specified headers are available in the request, or the No Credentials path if the specified headers are not present.

A common use for the Zero Page Login Collector authentication node is to connect the Has Credentials outcome connector to the input of a Data Store Decision node, and the No Credentials outcome connector to the input of a Username Collector node followed by a Password Collector node, and then into the same Data Store Decision node as earlier. For an example of this layout, see the default Example authentication tree provided in AM. See "Example Tree With Zero Page Login Node".

The password collected by the Zero Page Login Collector node is transient, persisting only until the authentication flow reaches the next node requiring user interaction.

Properties:
## Property Summary

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Username Header name | Enter the name of the header that contains the username value.  
  Default: **X-OpenAM-Username**  |
| Password Header name | Enter the name of the header that contains the password value.  
  Default: **X-OpenAM-Password**  |
| Allow without referer | If enabled, the node accepts incoming requests that do not contain a **Referer** HTTP header.  
  If a **Referer** HTTP header is present, the value is not checked.  
  If disabled, a **Referer** HTTP header must be present in the incoming request, and the value must appear in the **Referer whitelist** property.  
  Default: **Enabled**  |
| Referer whitelist | Specify a list of URLs allowed in the **Referer** HTTP header of incoming requests.  
  Incoming requests containing a **Referer** HTTP header value not specified in the whitelist causes tree evaluation to continue along the **No Credentials** outcome path. |
### Multi-Factor Authentication Nodes

Use the following nodes to configure trees with multi-factor authentication capabilities, such as web authentication and push authentication:

#### HOTP Generator Node

The HOTP Generator authentication node creates a string of random digits, of the length specified. The default length is 8 digits.

Passwords are stored in the `oneTimePassword` transient state property of the authentication tree.

Properties:
**Property** | **Usage**
--- | ---
One-time password length | Specify the number of digits in the one-time password.

Use alongside the following authentication nodes to add one-time password verification to the authentication tree:

- OTP Email Sender Node
- OTP SMS Sender Node
- OTP Collector Decision Node

**Example:**

*HmacOneTimePassword Tree With HOTP Generator Node*
OTP Collector Decision Node

The OTP Collector Decision authentication node requests and verifies one-time passwords.

Tree evaluation continues along the **True** outcome path if the entered one-time password is valid for the authentication in progress. Otherwise, the tree evaluation continues along the **False** outcome path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>One Time Password Validity Length</td>
<td>Specify the length of time, in minutes, that a one-time password remains valid. Default: 5</td>
</tr>
</tbody>
</table>

OTP Email Sender Node

The OTP Email Sender authentication node sends an email containing a generated one-time password to the user.

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mail Server Host Name</td>
<td>Specifies the hostname of the SMTP email server.</td>
</tr>
<tr>
<td>Mail Server Host Port</td>
<td>Specifies the outgoing mail server port. Common ports are 25, 465 (when connecting over SSL), or 587 (for StartTLS).</td>
</tr>
<tr>
<td>Mail Server Authentication Username</td>
<td>Specifies the username AM uses to connect to the mail server.</td>
</tr>
<tr>
<td>Mail Server Authentication Password</td>
<td>Specifies the password AM uses to connect to the mail server.</td>
</tr>
<tr>
<td>Email From Address</td>
<td>Specifies the email address from which the one-time password will appear to have been sent.</td>
</tr>
</tbody>
</table>
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Attribute Name</td>
<td>Specifies the user's profile attribute containing the email address to which to email the OTP.</td>
</tr>
<tr>
<td>Default: mail</td>
<td></td>
</tr>
<tr>
<td>Mail Server Secure Connection</td>
<td>Specifies how to connect to the mail server. If a secure method is specified, AM must trust the server certificate of the mail server.</td>
</tr>
<tr>
<td>The possible values for this property are:</td>
<td></td>
</tr>
<tr>
<td>• NON SSL/TLS</td>
<td></td>
</tr>
<tr>
<td>• SSL/TLS</td>
<td></td>
</tr>
<tr>
<td>• Start TLS</td>
<td></td>
</tr>
<tr>
<td>Default: SSL/TLS</td>
<td></td>
</tr>
<tr>
<td>Gateway Implementation Class</td>
<td>Specifies the class the node uses to send SMS and email messages. A custom class must implement the <code>com.sun.identity.authentication.modules.hotp.SMSGateway</code> interface.</td>
</tr>
<tr>
<td>Default: <code>com.sun.identity.authentication.modules.hotp.DefaultSMSGatewayImpl</code></td>
<td></td>
</tr>
</tbody>
</table>

### OTP SMS Sender Node

The OTP SMS Sender authentication node uses an email-to-SMS gateway provider to send an SMS message containing a generated one-time password to the user.

The node sends an email to an address formed by joining the following values together:

- The user's telephone number, obtained by querying a specified profile attribute, for example `telephoneNumber`.
- The `@` character.
- The email-to-SMS gateway domain, obtained by querying the profile attribute specified by the Mobile Carrier Attribute Name property.

For example, if configured to use the `TextMagic` email-to-SMS service, the node might send an email through the specified SMTP server to the address: `18005550187@textmagic.com`.

![OTP SMS Sender](image)

Properties:
### Property | Usage
---|---
Mail Server Host Name | Specifies the hostname of the SMTP email server.
Mail Server Host Port | Specifies the outgoing mail server port. Common ports are 25, 465 (when connecting over SSL), or 587 (for StartTLS).
Mail Server Authentication Username | Specifies the username AM uses to connect to the mail server.
Mail Server Authentication Password | Specifies the password AM uses to connect to the mail server.
Email From Address | Specifies the email address from which the one-time password will appear to have been sent.
### Property

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobile Phone Number Attribute Name</td>
<td>Specifies the user's profile attribute containing the mobile phone number to which to send the SMS containing the OTP.</td>
</tr>
<tr>
<td></td>
<td>Default: <code>telephoneNumber</code></td>
</tr>
<tr>
<td>Mobile Carrier Attribute Name</td>
<td>Specifies the user's profile attribute containing the mobile carrier domain used as the email to SMS gateway.</td>
</tr>
<tr>
<td>Mail Server Secure Connection</td>
<td>Specifies how to connect to the mail server. If a secure method is specified, AM must trust the server certificate of the mail server.</td>
</tr>
<tr>
<td></td>
<td>The possible values for this property are:</td>
</tr>
<tr>
<td></td>
<td>• NON SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>• SSL/TLS</td>
</tr>
<tr>
<td></td>
<td>• Start TLS</td>
</tr>
<tr>
<td></td>
<td>Default: <code>SSL/TLS</code></td>
</tr>
<tr>
<td>Gateway Implementation Class</td>
<td>Specifies the class the node uses to send SMS and email messages. A custom class must implement the <code>com.sun.identity.authentication.modules.hotp.SMSGateway</code> interface.</td>
</tr>
<tr>
<td></td>
<td>Default: <code>com.sun.identity.authentication.modules.hotp.DefaultSMSGatewayImpl</code></td>
</tr>
</tbody>
</table>

### Push Result Verifier Node

The Push Result Verifier node works together with the Push Sender Node to validate the user's response to a previously sent push notification message.

Tree evaluation continues along the **Success** outcome path if the push notification was positively responded to by the user. For example, using the ForgeRock Authenticator app, the user slid the switch with a checkmark on horizontally to the right.

Tree evaluation continues along the **Failure** outcome path if the push notification was negatively responded to by the user. For example, using the ForgeRock Authenticator app, the user tapped the cancel icon in the top-right of the screen.

If the push notification was not responded to within the Message Timeout value specified in the Push Sender Node then tree evaluation continues along the **Expired** outcome path.

If a response to the push message has not yet been received, then tree evaluation continues along the **Waiting** outcome path.
Tip

If the push message contained any additional information, for example if it was a registration request, the values are stored in the sharedState object of the tree, in a key named pushContent. For information on creating or customizing authentication nodes, see Authentication Node Development Guide.

Properties:

This node has no configurable properties.

Push Sender Node

The Push Sender authentication node sends push notification messages to a device such as a mobile phone, enabling multi-factor authentication.

The Push Sender authentication node requires that the Push Notification Service has also been configured. For information on the properties used by the service, see "Push Notification Service" in the Reference. For information on provisioning the credentials used by the service, see How To Configure Service Credentials (Push Auth, Docker) in Backstage in the ForgeRock Knowledge Base.

Tree evaluation continues along the Sent outcome path if the push notification was successfully sent to the handling service.

If the user does not have a registered device, tree evaluation continues along the Not Registered outcome path. To determine whether the user has a registered device, the tree must have already acquired a username, for example by using a Username Collector Node.

Note

Authentication trees are not capable of registering a device to a profile. For information on using authentication chains to register devices, see "Creating Chains for Push Authentication".

If the user chooses to skip push authentication, tree evaluation continues along the Skipped outcome path. You can configure whether the user is able to skip the node by setting the Two Factor Authentication Mandatory property. See "Letting Users Opt Out of One-Time Password Authentication (OATH)".
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Message Timeout</strong></td>
<td>Specifies the number of milliseconds the push notification message will remain valid. The Push Result Verifier Node rejects responses to push messages that have timed out.</td>
</tr>
<tr>
<td><strong>User Message</strong></td>
<td>Specifies the optional message to send to the user.</td>
</tr>
<tr>
<td></td>
<td>You can provide the message in multiple languages by specifying the locale in the KEY field, for example en-US. For information on valid locale strings, see JDK 11 Supported Locales. The locale selected for display is based on the user’s locale settings in their browser.</td>
</tr>
<tr>
<td></td>
<td>Messages provided in the node override the defaults provided by AM. For information about customizing and translating the default messages, see &quot;Internationalization&quot; in the Authentication Node Development Guide.</td>
</tr>
<tr>
<td></td>
<td>The following variables can be used in the VALUE field:</td>
</tr>
<tr>
<td>{{user}}</td>
<td>Replaced with the username value of the account registered in the ForgeRock Authenticator app, for example Demo.</td>
</tr>
<tr>
<td>{{issuer}}</td>
<td>Replaced with the issuer value of the account registered in the ForgeRock Authenticator app, for example ForgeRock.</td>
</tr>
<tr>
<td>Example:</td>
<td>Login attempt from {{user}} at {{issuer}}.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Remove 'skip' option</td>
<td>Enable this option in the node to make the push authentication mandatory. When set to Disabled the user can skip the push authentication requested by the node, and tree evaluation continues along the Skipped outcome path.</td>
</tr>
</tbody>
</table>

**Note**

Nodes in authentication trees are not affected by the Two Factor Authentication Mandatory property, available at Realms > Realm Name > Authentication > Settings > General, as it only applies to modules within authentication chains.

Example:

**Example Push Tree**

The example tree above shows one possible implementation of multi-factor push authentication.

If the user has a registered device:
1. A push notification is sent to their registered device.

2. The Polling Wait Node pauses the authentication tree for 8 seconds, during which time the user can respond to the push notification on their device, for example by using the ForgeRock Authenticator application.

   • If the user responds positively, they are authenticated successfully and logged in.

   • If the user responds negatively, they are not authenticated successfully and do not receive a session.

   • If the push notification expires, the tree will send a new push notification.

   **Tip**

   A Retry Limit Decision node could be used here to constrain the number of times a new code is sent.

   • If the user has not yet responded, the tree loops back a step and the Polling Wait Node pauses the authentication tree for another 8 seconds.

If the user exits the Polling Wait Node, they can enter a recovery code in order to authenticate.

   **Tip**

   In this situation, configure the Exit Message property in the Polling Wait node with a message such as: *Lost phone? Use a Recovery Code*, which appears as follows:
A Retry Limit Decision node allows three attempts at entering a recovery code before failing the authentication.

If the user *does not have a registered device*:

1. Because trees cannot currently register devices, a Set Failure URL node redirects the user to an authentication chain which can register a device to the user's profile.

2. That registration chain redirects the user back to the push example tree when registration is complete.

If the configuration allows it and the user *chooses to skip multi-factor authentication*:

1. An Inner Tree Evaluator node provides an alternative method of authentication, for example an LDAP Decision node.

2. Depending on the outcome of the inner tree, the push example tree evaluation continues to the *Success* or *Failure* outcome.

**Recovery Code Collector Decision Node**

The Recovery Code Collector Decision authentication node allows users to authenticate using a recovery code provided when registering a device for multi-factor authentication.

Use this node when a tree is configured to use push notifications or one-time passwords but the user has lost the registered device, and must therefore use an alternative method for authentication. For
more information on viewing the recovery codes when registering a device, see "Registering the ForgeRock Authenticator for Multi-Factor Authentication".

Tree evaluation continues along the True outcome path if the provided recovery code matches one belonging to the user. To determine whether the provided code belongs to the user, the tree must have already acquired the username, for example by using a Username Collector Node.

If the recovery code does not match, or a username has not been acquired, tree evaluation continues along the False outcome path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recovery Code Type</td>
<td>Specify the type of recovery code the user will submit for verification.</td>
</tr>
<tr>
<td></td>
<td>Default: OATH</td>
</tr>
</tbody>
</table>

Recovery Code Display Node

The Recovery Code Display node is used in conjunction with the WebAuthn Registration Node. It retrieves generated recovery codes from the transient state and presents them to the user, for safekeeping. The codes can be used to authenticate if a registered device is lost or stolen.

Generated recovery codes are inserted into transient state when tree evaluation continues along the Success outcome path of the WebAuthn Registration Node. Connect the Recovery Code Display node to the Success outcome path to display the codes.

If no recovery codes are available in transient state, tree evaluation continues along the only outcome path, and nothing is displayed to the user.
Important

Generated recovery codes cannot be retrieved from the user's profile - they are one-way encrypted. The Recovery Code Display node is the one and only opportunity to view the recovery codes, and keep them safe.

Properties:

This node has no configurable properties.

Example:

The following is an example of the output of the Recovery Code Display node:

Example output of the Recovery Code Display node

![Example output of the Recovery Code Display node](image-url)
WebAuthn Authentication Node

The WebAuthn Authentication node allows users of supported clients to use a registered FIDO device during authentication.

To determine whether the user has a registered device, the tree must have already acquired a username, for example by using a Username Collector Node.

If the user's client does not support web authentication, tree evaluation will continue along the Unsupported outcome path. For example, clients connected over the HTTP protocol rather than HTTPS do not support WebAuthn.  

If the user does not have a registered device, tree evaluation continues along the No Device Registered outcome path.

If AM encounters an issue when attempting to authenticate using the device, tree evaluation continues along the Failure outcome path. For example, AM could not verify that the response from the authenticator was appropriate for the specific instance of the authentication ceremony.

If the user's client encounters an issue when attempting to authenticate using the device, for example, if the timeout was reached, then tree evaluation continues along the Client Error outcome path. This outcome is used whenever the client throws a DOMException, as required by the Web Authentication: An API for accessing Public Key Credentials Level 1 specification.

Tip

If a client error occurs, the error type and description are added to a property named WebAuthenticationDOMException in the shared state. This property can be read by other nodes later in the tree, if required.

If the Allow recovery code property is enabled, AM provides the user the option to enter a recovery code rather than authenticate using a device. Tree evaluation continues along the Recovery Code outcome path if the users chooses to enter a recovery code. To accept and verify the recovery code, ensure the outcome path leads to a Recovery Code Collector Decision Node.

If the user successfully authenticates with a device of the type determined by the User verification requirement property, tree evaluation continues along the Success outcome path.

HTTPS may not be required when testing locally, on http://localhost, for example. For more information, see Is origin potentially trustworthy?.

---

1 HTTPS may not be required when testing locally, on http://localhost, for example. For more information, see Is origin potentially trustworthy?.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relying party identifier</td>
<td>Specifies the domain used as the relying party identifier during web authentication. If not specified, AM uses the domain name of the instance, for example openam.example.com. Specify an alternative domain if your AM instances are behind a load balancer, for example.</td>
</tr>
<tr>
<td>Origin domains</td>
<td>Specifies a list of fully qualified URLs to accept as the origin of incoming requests. If left empty, AM accepts any incoming domain.</td>
</tr>
<tr>
<td>User verification requirement</td>
<td>Specifies the required level of user verification. The available options are:</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td><strong>REQUIRED</strong></td>
<td>The authenticator used must verify the identity of the user, for example, by using biometrics. Authenticators that do not verify the identity of the user should not be activated for authentication.</td>
</tr>
<tr>
<td><strong>PREFERRED</strong></td>
<td>Use of an authenticator that verifies the identity of the user is preferred, but if none are available any authenticator is accepted.</td>
</tr>
<tr>
<td><strong>DISCOURAGED</strong></td>
<td>Use of an authenticator that verifies the identity of the user is not required. Authenticators that do not verify the identity of the user should be preferred.</td>
</tr>
<tr>
<td>Allow recovery codes</td>
<td>Specify whether to allow the user to enter one of their recovery codes instead of performing an authentication gesture. Enabling this options adds a Recovery Code outcome path to the node. This outcome path should lead to a Recovery Code Collector Decision Node in order to collect and verify the recovery code.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify the number of seconds to wait for a response from an authenticator. If the specified time is reached, tree evaluation continues along the Client error outcome path, and a relevant message is stored in the WebAuthenticationDOMException property of the shared state.</td>
</tr>
<tr>
<td>Username from device</td>
<td>Specifies whether AM requests that the device provides the username. When enabled, if the device is unable to store or provide usernames, the node will fail and results in the Failure outcome. For information on using this property for usernameless authentication with ForgeRock Go, see &quot;Configuring Usernameless Authentication with ForgeRock Go&quot;.</td>
</tr>
<tr>
<td>Return challenge as JavaScript</td>
<td>Specifies that the node returns its challenge as a fully encapsulated client-side JavaScript that interacts directly with the WebAuthn API, and auto-submits the response back. If disabled, the node returns the challenge and associated data in a metadata callback. A custom UI, for example an application using the ForgeRock SDKs, uses the information from the callback to interact with the WebAuthn API on AM's behalf.</td>
</tr>
</tbody>
</table>

Example:
The example tree above shows one possible implementation of a tree for authenticating with WebAuthn devices.

After verifying the users credentials against the configured data store, tree evaluation continues to the WebAuthn Authentication Node.

If the user's client does not support WebAuthn, the tree fails and the user does not get a session. A more user-friendly approach would be to set a success URL to redirect the user to a page explaining the benefits of multi-factor authentication, and then proceeding to the Success node.

If there are no registered WebAuthn devices present in the user's profile, the failure URL is set, pointing to a tree that allows the user to register a device. This stage could also be an Inner Tree Evaluator, with a registration tree inside.

If the user's client does support WebAuthn, and the connection is secured with TLS, the user will be asked to complete an authorization gesture, for example scanning a fingerprint, or entering a PIN number:
The user's browser may present a consent pop-up to allow access to the authenticators available on the client. When consent has been granted, the browser activates the relevant authenticators, ready for authentication.

**Tip**

The relying party details configured in the node are often included in the consent message to help the user verify the entity that is requesting access.

The authenticators the client activates for authentication depends in the value of the properties in the node. For example, if the **User verification requirement** property is set to **REQUIRED**, the client SHOULD only activate authenticators which verify the identity of the user. For extra protection, AM WILL verify that the response from an authenticator matches the criteria configured for the node, and will reject - by using the **Failure** outcome - an authentication attempt by an inappropriate authenticator type.

When the user completes an **authorization gesture**, for example scanning a fingerprint, or entering a PIN number, tree evaluation continues along the **Success** outcome path. In this example, their authentication level is increased by ten to signify the stronger authentication that has occurred, and the user is taken to their profile page.

If the user clicks the **Use Recovery Code** button, tree evaluation continues to the **Recovery Code Collector Decision Node**, ready to accept the recovery code. If verified, the user is taken to their profile page.
Any problems encountered during the authentication (through the **Failure** outcome), including a timeout (through the **Client Error** outcome), results in the overall failure of the authentication tree.

**WebAuthn Device Storage Node**

The WebAuthn Device Storage node writes information about FIDO2 devices to a user's profile, so that they can subsequently authenticate using the device.

Use this node to store the device data that the "WebAuthn Registration Node" places into the tree's transient state when its Store device data in transient state property is enabled.

If AM encounters an issue when attempting to save the device data to the user's profile; for example, the user has not been identified earlier in the tree, then tree evaluation continues along the **Failure** outcome path.

If the node successfully stores the device data to the user's profile, tree evaluation continues along the **Success** outcome path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Generate recovery codes</td>
<td>Specify whether WebAuthn device recovery codes should be generated. If enabled, recovery codes are generated and stored in the tree's transient state, and stored alongside the device profile. Use the Recovery Code Display Node to display the codes to the user for safe keeping.</td>
</tr>
</tbody>
</table>

**Important**

Generating recovery codes will overwrite all existing WebAuthn device recovery codes.
WebAuthn Registration Node

The WebAuthn Registration authentication node allows users of supported clients to register FIDO2 devices for use during authentication.

AM interacts with FIDO2/WebAuthn capable browsers, for example Chrome, Firefox and Microsoft Edge. These browsers interact with CTAP2 authenticators, including U2F and FIDO2 Security Keys, and platforms such as Windows Hello or MacOS TouchId.

If the user's client does not support WebAuthn, tree evaluation will continue along the Unsupported outcome path. For example, clients connected over the HTTP protocol rather than HTTPS do not support WebAuthn.

If AM encounters an issue when attempting to register using a device, tree evaluation continues along the Failure outcome path. For example, AM could not verify that the response from the authenticator was appropriate for the specific instance of the authentication ceremony.

If the user's client encounters an issue when attempting to register using a device, for example, if the timeout was reached, then tree evaluation continues along the Client Error outcome path. This outcome is used whenever the client throws a DOMException, as required by the Web Authentication: An API for accessing Public Key Credentials Level 1 specification.

Tip

If a client error occurs, the error type and description are added to a property named WebAuthenticationDOMException in the shared state. This property can be read by other nodes later in the tree, if required.

If the user successfully registers an authenticator of the correct type as determined by the node's properties, tree evaluation continues along the Success outcome path.

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Relying party</td>
<td>Specify the name of the relying party entity that is registering and authenticating users by using WebAuthn. For example, Example Inc.</td>
</tr>
<tr>
<td>Relying party identifier</td>
<td>Specifies the domain used as the relying party identifier during WebAuthn. If not specified, AM uses the domain name of the instance, for example openam.example.com. Specify an alternative domain if your AM instances are behind a load balancer, for example.</td>
</tr>
<tr>
<td>Origin domains</td>
<td>Specifies a list of fully qualified URLs to accept as the origin of incoming requests.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>If left empty, AM accepts any incoming domain.</td>
<td>If left empty, AM accepts any incoming domain.</td>
</tr>
<tr>
<td>User verification requirement</td>
<td>Specifies the required level of user verification.</td>
</tr>
<tr>
<td></td>
<td>The available options are:</td>
</tr>
<tr>
<td></td>
<td>REQUIRED</td>
</tr>
<tr>
<td></td>
<td>The authenticator used must verify the identity of the user, for example by using biometrics. Authenticators that do not verify the identity of the user should not be activated for registration.</td>
</tr>
<tr>
<td></td>
<td>PREFERRED</td>
</tr>
<tr>
<td></td>
<td>Use of an authenticator that verifies the identity of the user is preferred, but if none are available any authenticator is accepted.</td>
</tr>
<tr>
<td></td>
<td>DISCOURAGED</td>
</tr>
<tr>
<td></td>
<td>Use of an authenticator that verifies the identity of the user is not required. Authenticators that do not verify the identity of the user should be preferred.</td>
</tr>
<tr>
<td>Preferred mode of attestation</td>
<td>Specifies whether AM requires that the authenticator provides attestation statements.</td>
</tr>
<tr>
<td></td>
<td>The available options are:</td>
</tr>
<tr>
<td></td>
<td>NONE</td>
</tr>
<tr>
<td></td>
<td>AM does not require the authenticator to provide attestation statements. If the authenticator does send attestation statements, AM will not verify them, and will not fail the process.</td>
</tr>
<tr>
<td></td>
<td>INDIRECT</td>
</tr>
<tr>
<td></td>
<td>AM does not require the authenticator to provide attestation statements. If the authenticator does send attestation statements, AM will verify them, and will fail the process if they fail verification.</td>
</tr>
<tr>
<td></td>
<td>DIRECT</td>
</tr>
<tr>
<td></td>
<td>AM requires that the authenticator provides attestation statements, and will verify them. The process will fail if the attestation statements cannot be verified.</td>
</tr>
<tr>
<td></td>
<td>AM supports the following attestation formats:</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>• Packed</td>
</tr>
<tr>
<td></td>
<td>• FIDO U2F</td>
</tr>
<tr>
<td></td>
<td>• TPM</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Important</strong></td>
<td>You must set the Preferred mode of attestation property to <strong>NONE</strong> to use an authenticator that provides attestation statements in a format other than the supported formats above.</td>
</tr>
<tr>
<td></td>
<td>Specifically, AM <strong>does not</strong> currently support:</td>
</tr>
<tr>
<td></td>
<td>• android-safetynet</td>
</tr>
<tr>
<td></td>
<td>• android-key</td>
</tr>
<tr>
<td>Accepted signing algorithms</td>
<td>Specify the algorithms that authenticators can use to sign their assertions.</td>
</tr>
<tr>
<td>Authentication attachment</td>
<td>Specifies whether AM requires that the authenticator is a particular attachment type.</td>
</tr>
<tr>
<td></td>
<td>There are two types of authenticator attachment:</td>
</tr>
<tr>
<td></td>
<td>• An authenticator that is built-in to the client device is labelled a <em>platform attachment</em>.</td>
</tr>
<tr>
<td></td>
<td>A fingerprint scanner built-in to a phone or laptop is an example of a platform attachment authenticator.</td>
</tr>
<tr>
<td></td>
<td>An authenticator that can roam, or move, between different client devices is labelled a <em>cross-platform attachment</em>.</td>
</tr>
<tr>
<td></td>
<td>A USB hardware security key is an example of a cross-platform attachment authenticator.</td>
</tr>
<tr>
<td></td>
<td>There are two types of authenticator attachment:</td>
</tr>
<tr>
<td></td>
<td>• An authenticator that is built-in to the client device is labelled a <em>platform attachment</em>.</td>
</tr>
<tr>
<td></td>
<td>A fingerprint scanner built-in to a phone or laptop is an example of a platform attachment authenticator.</td>
</tr>
<tr>
<td></td>
<td>• An authenticator that can roam, or move, between different client devices is labelled a <em>cross-platform attachment</em>.</td>
</tr>
<tr>
<td></td>
<td>A USB hardware security key is an example of a cross-platform attachment authenticator.</td>
</tr>
<tr>
<td></td>
<td>The available options are:</td>
</tr>
<tr>
<td></td>
<td><strong>UNSPECIFIED</strong></td>
</tr>
<tr>
<td></td>
<td>AM accepts any attachment type.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>PLATFORM</strong></td>
<td>The authenticator must be a <em>platform</em> attachment type. The client should not activate other authenticator types for registration.</td>
</tr>
<tr>
<td><strong>CROSS_PLATFORM</strong></td>
<td>The authenticator must be a <em>cross-platform</em> attachment type. The client should not activate other authenticator types for registration.</td>
</tr>
<tr>
<td>Trust Store alias</td>
<td>Specifies the name of a secret store configured in the realm that contains CA-issued certificate chains, which can be used to verify attestation data provided by a device. The value is also appended to the string <code>am.authentication.nodes.webauthn.truststore</code> to form the dynamic secret ID used to map the certificate chains. For more information, see &quot;Configuring WebAuthn Trust Anchors&quot;.</td>
</tr>
<tr>
<td>Enforce revocation check</td>
<td>Specifies whether to enforce certificate revocation checks. When enabled, then any attestation certificate's trust chain <strong>MUST</strong> have a CRL or OCSP entry that can be verified by AM during processing. When disabled, certificates are not checked for revocation. You must ensure expired or revoked certificates are manually removed.</td>
</tr>
<tr>
<td>Timeout</td>
<td>Specify the number of seconds to wait for a response from an authenticator. If the specified time is reached, tree evaluation continues along the Client error outcome path, and a relevant message is stored in the <code>WebAuthenticationDOMException</code> property of the shared state.</td>
</tr>
<tr>
<td>Limit registrations</td>
<td>Specify whether the same authenticator can be registered multiple times. If enabled, the client should not activate an authenticator that is already registered for registration.</td>
</tr>
<tr>
<td>Generate recovery codes</td>
<td>Specify whether WebAuthn-specific recovery codes should be generated. If enabled, recovery codes are generated and stored in transient state if registration was successful. Use the Recovery Code Display Node to display the codes to the user for safekeeping. If you have enabled the Store device data in transient state and there are not saving the device data to the user's profile immediately, do not enable this property. Enable the Generate recovery codes property in the WebAuthn Device Storage node instead. Generating recovery codes will overwrite all existing WebAuthn-specific recovery codes.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Store data in transient state | Specify whether the information provided by the device to the node will be stored in the tree's transient state for later analysis by subsequent nodes, using the key `webauthnData`.  
  In addition to the information provided by the device, the type of attestation achieved; for example, `BASIC`, `CA`, `SELF` and so on, will be stored in the tree's transient data, using the key `webauthnAttestationType`.  
  **Warning**  
  The amount of data involved can be large. Only enable this option if you intend to analyze it. |
| Store device data in transient state | Specify whether the information about the device required for WebAuthn is stored in the tree's transient state rather than saved immediately to the user's profile.  
  Enable this option if you intend to make decisions in scripts, and have enabled the Store data in transient state property, and therefore do not want to register the device to the user until the outcome of the analysis is complete.  
  **Important**  
  Do not alter the data whilst it is in the tree's transient state, nor when saved to a user's profile.  
  Modifying the device data will likely cause the device to be unable to authenticate.  
  Use the "WebAuthn Device Storage Node" to write the device data to the user's profile when this option is enabled.  
  When disabled, device data is written automatically to the user's profile when registration is successful. |
| Username to device            | Specifies whether AM requests that the device stores the user's username.  
  When enabled, if the device is unable to store or provide usernames, the node will fail and results in the `Failure` outcome.  
  For information on using this property for usernameless authentication with ForgeRock Go, see “Configuring Usernameless Authentication with ForgeRock Go”. |
<p>| Shared state attribute for display name | Specifies a variable in tree's shared state that contains a display name for the user; for example, their full name, or email address. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Username to device property</td>
<td>The value is written to devices alongside the username when the Username to device property is enabled, and helps the user select between the accounts they may have on their devices. If not specified, or the variable is not found in shared state, the user name is used. For information on using this property for usernameless authentication with ForgeRock Go, see &quot;Configuring Usernameless Authentication with ForgeRock Go&quot;.</td>
</tr>
<tr>
<td>Return challenge as JavaScript</td>
<td>Specifies that the node returns its challenge as a fully encapsulated client-side JavaScript that interacts directly with the WebAuthn API, and auto-submits the response back. If disabled, the node returns the challenge and associated data in a metadata callback. A custom UI; for example, an application using the ForgeRock SDKs, uses the information from the callback to interact with the WebAuthn API on AM's behalf. Example:</td>
</tr>
</tbody>
</table>

**Example WebAuthn Registration Tree**

![Example WebAuthn Registration Tree](image)

The example tree above shows a possible implementation of a tree for registering WebAuthn devices.

After verifying the users credentials against the configured data store, tree evaluation continues to the WebAuthn Registration Node.

If the user's client does not support WebAuthn, the failure URL is altered, for example to redirect the user to a page explaining which clients and operating systems support WebAuthn.

If the user's client does support WebAuthn, and the connection is secured with TLS, the user will be asked to register an authenticator:
The user's browser may present a consent pop-up to allow access to the authenticators available on the client. When consent has been granted the browser activates the relevant authenticators, ready for registration.

**Tip**

The relying party details configured in the node are often included in the consent message to help the user verify the entity that is requesting access.

The authenticators the client activates for registration depends on the value of the properties in the node. For example, if the `User verification requirement` property is set to **REQUIRED**, the client would not activate a USB hardware security key for registration.

When the user completes an `authorization` gesture, for example scanning a fingerprint, or entering a PIN number, tree evaluation continues along the `Success` outcome path, and in this example will be taken to their profile page.

The registered authenticator appears on the user's dashboard page, with the label *New Security Key*. To rename the authenticator, click its vertical ellipsis context icon (ências), and then click Rename.

Any problems encountered during the registration, including a timeout, result in tree evaluation continuing to the `Failure` outcome.

**Risk Management Authentication Nodes**

Use the following nodes to examine the perceived risk associated to the authentication and act on it:
Account Active Decision Node

Checks if the account the user has entered is activated. This node relies on the tree's shared state to determine which account to check. Use this node to validate whether an account is currently activated, such as in login flows where an account may already be created, but not enabled until a later date.

For more information, see "About Account Lockout for Trees".

Properties:

This node has no configurable properties.

Account lockout Node

The Account lockout node can lock or unlock the authenticating user's account profile.

For more information, see "About Account Lockout for Trees".

![Account lockout node](image)

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock Action</td>
<td>Choose whether to <strong>LOCK</strong> or <strong>UNLOCK</strong> the authenticating user's account profile.</td>
</tr>
<tr>
<td></td>
<td>The Data Store Decision authentication node checks if the account profile is in the LOCK state. For more information, see &quot;Data Store Decision Node&quot;.</td>
</tr>
</tbody>
</table>

Example:

The following example uses the Account lockout Decision authentication node with the Retry Limit Decision Node to lock an account after a number of invalid attempts:
Auth Level Decision Node

The Auth Level Decision authentication node compares the current authentication level value against a configured value.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sufficient Authentication Level</td>
<td>Tree evaluation continues along the True path if the current authentication level is equal to or greater than the entered integer. Otherwise, the tree evaluation continues along the False path.</td>
</tr>
</tbody>
</table>

Modify Auth Level Node

The Modify Auth Level authentication node lets you increase or decrease the current authentication level value.

Tree evaluation continues along the single outcome path after modifying the authentication level.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Value to add</td>
<td>Enter a positive integer to increase the current authentication level, or a negative integer to decrease the current authentication level by the specified value.</td>
</tr>
</tbody>
</table>

CAPTCHA Node

The CAPTCHA node implements Google's reCAPTCHA v2 widget and hCaptcha's hCaptcha v1 widget, to add CAPTCHA support to authentication trees. This node verifies the response token received from Google or hCaptcha in addition to creating a CAPTCHA callback for the UI to interact with.

The node is configured by default for Google's reCAPTCHA.

Properties:
### CAPTCHA Node

#### CAPTCHA Site Key
Specifies the CAPTCHA site key. This is provided by Google or hCaptcha when signing up for access to the API. This is a required property.

#### CAPTCHA Secret Key
Specifies the CAPTCHA secret key. This is provided by Google or hCaptcha when signing up for access to the API. This is a required property.

#### CAPTCHA Verification URL
Specifies the URL used to verify the CAPTCHA submission. This is a required property. Possible values are:
- **Google**: `https://www.google.com/recaptcha/api/siteverify`
- **hCaptcha**: `https://hcaptcha.com/siteverify`

#### CAPTCHA API URL
Specifies the URL of the JavaScript that loads the CAPTCHA widget. This is a required property. Possible values are:
- **Google**: `https://www.google.com/recaptcha/api.js`
- **hCaptcha**: `https://hcaptcha.com/1/api.js`

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CAPTCHA Site Key</td>
<td>Specifies the CAPTCHA site key. This is provided by Google or hCaptcha when signing up for access to the API. This is a required property.</td>
</tr>
<tr>
<td>CAPTCHA Secret Key</td>
<td>Specifies the CAPTCHA secret key. This is provided by Google or hCaptcha when signing up for access to the API. This is a required property.</td>
</tr>
<tr>
<td>CAPTCHA Verification URL</td>
<td>Specifies the URL used to verify the CAPTCHA submission. This is a required property. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Google: <code>https://www.google.com/recaptcha/api/siteverify</code></td>
</tr>
<tr>
<td></td>
<td>- hCaptcha: <code>https://hcaptcha.com/siteverify</code></td>
</tr>
<tr>
<td>CAPTCHA API URL</td>
<td>Specifies the URL of the JavaScript that loads the CAPTCHA widget. This is a required property. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>- Google: <code>https://www.google.com/recaptcha/api.js</code></td>
</tr>
<tr>
<td></td>
<td>- hCaptcha: <code>https://hcaptcha.com/1/api.js</code></td>
</tr>
</tbody>
</table>
Behavioral Authentication Nodes

Use the following nodes to adjust the behavior of authentication trees:

Increment Login Count Node

Increments the successful login count property of a managed object in IDM. This requires integration with IDM to work, and is used in conjunction with the "Login Count Decision Node". If you plan to track the number of logins, this node will need to be included in your login authentication flow, but can be safely omitted if you are not planning to use that functionality.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

Login Count Decision Node

Triggers an action when a user's successful login count property reaches a specified number. The action can either be triggered once, by setting the interval property to happen AT the set amount of successful login attempts; or set to occur EVERY time the specified number of additional successful login attempts occur. This requires integration with IDM to work, and is used in conjunction with the "Increment Login Count Node". The Increment Login Count Node needs to be present in your login authentication flow for the Login Count Decision Node to have the data necessary to trigger a decision.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interval</td>
<td>The type of interval the decision should trigger on. Valid types are every and at. Every refers to a recurring action that happens every specified number of successful logins, such as prompting a user to update their contact information every 30 days. At refers to an action that occurs once, after the specified number of successful logins. For example, prompting the user to set their communication preferences once they have logged in 10 times.</td>
</tr>
<tr>
<td>Amount</td>
<td>The amount (count) of logins the interval should trigger on.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

Contextual Authentication Nodes

Use the following nodes to examine the authentication context and act on it:

Certificate Collector Node

This node collects an X.509 digital certificate from the request coming from the authenticating user so that AM can use it as the user's credentials.

The tree continues through the Collected path if AM collects the digital certificate, and through the Not Collected path, otherwise.

To validate the certificate, add a "Certificate Validation Node" to the tree.

Properties:
### Certificate Collector Node

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Collection Method</td>
<td>Specifies how AM should collect the certificate from the request. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Request. AM looks for the certificate in the request. Use this value if TLS termination happens at the container where AM runs.</td>
</tr>
<tr>
<td></td>
<td>• Header. AM looks for the certificate in the HTTP header name specified in the HTTP Header Name for the Client Certificate property.</td>
</tr>
<tr>
<td></td>
<td>• Either. AM looks for the certificate in the request; if it cannot find it, AM looks for the certificate in the HTTP header specified</td>
</tr>
<tr>
<td></td>
<td>in the HTTP Header Name for the Client Certificate property. Use this value if TLS termination happens in a proxy or load balancer</td>
</tr>
<tr>
<td></td>
<td>placed in front of the container where AM runs.</td>
</tr>
<tr>
<td></td>
<td>Default: <strong>Either</strong></td>
</tr>
</tbody>
</table>

**HTTP Header Name for the Client Certificate**

Specifies the name of the HTTP header containing the certificate when the Certificate Collection Method property is configured to **Header** or **Either**.

Default: No value specified.

**Trusted Remote Hosts**

Specifies a list of IP addresses trusted to supply certificates on behalf of the authenticating client, such as load balancers doing SSL termination.

If no value is specified, AM will reject certificates supplied by remote hosts. If you specify the **any** value, AM will trust certificates on behalf of the authenticating client supplied by any remote host.

Default: No value specified.
Certificate Validation Node

This node validates a digital X.509 certificate collected by the "Certificate Collector Node".

The node has different outcomes, some of which are used depending on the configuration of the node:

- **True**: The node could validate the certificate.
- **False**: The node could not validate the certificate. The node will use this path when it cannot validate the certificate but the cause is not managed by any of the other outcomes.
- **Not found**: The Match Certificate in LDAP property is enabled, but the certificate was not found in the LDAP store.
- **Expired**: The Check Certificate Expiration property is enabled, and the certificate has expired.
- **Path Validation Failed**: The Match Certificate to CRL property is enabled, and the certificate path is invalid.
- **Revoked**: The OCSP Validation property is enabled, and the certificate has been revoked.

When the outcome is **True**, append a "Certificate User Extractor Node" to extract the values of the certificate and return them to AM.

![Certificate Validation Node Diagram]

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Match Certificate in LDAP</td>
<td>When enabled, AM matches the certificate collected with the one stored in an LDAP directory entry. This entry, and additional security-related properties, are defined later in the node. Default: Disabled</td>
</tr>
<tr>
<td>Check Certificate Expiration</td>
<td>When enabled, AM checks whether the certificate has expired. Default: Disabled</td>
</tr>
<tr>
<td>Subject DN Attribute Used to Search LDAP for Certificates</td>
<td>Specifies the attribute that AM will use to search the LDAP directory for the certificate. The search filter will also use the value of the Subject DN as it appears in the certificate.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------</td>
<td>-------</td>
</tr>
<tr>
<td><strong>Match Certificate to CRL</strong></td>
<td>When enabled, AM checks whether the certificate has been revoked according to a CRL in the LDAP directory. Related properties are defined later in the node. Default: Disabled.</td>
</tr>
</tbody>
</table>
| **Issuer DN Attribute(s) Used to Search LDAP for CRLs** | Specifies which attribute and value in the certificate Issuer DN AM will use to find the CRL in the LDAP directory.  
If only one attribute is specified, the LDAP search filter used is \( (attr\text{-}name=attr\text{-}value-in-subject-DN) \).  
For example, if the subject DN of the issuer certificate is \( C=US, \text{CN}=Some \text{ CA}, \text{serialNumber}=123456 \), and the attribute specified is \( \text{CN} \), then the LDAP search filter used to find the CRL is \( (\text{CN}=Some \text{ CA}) \).  
Specify several CRLs for the same CA issuer in a comma-separated list (,) where the names are in the same order as they occur in the subject DN.  
In this case, the LDAP search filter used is \( (\text{cn}=\text{attr1}=\text{attr1-value-in-subject-DN}, \text{attr2}=\text{attr2-value-in-subject-DN},..., \text{and so on.} \)  
For example, if the subject DN of the issuer certificate is \( C=US, \text{CN}=Some \text{ CA}, \text{serialNumber}=123456 \), and the attributes specified are \( \text{CN}, \text{serialNumber} \), then the LDAP search filter used to find the CRL is \( (\text{cn}=\text{CN}=Some \text{ CA}, \text{serialNumber}=123456) \). Default: \( \text{CN} \) |
| **HTTP Parameters for CRL Update** | Specifies parameters that AM will include in any HTTP CRL call to the CA that issued the certificate.  
If the client or CA contains the Issuing Distribution Point Extension, AM uses this information to retrieve the CRL from the distribution point.  
Add the parameters as key pairs of values in a comma-separated list (,). For example, \( \text{param1}=\text{value1}, \text{param2}=\text{value2} \). |
| **Cache CRLs in Memory** | (LDAP distribution points only) When enabled, AM caches CRLs. Default: Enabled |
| **Update CA CRLs from CRLDistributionPoint** | When enabled, AM updates the CRLs stored in the LDAP directory store if the CA certificate includes either the IssuingDistributionPoint or the CRLDistributionPoint extensions. Default: Enabled |
| **OCSP Validation** | When enabled, AM checks the revocation status of certificates using the Online Certificate Status Protocol (OCSP).  
The AM instance must have internet access, and you must configure OSCP for AM by going to Configure > Server Defaults > Security > Online Certificate Status Protocol Check. |
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
| LDAP Server Where Certificates are Stored    | Specifies the LDAP server that holds the certificates. Enter each server in the `ldap_server:port` format. AM servers can be associated with LDAP servers by writing multiple chains with the format `openam_server|ldapserver:port`. For example, `openam.example.com|ldap1.example.com:636`.
|                                             | To configure a secure connection, enable the Use SSL/TLS for LDAP Access property. |
| LDAP Search Start or Base DN                 | Valid base DN for the LDAP search, such as `dc=example,dc=com`. To associate AM servers with different search base DNs, use the format `am_server|base_dn`. For example, `openam.example.com|dc=example,dc=com` openam1.test.com|dc=test, `dc=com`.
| LDAP Server Authentication User              | Specifies the DN of the service account that AM will use to authenticate to the LDAP that holds the certificates. For example, `cn=LDAP User`. Default: `cn=Directory Manager` |
| LDAP Server Authentication Password          | Specifies the password of the user configured in the LDAP Server Authentication User property. |
| Use SSL/TLS for LDAP Access                  | Specifies whether AM should use SSL/TLS to access the LDAP. When enabled, AM must be able to trust the LDAP server certificate. Default: Disabled |

Example:

The following is an example of how to use the certificate nodes. Note that all the failure outcomes of the "Certificate Validation Node" are linked so that the user provides a username and password, but you could choose different authentication methods for each outcome.

Certificate User Extractor Node

This node extracts a value from the certificate collected by the "Certificate Collector Node", and searches for it in the identity store. The goal is to match the certificate with a user in the identity store.

The tree continues through the Extracted path if AM was able to match the certificate to a user in the identity store, and through the Not Extracted path otherwise.
The extracted value is stored in the `username` key in the shared state of the authentication tree.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Field Used to Access User Profile</td>
<td>Specifies the field in the certificate that AM will use to search for the user in the identity store. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Subject DN</td>
</tr>
<tr>
<td></td>
<td>• Subject CN</td>
</tr>
<tr>
<td></td>
<td>• Subject UID</td>
</tr>
<tr>
<td></td>
<td>• Email Address</td>
</tr>
<tr>
<td></td>
<td>• Other</td>
</tr>
<tr>
<td></td>
<td>• None</td>
</tr>
<tr>
<td></td>
<td>If you select Other, provide an attribute name in the Other Certificate Field Used to Access User Profile property.</td>
</tr>
<tr>
<td></td>
<td>Select None if you want to specify an alternate way of looking up the user profile in the SubjectAltNameExt Value Type to Access User Profile property.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>Other Certificate Field Used to Access User Profile</td>
<td>Specifies a custom certificate field to use as the base of the user search.</td>
</tr>
<tr>
<td>SubjectAltNameExt Value Type to Access User Profile</td>
<td>Specifies how to look up the user profile. Possible values are:</td>
</tr>
<tr>
<td></td>
<td>• None. AM uses the value specified in the Certificate Field Used to Access User Profile or the Other Certificate Field Used to Access User Profile properties when looking up the user profile.</td>
</tr>
<tr>
<td></td>
<td>• RFC822Name. AM looks up for the user profile using the value of the RFC822Name field.</td>
</tr>
<tr>
<td></td>
<td>• UPN. AM looks up the user profile as the User Principal Name attribute used in Active Directory.</td>
</tr>
<tr>
<td></td>
<td>Default: None</td>
</tr>
</tbody>
</table>

**Cookie Presence Decision Node**

The Cookie Presence Decision authentication node checks if a named cookie is present in the incoming authentication request.

Note that the node does not check the value of the named cookie, only that it exists.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of Cookie</td>
<td>Tree evaluation continues along the True path if the named cookie is present in the incoming authentication request. Otherwise, the tree evaluation continues along the False path.</td>
</tr>
</tbody>
</table>
Device Profile Collector

The Device Profile Collector authentication node gathers metadata about the device the user is authenticating with.

The Device Profile Collector authentication node sends a DeviceProfileCallback callback. For more information, see "Interactive Callbacks".

**Important**

The AM XUI user interface does not support completing the callback that this node uses.

Support for the callback this node uses is provided by:

- The ForgeRock SDKs.
- The Login UI component of the Platform UI.

When used with the ForgeRock SDKs, the node can collect the following:

**Device Metadata**

Information such as the platform, versions, device name, hardware information, and the brand of the device being used.

The captured data is in JSON format, and stored in the authentication tree's shared state, in a variable named forgeRock.device.metadata.

**Device Location**

Provides the last known latitude and longitude of the device's location.

The captured data is in JSON format, and stored in the authentication tree's shared state, in a variable named forgeRock.device.location.

**Important**

It is up to you what information you collect from users and devices.

You should always use data responsibly and provide your users appropriate control over data they share with you.

You are responsible for complying with any regulations or data protection laws.

Alongside the collected metadata, an identifier string in the JSON uniquely identifies the device.

Use this node alongside the "Device Profile Save" authentication node when you want to create a trusted profile from the collected data. The trusted device profile can be used in subsequent authentication attempts; for example, with the "Device Match" and "Device Profile Location Match" authentication nodes.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Profile Size (KB)</td>
<td>Specifies the maximum accepted size, in kilobytes, of a device profile. If the collected profile data exceeds this size, authentication fails.</td>
</tr>
<tr>
<td>Collect Device Metadata</td>
<td>Specifies whether device metadata is requested.</td>
</tr>
<tr>
<td>Collect Device Location</td>
<td>Specifies whether device location is requested.</td>
</tr>
<tr>
<td>Message</td>
<td>Specifies an optional message to display to the user while the node collects the requested data.</td>
</tr>
<tr>
<td></td>
<td>You can provide the message in multiple languages by specifying the locale in the KEY field, for example en-US. For information on valid locale strings, see JDK 11 Supported Locales. The locale selected for display is based on the user's locale settings in their browser. Messages provided in the node override the defaults provided by AM. For information about customizing and translating the default messages, see &quot;Internationalization&quot; in the Authentication Node Development Guide.</td>
</tr>
</tbody>
</table>

Device Match

The Device Match authentication node compares any collected device metadata with that stored in the user's profile.

Use this node alongside the "Device Profile Collector" authentication node to determine if the authenticating user is on a previously saved, trusted device.

You can choose between two methods of comparison:

1. Built-in Matching

   The node handles the comparison and matching, and you can configure the acceptable variance, and specify a time frame that profiles are considered current.

2. Custom Matching

   Create scripts to do the comparison of captured device data against trusted device profiles.

   AM includes a template script that you can customize to your requirements. Go to Realms > Realm Name > Scripts, and then click Device Match Template - Decision Node Script.

   ForgeRock also provides a more complete sample script, as well as instructions for its use, and a development toolkit. Find these resources on GitHub, at: https://github.com/ForgeRock/forgerock-device-match-script.

You must establish the identity of the user in the tree before attempting to match device profiles.
Tree evaluation continues along the **True** path if the collected device profile matches a saved profile, within the configured variance; otherwise, tree evaluation continues along the **False** path.

If the user has no trusted device profiles, or the identity of the user has not been established, tree evaluation continues along the **Unknown Device** path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Acceptable Variance</td>
<td>Specify the maximum amount of device attribute differences that is still acceptable for a match.</td>
</tr>
<tr>
<td>Expiration</td>
<td>Specify the maximum age, in the number of days since being saved, that existing profiles can be considered for comparison. Device profiles that were saved to the user's profile before this time will not be compared to the collected metadata.</td>
</tr>
<tr>
<td>Use Custom Matching Script</td>
<td>Specifies whether to use a custom script to compare the collected metadata with saved device profiles. The script type has to be <em>Decision node script for authentication trees</em>. Note When a custom matching script is used, the Acceptable Variance and Expiration properties are ignored.</td>
</tr>
<tr>
<td>Custom Matching Script</td>
<td>Specifies the custom script to use if the Use Custom Matching Script property is enabled. Only scripts of type <em>Decision node script for authentication trees</em> appear in the list.</td>
</tr>
</tbody>
</table>

**Device Profile Save**

The Device Profile Save authentication node persists collected device data to a user's profile in the identity store.

Use this node alongside the "Device Profile Collector" authentication node when you want to reuse the collected data in future authentications; for example, with the "Device Match" and "Device Profile Location Match" authentication nodes.

You must establish the identity of the user in the tree before attempting to save to their profile.

A user profile can contain multiple device profiles. Use the Maximum Saved Profiles property to configure the maximum number of device profiles to persist per user. Saving a device profile with the same identifier as an existing entry overwrites the original record, and does not increment the device profile count.

The **user UI** component of the platform UI displays saved device profiles to end users. Note that the Access Management UI **does not** display saved device profiles to end users.

You can manage device profiles with REST, by using the `/json/users/user/devices/profile` endpoint.
Use the AM API Explorer for detailed information about the parameters supported by the `/devices/profile` endpoint, and to test it against your deployed AM instance.

In the AM console, select the Help icon, and then navigate to API Explorer > `/users` > `/{user}` > `/devices` > `/profile`.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name Variable</td>
<td>Specifies the name of a variable in the authentication tree's shared state that contains an alias label for the device profile.</td>
</tr>
<tr>
<td>Maximum Saved Profiles</td>
<td>Specify the maximum number of device profiles to save in a user's profile. When the maximum is reached, saving a new device profile replaces the oldest record.</td>
</tr>
<tr>
<td>Save Device Metadata</td>
<td>Specifies whether device metadata is saved to the user's profile.</td>
</tr>
<tr>
<td>Save Device Location</td>
<td>Specifies whether device location metadata is saved to the user's profile.</td>
</tr>
</tbody>
</table>

Device Profile Location Match

The Device Profile Location Match authentication node compares any collected device location metadata with that stored in the user's profile.

Use this node alongside the "Device Profile Collector" authentication node to determine if the authenticating user's device is located within range of somewhere they have authenticated from, and saved, previously.

You must establish the identity of the user in the tree before attempting to match locations.

Tree evaluation continues along the **True** path if the collected location is within the specified range of saved location data; otherwise, tree evaluation continues along the **False** path.

If the user has no saved device profiles, or the identity of the user has not been established, tree evaluation continues along the **Unknown Device** path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Radius (km)</td>
<td>Specifies the maximum distance, in kilometers, that a device can be from a previously saved location.</td>
</tr>
<tr>
<td></td>
<td>The distance is calculated point-to-point.</td>
</tr>
</tbody>
</table>

Device Geofencing

The Device Geofencing authentication node compares any collected device location metadata with the trusted locations configured in the authentication node.
Use this node alongside the "Device Profile Collector" authentication node to determine if the authenticating user's device is located within range of configured, trusted locations.

Tree evaluation continues along the **Inside** path if the collected location is within the specified range of a configured trusted location; otherwise, tree evaluation continues along the **Outside** path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trusted Locations</td>
<td>Specify the latitude and longitude of at least one trusted location. Separate the values with a comma; for example, 37.7910855,-122.3951663.</td>
</tr>
<tr>
<td>Geofence Radius (km)</td>
<td>Specifies the maximum distance, in kilometers, that a device can be from a configured trusted location. The distance is calculated point-to-point.</td>
</tr>
</tbody>
</table>

**Device Tampering Verification**

The Device Tampering Verification authentication node specifies a threshold for deciding if the device has been tampered with; for example, if it has been rooted or jailbroken.

A score between zero and one is returned by the device, based on the likelihood that is has been tampered with or may pose a security risk. For example, an emulator scores the maximum of 1.

Use this node alongside the "Device Profile Collector" authentication node to retrieve the tampering score from the device.

Tree evaluation continues along the **Not Tampered** path if the device scores less than or equal to the configured threshold, otherwise tree evaluation continues along the **Tampered** path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Score Threshold</td>
<td>Specifies the score threshold for determining if a device has been tampered with. Enter a decimal fraction, between 0 and 1; for example, 0.75. The higher the score returned from the device, the more likely the device is jailbroken, rooted, or is a potential security risk.</td>
</tr>
</tbody>
</table>

**Note**

Emulators score the maximum; 1.

**Persistent Cookie Decision Node**

The Persistent Cookie Decision authentication node checks for the existence of the persistent cookie specified in the Persistent cookie name property, the default being `session-jwt`. 
If the cookie is present, the node verifies the signature of the JWT stored in the cookie by using the signing key specified in the HMAC signing key property.

If the signature is valid, the node will decrypt the payload of the JWT by using the key pair specified in the Persistent Cookie Encryption Certificate Alias property. This property can be found at the global level by navigating to Configure > Authentication > Core Attributes > Security, or at the realm level by navigating to Realms > Realm Name > Authentication > Settings > Security.

Within the decrypted JSON payload is information such as the UID of the identity, and the client IP address. Enable the Enforce client IP property to verify that the current IP address and the client IP address in the cookie are identical.

**Note**

The Persistent Cookie Decision authentication node recreates the received persistent cookie, updating the value for the idle time property. Therefore, cookie creation properties as used by the Set Persistent Cookie Node are also available in the Persistent Cookie Decision authentication node.

Tree evaluation continues along the True outcome path if the persistent cookie is present and all the verification checks above are satisfied. Otherwise, tree evaluation continues along the False outcome path.

Properties:
### Property | Usage
--- | ---
**Idle Timeout** | Specifies the maximum amount of idle time allowed before the persistent cookie is invalidated, in hours. If no requests are received and the time is exceeded, the cookie is no longer valid.

**Enforce Client IP** | When enabled, ensures that the persistent cookie is only used from the same client IP to which the cookie was issued.

**Use secure cookie** | When enabled, adds the `Secure` flag to the persistent cookie.

If the `Secure` flag is included, the cookie can only be transferred over HTTPS. When a request is made over HTTP, the cookie is not made available to the application.

**Use HTTP only cookie** | When enabled, adds the `HttpOnly` flag to the persistent cookie.

When the `HttpOnly` flag is included, that cookie will not be accessible through JavaScript. According to RFC 6265, the `HttpOnly` flag:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>instructs the user agent to omit the cookie when providing access to cookies via 'non-HTTP' APIs (for example, a web browser API that exposes cookies to scripts).</td>
</tr>
<tr>
<td>HMAC Signing Key</td>
<td>Specifies a key to use for HMAC signing of the persistent cookie. Values must be base64-encoded and at least 256 bits (32 bytes) long.</td>
</tr>
<tr>
<td></td>
<td><strong>Important</strong></td>
</tr>
<tr>
<td></td>
<td>To consume the persistent cookies generated by instances of the Set Persistent Cookie Node in the tree, ensure they are using the same HMAC signing key.</td>
</tr>
<tr>
<td></td>
<td>To generate an HMAC signing key, run one of the following commands:</td>
</tr>
<tr>
<td></td>
<td>$ openssl rand -base64 32</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td></td>
<td>$ cat /dev/urandom</td>
</tr>
<tr>
<td>Persistent cookie name</td>
<td>Specifies the name of the persistent cookie to check.</td>
</tr>
</tbody>
</table>

Example:

**PersistentCookie Tree**

Set Persistent Cookie Node

The Set Persistent Cookie authentication node creates a persistent cookie named after the value specified in the Persistent cookie name property, the default being `session-jwt`.

The cookie contains a JWT, inside which there is a JSON payload with information such as the UID of the identity, and the client IP address.
The node encrypts the JWT using the key pair specified in the Persistent Cookie Encryption Certificate Alias property. This property can be found by navigating to Configure > Authentication > Core Attributes > Security.

The node signs the cookie with the signing key specified in the HMAC signing key property. Any node that will read the persistent cookie must be configured with the same HMAC signing key.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Idle Timeout</td>
<td>Specifies the maximum amount of idle time allowed before the persistent cookie is invalidated, in hours. If no requests are received and the time is exceeded, the cookie is no longer valid.</td>
</tr>
<tr>
<td>Max life</td>
<td>Specifies the length of time the persistent cookie remains valid, in hours. If that time is exceeded, the cookie is no longer valid.</td>
</tr>
<tr>
<td>Use Secure Cookie</td>
<td>When enabled, adds the Secure flag to the persistent cookie.</td>
</tr>
</tbody>
</table>
### Property | Usage
--- | ---
Secure | If the Secure flag is included, the cookie can only be transferred over HTTPS. When a request is made over HTTP, the cookie is not made available to the application.

Use HTTP Only Cookie | When enabled, adds the HttpOnly flag to the persistent cookie.

When the HttpOnly flag is included, that cookie will not be accessible through JavaScript. According to RFC 6265, the HttpOnly flag:

> instructs the user agent to omit the cookie when providing access to cookies via 'non-HTTP' APIs (for example, a web browser API that exposes cookies to scripts).

HMAC Signing Key | Specifies a key to use for HMAC signing of the persistent cookie. Values must be base64-encoded and at least 256 bits (32 bytes) long.

**Important**

To consume the persistent cookies generated by instances of the Set Persistent Cookie Node in the tree, ensure they are using the same HMAC signing key.

To generate an HMAC signing key, run one of the following commands:

```
$ openssl rand -base64 32
```

or

```
$ cat /dev/urandom | LC_ALL=C tr -dc 'a-zA-Z0-9' | fold -w 32 | head -n 1| base64
```

Persistent Cookie Name | Specifies the name used for the persistent cookie.

---

**Federation Authentication Nodes**

Use the following nodes to configure trees with federation capabilities, such as OAuth 2.0, social authentication, and account provisioning:

**OAuth 2.0 Node**

The OAuth 2.0 authentication node lets AM authenticate users of OAuth 2.0-compliant resource servers. References in this section are to RFC 6749, The OAuth 2.0 Authorization Framework.

Tree evaluation continues along the Account Exists path if an account matching the attributes retrieved from the social identity provider is found in the user data store. Otherwise, the tree evaluation continues along the No account exists path.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Specifies the <code>client_id</code> parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Specifies the <code>client_secret</code> parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td>Authentication Endpoint URL</td>
<td>Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Example: <code>https://accounts.google.com/o/oauth2/v2/auth</code></td>
</tr>
<tr>
<td>Access Token Endpoint URL</td>
<td>Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>User Profile Service URL</strong></td>
<td>Specifies the user profile URL that returns profile information.</td>
</tr>
<tr>
<td>Example:</td>
<td><a href="https://www.googleapis.com/oauth2/v4/token">https://www.googleapis.com/oauth2/v4/token</a></td>
</tr>
<tr>
<td><strong>OAuth Scope</strong></td>
<td>Specifies a list of user profile attributes that the client application requires, according to <em>The OAuth 2.0 Authorization Framework (RFC 6749)</em>. Ensure you use the correct scope delimiter as required by the identity provider, for example commas or spaces.</td>
</tr>
<tr>
<td>Example:</td>
<td><a href="https://www.googleapis.com/oauth2/v3/userinfo">https://www.googleapis.com/oauth2/v3/userinfo</a></td>
</tr>
<tr>
<td><strong>Scope Delimiter</strong></td>
<td>Specifies the delimiter used to separate scope values.</td>
</tr>
<tr>
<td>Example:</td>
<td>Some authorization servers use non-standard separators for scopes, for example commas.</td>
</tr>
<tr>
<td><strong>Redirect URL</strong></td>
<td>Specifies the URL the user is redirected to by the social identity provider after authenticating.</td>
</tr>
<tr>
<td>Example:</td>
<td>For authentication trees in AM, set this property to the URL of the UI. For example, <a href="https://openam.example.com:8443/openam/XUI/">https://openam.example.com:8443/openam/XUI/</a>.</td>
</tr>
<tr>
<td><strong>Social Provider</strong></td>
<td>Specifies the name of the social provider for which this module is being set up.</td>
</tr>
<tr>
<td>Example:</td>
<td>Google</td>
</tr>
<tr>
<td><strong>Auth ID Key</strong></td>
<td>Specifies the attribute the social identity provider uses to identify an authenticated individual.</td>
</tr>
<tr>
<td>Example:</td>
<td>id</td>
</tr>
<tr>
<td><strong>Use Basic Auth</strong></td>
<td>Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.</td>
</tr>
<tr>
<td>Default:</td>
<td>true</td>
</tr>
<tr>
<td><strong>Account Provider</strong></td>
<td>Specifies the name of the class that implements the account provider.</td>
</tr>
<tr>
<td>Default:</td>
<td>org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider</td>
</tr>
<tr>
<td><strong>Account Mapper</strong></td>
<td>Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from the social identity provider.</td>
</tr>
<tr>
<td>Provided implementations are:</td>
<td>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</td>
</tr>
<tr>
<td>The Account Mapper classes can take two constructor parameters: a comma-separated list of attributes and a prefix to apply to their values. For example, to prefix all received property values with facebook- before searching, specify:</td>
<td></td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Attribute Mapper              | Specifies the list of fully qualified class names for implementations that map attributes from the OAuth 2.0 authorization server to AM profile attributes. Provided implementations are: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper *
|                               | *facebook-                                                                                                                                 |
| Account Mapper Configuration  | Specifies the attribute configuration used to map the account of the user authenticated in the OAuth 2.0 provider to the local data store in AM. Valid values are in the form provider-attr=local-attr. Examples: email=mail and id=facebook-id. |
|                               | **Tip** When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation. For example, given a JSON payload of: |
|                               | `{  
|                               | "sub" : "12345",  
|                               | "name" : {  
|                               | "first_name" : "Demo",  
|                               | "last_name" : "User"  
|                               | }  
<p>|                               | You can create a mapper such as: name.first_name=cn                                                                                                                                 |
| Attribute Mapper Configuration| Map of OAuth 2.0 provider user account attributes to local user profile attributes, with values in the form provider-attr=local-attr. Examples: first_name=givenname, last_name=sn, name=cn, email=mail, id=facebook-id, first_name=facebook-fname, last_name=facebook-lname, email=facebook-email. |</p>
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Tip</strong></td>
<td>When using the <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</code> class, you can parse JSON objects in mappings, by using dot notation. For example, given a JSON payload of:</td>
</tr>
</tbody>
</table>
|                                | `{  
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}`                                                                                                                                                                                                                                                                          |
|                                | You can create a mapper such as:                                                                                                                                                                                                                                                                                                       |
|                                | `name.first_name=cn`                                                                                                                                                                                                                                                                                                                  |
| Save attributes in the session | When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.                                                                                                                                                                                                                                     |
| OAuth 2.0 Mix-Up Mitigation Enabled | Controls whether the OAuth 2.0 authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter. The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (`iss`) that will be validated by the client. |
| Note                           | Consult with the authorization server's documentation on what value it uses for the issuer field.                                                                                                                                                                                                                                     |
|                                | For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.                                                                                                                                                                                                                                                              |
| Token Issuer                   | Corresponds to the expected issuer identifier value in the `iss` field of the ID token.                                                                                                                                                                                                                                              |
|                                | Example: `https://accounts.google.com`                                                                                                                                                                                                                                                                                               |
OpenID Connect Node

The OpenID Connect authentication node lets AM authenticate users of OpenID Connect-compliant resource servers. As OpenID Connect is an additional layer on top of OAuth 2.0, many references in this section are to RFC 6749, The OAuth 2.0 Authorization Framework. OpenID Connect-specific references are to the OpenID Connect Core 1.0 incorporating errata set 1 specification.

Tree evaluation continues along the Account Exists path if an account matching the attributes retrieved from the OpenID Connect identity provider is found in the identity store. Otherwise, the tree evaluation continues along the No account exists path.

The OpenID Connect node implements the "Authorization Code Grant" flow.

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Specifies the <code>client_id</code> parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Specifies the <code>client_secret</code> parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td>Authentication Endpoint URL</td>
<td>Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> <a href="https://accounts.google.com/o/oauth2/v2/auth">https://accounts.google.com/o/oauth2/v2/auth</a></td>
</tr>
<tr>
<td>Access Token Endpoint URL</td>
<td>Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Profile Service URL</td>
<td>Specifies the user profile URL that returns profile information.</td>
</tr>
<tr>
<td></td>
<td>If not specified, attributes are mapped from the claims returned by the id_token, and no call to a user profile endpoint is made.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://www.googleapis.com/oauth2/v4/token">https://www.googleapis.com/oauth2/v4/token</a></td>
</tr>
<tr>
<td>OAuth Scope</td>
<td>Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). Ensure you use the correct scope delimiter as required by the identity provider, for example commas or spaces. The list depends on the permissions that the resource owner, such as the end user, grants to the client application.</td>
</tr>
<tr>
<td></td>
<td>Example: <a href="https://www.googleapis.com/oauth2/v3/userinfo">https://www.googleapis.com/oauth2/v3/userinfo</a></td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Specifies the URL the user is redirected to by the social identity provider after authenticating. For authentication trees in AM, set this property to the URL of the UI. For example <a href="https://openam.example.com:8443/openam/XUI/">https://openam.example.com:8443/openam/XUI/</a>.</td>
</tr>
<tr>
<td>Social Provider</td>
<td>Specifies the name of the OpenID Connect provider for which this node is being set up. Example: Google</td>
</tr>
<tr>
<td>Auth ID Key</td>
<td>Specifies the attribute the social identity provider uses to identify an authenticated individual. Example: sub</td>
</tr>
<tr>
<td>Use Basic Auth</td>
<td>Specifies that the client uses HTTP Basic authentication when authenticating to the social provider. Default: true</td>
</tr>
<tr>
<td>Account Provider</td>
<td>Specifies the name of the class that implements the account provider. Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider</td>
</tr>
<tr>
<td>Account Mapper</td>
<td>Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from the social identity provider. The provided implementations is org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper. The Account Mapper classes can take two constructor parameters: a comma-separated list of attributes and a prefix to apply to their values. For example, to prefix all received property values with openid- before searching, specify: org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Attribute Mapper</td>
<td>Specifies the list of fully qualified class names for implementations that map attributes from the authorization server to AM profile attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Account Mapper Configuration</td>
<td>Specifies the attribute configuration used to map the account of the user authenticated in the provider to the local identity store in AM.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Attribute Mapper Configuration</td>
<td>Specifies how to map provider user attributes to local user profile attributes.</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>Examples</td>
<td></td>
</tr>
</tbody>
</table>
|                                  |                                                                                                                                         | ```first_name=givenname
  last_name=sn
  name=cn
  email=mail
  id=facebook-id
  first_name=facebook-fname
  last_name=facebook-lname
  email=facebook-email```                                                                                                                          |
| Save attributes in the session   | When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.                                                                                                        |                                                                                                                                               |
| OAuth 2.0 Mix-Up Mitigation Enabled | Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server.                                                      | Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the `iss` response.                                        |
The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (iss) that will be validated by the client.

**Note**
Consult with the authorization server's documentation on what value it uses for the issuer field.

For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Token Issuer</strong></td>
<td>Corresponds to the expected issuer identifier value in the iss field of the ID token.</td>
</tr>
<tr>
<td>Example:</td>
<td><a href="https://accounts.google.com">https://accounts.google.com</a></td>
</tr>
<tr>
<td><strong>OpenID Connect Validation Type</strong></td>
<td>Specifies how to validate the ID token received from the OpenID Connect provider. AM ignores keys specified in JWT headers, such as jku and jwe; the following options are available to validate an incoming OpenID Connect ID token:</td>
</tr>
<tr>
<td><strong>Well Known URL (Default)</strong></td>
<td>Retrieves the provider's keys based on the information provided in its OpenID Connect configuration URL.</td>
</tr>
<tr>
<td>Specify the provider's configuration URL in the OpenID Connect Validation Value field, for example <a href="https://accounts.google.com/.well-known/openid-configuration">https://accounts.google.com/.well-known/openid-configuration</a>.</td>
<td></td>
</tr>
<tr>
<td><strong>Client Secret</strong></td>
<td>Validates the ID token signature with a specified client secret key.</td>
</tr>
<tr>
<td>Specify the key to use in the OpenID Connect Validation Value field.</td>
<td></td>
</tr>
<tr>
<td><strong>JWK URL</strong></td>
<td>Retrieve the necessary JSON web key from the URL that you specify.</td>
</tr>
<tr>
<td>Specify the provider's JWK URI in the OpenID Connect Validation Value field, for example <a href="https://www.googleapis.com/oauth2/v3/certs">https://www.googleapis.com/oauth2/v3/certs</a>.</td>
<td></td>
</tr>
<tr>
<td><strong>OpenID Connect Validation Value</strong></td>
<td>Provide the URL or secret key used to verify an incoming ID token, depending on the value selected in the OpenID Connect Validation Type property.</td>
</tr>
</tbody>
</table>
Provision Dynamic Account Node

The Provision Dynamic Account node provisions an account following successful authentication by a social identity provider node, or a SAML2 authentication node. Accounts are provisioned using properties defined in the attribute mapper configuration of a social authentication or SAML2 authentication node earlier in the tree evaluation; for example, the OAuth 2.0 Node.

If a password has been acquired from the user, for example by using the Create Password Node, it is used when provisioning the account. Otherwise, a 20 character random string is used.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Provider</td>
<td>Specifies the name of the class that implements the account provider. Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider</td>
</tr>
</tbody>
</table>

Example:

The following example uses the Provision Dynamic Account authentication node to allow users who have performed social authentication using Google to provide a password and provision an account, if they do not have a matching existing profile. They must enter a one-time password to verify they are the owner of the Google account.
Provision IDM Account Node

The Provision IDM Account node redirects users to an IDM instance to provision an account.

Ensure you have configured the details of the IDM instance in AM, by navigating to Configure > Global Services > IDM Provisioning.

For information on using IDM for provisioning, see the Platform Setup Guide.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Account Provider</td>
<td>Specifies the name of the class that implements the account provider.</td>
</tr>
<tr>
<td>Default:</td>
<td>org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider</td>
</tr>
</tbody>
</table>
Example:

The following example uses the Provision IDM Account authentication node to allow users who have performed social authentication using Facebook to provision an account using IDM, if they do not have a matching existing profile.

*Facebook-ProvisionIDMAccount Tree With Provision IDM Account Node*

SAML2 Authentication Node

This node lets you integrate SAML v2.0 SSO into an AM authentication tree. Use it when deploying SAML v2.0 single sign-on in integrated mode (SP-initiated SSO only).

**Important**

SLO is not supported, even though the UI has an option to enable it.

If a user account is found that matches the federated account, tree evaluation continues along the "Account Exists" outcome. Otherwise, a matching account could not be found, and tree evaluation continues along the "No Account Exists" outcome.

You can dynamically provision an account on the SP if it does not exist, or you can link the remote account to a local account, as described in the example below.

Before attempting to configure a SAML2 authentication node, ensure that:

- You have configured a remote IdP and a hosted SP in a CoT in the same realm where the authentication node will be configured.

- The SP is configured for integrated mode. See "Implementing SSO in Integrated Mode (Chains)" in the SAML v2.0 Guide.

**Properties:**
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>IdP Entity ID</td>
<td>Specifies the name of the remote IdP.</td>
</tr>
<tr>
<td>SP MetaAlias</td>
<td>Specifies the local alias for the SP, in the format /Realm Name/SP Name.</td>
</tr>
<tr>
<td>Allow IdP to Create NameID</td>
<td>Specifies whether the IdP should create a new identifier for the authenticating user if none exists. For detailed information, see the section on the AllowCreate property in SAML Version 2.0 Errata 05. Default: Enabled</td>
</tr>
<tr>
<td>Comparison Type</td>
<td>Specifies a comparison method to evaluate authentication context classes or statements. The value specified in this property overrides the value set in the SP</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>configuration under Realms &gt; Realm Name &gt; Applications &gt; Federation &gt; Entity Providers &gt; Service Provider Name &gt; Assertion Content &gt; Authentication Context &gt; Comparison Type.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid comparison methods are</strong> exact, minimum, maximum, or better.</td>
</tr>
<tr>
<td></td>
<td>For more information about the comparison methods, see the section on the <code>&lt;RequestedAuthnContext&gt;</code> element in Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.</td>
</tr>
<tr>
<td>Authentication Context Class Reference</td>
<td>(Optional) Specifies one or more URIs for authentication context classes to be included in the SAML request.</td>
</tr>
<tr>
<td></td>
<td>+ <strong>What Are Authentication Context Classes?</strong></td>
</tr>
<tr>
<td></td>
<td>They are unique identifiers for an authentication mechanism. The SAML v2.0 protocol supports a standard set of authentication context classes, defined in Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0. In addition to the standard authentication context classes, you can specify customized authentication context classes.</td>
</tr>
<tr>
<td></td>
<td>Any authentication context class that you specify in this field must be supported for the service provider.</td>
</tr>
<tr>
<td></td>
<td>+ <strong>Where Can I Find This Information?</strong></td>
</tr>
<tr>
<td></td>
<td>Go to Realms &gt; Realm Name &gt; Applications &gt; Federation &gt; Entity Providers &gt; Service Provider Name &gt; Assertion Content &gt; Authentication Context.</td>
</tr>
</tbody>
</table>

When specifying multiple authentication context classes, use the | character to separate the classes. For example:
### Property

### Usage

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Context Declaration Reference</td>
<td>(Optional) Specifies one or more URIs that identify authentication context declarations. When specifying multiple URIs, use the</td>
</tr>
<tr>
<td>Request Binding</td>
<td>Specifies the format the SP will use to send the authentication request to the IdP. Valid values are <code>&lt;HTTP-Redirect&gt;</code> and <code>&lt;HTTP-POST&gt;</code>. Default: <code>HTTP-Redirect</code></td>
</tr>
<tr>
<td>Response Binding</td>
<td>Specifies the format the IdP will use to send the response to the SP. Valid values are <code>&lt;HTTP-POST&gt;</code> and <code>&lt;HTTP-Artifact&gt;</code>. Default: <code>HTTP-Artifact</code></td>
</tr>
<tr>
<td>Force IdP Authentication</td>
<td>Specifies whether the IdP forces authentication or if it can reuse existing security contexts. Default: Disabled</td>
</tr>
<tr>
<td>Passive Authentication</td>
<td>Specifies whether the IdP uses passive authentication or not. Passive authentication requires the IDP to only use authentication methods that do not require user interaction. For example, authenticating using an X.509 certificate. Default: Disabled</td>
</tr>
<tr>
<td>Single Logout Enabled</td>
<td>Not implemented.</td>
</tr>
<tr>
<td>Single Logout URL</td>
<td>Not implemented.</td>
</tr>
</tbody>
</table>

### Example:

The following example federates to a remote IdP, and dynamically provisions an account for the user in the SP if one does not exist:
Example Tree With SAML2 Authentication Node

To create a persistent link with an existing account in the SP, see the "Write Federation Information Node".

Social Facebook Node

The Social Facebook authentication node is a duplicate of the OAuth 2.0 Node node, preconfigured to work with Facebook. Only the Client ID and Client Secret are required to be populated.

Tree evaluation continues along the Account Exists path if an account matching the attributes retrieved from Facebook are found in the user data store. Otherwise, the tree evaluation continues along the No account exists path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Specifies the client_id parameter as provided by Facebook.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Specifies the client_secret parameter as provided by Facebook.</td>
</tr>
<tr>
<td>Authentication Endpoint URL</td>
<td>Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: <a href="https://www.facebook.com/dialog/oauth">https://www.facebook.com/dialog/oauth</a></td>
</tr>
<tr>
<td>Access Token Endpoint URL</td>
<td>Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: <a href="https://graph.facebook.com/v2.12/oauth/access_token">https://graph.facebook.com/v2.12/oauth/access_token</a></td>
</tr>
<tr>
<td>User Profile Service URL</td>
<td>Specifies the user profile URL that returns profile information.</td>
</tr>
<tr>
<td></td>
<td>Default: <a href="https://graph.facebook.com/v2.6/me?fields=name%2Cemail%2Cfirst_name%2Clast_name">https://graph.facebook.com/v2.6/me?fields=name%2Cemail%2Cfirst_name%2Clast_name</a></td>
</tr>
<tr>
<td>OAuth Scope</td>
<td>Specifies a comma-separated list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.</td>
</tr>
</tbody>
</table>
### Property | Usage
--- | ---
**Redirect URL** | Specifies the URL the user is redirected to by Facebook after authenticating, to continue the authentication tree flow.

Set this property to the URL of the AM UI. For example, `https://openam.example.com:8443/openam/XUI/`.

**Tip**

If the tree is not in the Top Level Realm, you can specify the realm in the redirect URL. Use a DNS alias for the realm, or add the realm as a query parameter, for example `https://openam.example.com:8443/openam/XUI/?realm=\mySubRealm`.

For more information, see "To Configure DNS Aliases for Accessing a Realm" in the Setup Guide.

**Social Provider** | Specifies the name of the social provider for which this node is being set up.

Default: facebook

**Auth ID Key** | Specifies the attribute the social identity provider uses to identify an authenticated individual.

Default: id

**Use Basic Auth** | Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.

Default: true

**Account Provider** | Specifies the name of the class that implements the account provider.

Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider

**Account Mapper** | Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from Facebook.

Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper

**Attribute Mapper** | Specifies the list of fully qualified class names for implementations that map attributes from Facebook to AM profile attributes.

Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|facebook-

**Account Mapper Configuration** | Specifies the attribute configuration used to map the account of the user authenticated in the Social Facebook provider to the local data store in AM. Valid values are in the form `provider-attr=local-attr`. 
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td><strong>Default:</strong> <code>id=uid</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong></td>
</tr>
<tr>
<td></td>
<td>When using the <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</code> class, you can parse JSON objects in mappings, by using dot notation.</td>
</tr>
<tr>
<td></td>
<td>For example, given a JSON payload of:</td>
</tr>
<tr>
<td></td>
<td>`{</td>
</tr>
<tr>
<td></td>
<td>&quot;sub&quot; : &quot;12345&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;name&quot; : {</td>
</tr>
<tr>
<td></td>
<td>&quot;first_name&quot; : &quot;Demo&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;last_name&quot; : &quot;User&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>You can create a mapper such as:</td>
</tr>
<tr>
<td></td>
<td><code>name.first_name=cn</code></td>
</tr>
<tr>
<td>Attribute Mapper</td>
<td><strong>Map of Facebook user account attributes to local user profile attributes, with values in the form <code>provider-attr=local-attr</code>.</strong></td>
</tr>
<tr>
<td>Configuration</td>
<td><strong>Default:</strong> <code>name=cn, last_name=sn, id=uid, first_name=givenname, email=mail</code>.</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong></td>
</tr>
<tr>
<td></td>
<td>When using the <code>org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</code> class, you can parse JSON objects in mappings, by using dot notation.</td>
</tr>
<tr>
<td></td>
<td>For example, given a JSON payload of:</td>
</tr>
<tr>
<td></td>
<td>`{</td>
</tr>
<tr>
<td></td>
<td>&quot;sub&quot; : &quot;12345&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;name&quot; : {</td>
</tr>
<tr>
<td></td>
<td>&quot;first_name&quot; : &quot;Demo&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;last_name&quot; : &quot;User&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>You can create a mapper such as:</td>
</tr>
<tr>
<td></td>
<td><code>name.first_name=cn</code></td>
</tr>
<tr>
<td>Save attributes in the</td>
<td><strong>When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.</strong></td>
</tr>
<tr>
<td>session</td>
<td><strong>Default:</strong> <code>true</code>.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>OAuth 2.0 Mix-Up Mitigation Enabled</td>
<td>Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server. Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the <code>iss</code> response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server’s response is intended for the client by comparing the client's client identifier to the value of the <code>client_id</code> response parameter. The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (iss) that will be validated by the client. Note Consult with the authorization server's documentation on what value it uses for the issuer field. For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.</td>
</tr>
<tr>
<td><strong>Token Issuer</strong></td>
<td>Corresponds to the expected issuer identifier value in the <code>iss</code> field of the ID token. Example: <a href="https://graph.facebook.com">https://graph.facebook.com</a></td>
</tr>
</tbody>
</table>

Example:

The following example uses the Provision IDM Account authentication node to allow users who have performed social authentication using Facebook to provision an account using IDM, if they do not have a matching existing profile.

**Facebook-ProvisionIDMAccount Tree With Provision IDM Account Node**

![Diagram of Facebook-ProvisionIDMAccount Tree With Provision IDM Account Node](image)

**Social Google Node**

The Social Google authentication node is a duplicate of the OAuth 2.0 Node node, preconfigured to work with Google. Only the **Client ID** and **Client Secret** are required to be populated.
Tree evaluation continues along the **Account Exists** path if an account matching the attributes retrieved from Google are found in the user data store. Otherwise, the tree evaluation continues along the **No account exists** path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client ID</td>
<td>Specifies the <code>client_id</code> parameter as provided by Google.</td>
</tr>
<tr>
<td>Client Secret</td>
<td>Specifies the <code>client_secret</code> parameter as provided by Google.</td>
</tr>
<tr>
<td>Authentication Endpoint URL</td>
<td>Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: <code>https://accounts.google.com/o/oauth2/v2/auth</code></td>
</tr>
<tr>
<td>Access Token Endpoint URL</td>
<td>Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749). Default: <code>https://www.googleapis.com/oauth2/v4/token</code></td>
</tr>
<tr>
<td>User Profile Service URL</td>
<td>Specifies the user profile URL that returns profile information.</td>
</tr>
<tr>
<td></td>
<td>Default: <code>https://www.googleapis.com/oauth2/v3/userinfo</code></td>
</tr>
<tr>
<td>OAuth Scope</td>
<td>Specifies a space-separated list of user profile attributes that the client application requires, according to <em>The OAuth 2.0 Authorization Framework (RFC 6749)</em>. The list depends on the permissions that the resource owner, such as the end user, grants to the client application. Default: <code>profile email</code>.</td>
</tr>
<tr>
<td>Redirect URL</td>
<td>Specifies the URL the user is redirected to by Google after authenticating, to continue the authentication tree flow.</td>
</tr>
<tr>
<td></td>
<td>Set this property to the URL of the AM UI. For example, <code>https://openam.example.com:8443/openam/XUI/</code>.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>If the tree is not in the Top Level Realm, you can specify the realm in the redirect URL. Use a DNS alias for the realm, or add the realm as a query parameter, for example <code>https://openam.example.com:8443/openam/XUI/?realm=mySubRealm</code>. For more information, see &quot;To Configure DNS Aliases for Accessing a Realm&quot; in the Setup Guide.</td>
</tr>
<tr>
<td>Social Provider</td>
<td>Specifies the name of the social provider for which this node is being set up.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default: google</td>
<td></td>
</tr>
<tr>
<td>Auth ID Key</td>
<td>Specifies the attribute the social identity provider uses to identify an authenticated individual.</td>
</tr>
<tr>
<td>Default: sub</td>
<td></td>
</tr>
<tr>
<td>Use Basic Auth</td>
<td>Specifies that the client uses HTTP Basic authentication when authenticating to Google.</td>
</tr>
<tr>
<td>Default: true</td>
<td></td>
</tr>
<tr>
<td>Account Provider</td>
<td>Specifies the name of the class that implements the account provider.</td>
</tr>
<tr>
<td>Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider</td>
<td></td>
</tr>
<tr>
<td>Account Mapper</td>
<td>Specifies the name of the class that implements the method of locating local accounts based on the attributes returned from Google.</td>
</tr>
<tr>
<td>Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</td>
<td></td>
</tr>
<tr>
<td>Attribute Mapper</td>
<td>Specifies the list of fully qualified class names for implementations that map attributes from Google to AM profile attributes.</td>
</tr>
<tr>
<td>Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper</td>
<td>iplanet-am-user-alias-list</td>
</tr>
<tr>
<td>Account Mapper Configuration</td>
<td>Specifies the attribute configuration used to map the account of the user authenticated in the Social Google provider to the local data store in AM. Valid values are in the form provider-attr=local-attr.</td>
</tr>
<tr>
<td>Default: sub=uid</td>
<td></td>
</tr>
</tbody>
</table>

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:
## Property Usage

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute Mapper Configuration</strong></td>
<td>Map of Google user account attributes to local user profile attributes, with values in the form <code>provider-attr=local-attr</code>.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td><code>sub=uid, name=cn, given_name=givenName, family_name=sn, email=email.</code></td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation.</td>
</tr>
<tr>
<td></td>
<td>For example, given a JSON payload of:</td>
</tr>
<tr>
<td></td>
<td>`{</td>
</tr>
<tr>
<td></td>
<td>&quot;sub&quot; : &quot;12345&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;name&quot; : {</td>
</tr>
<tr>
<td></td>
<td>&quot;first_name&quot; : &quot;Demo&quot;,</td>
</tr>
<tr>
<td></td>
<td>&quot;last_name&quot; : &quot;User&quot;</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>You can create a mapper such as:</td>
</tr>
<tr>
<td></td>
<td><code>name.first_name=cn</code></td>
</tr>
<tr>
<td><strong>Save attributes in the session</strong></td>
<td>When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td><code>true</code>.</td>
</tr>
<tr>
<td><strong>OAuth 2.0 Mix-Up Mitigation Enabled</strong></td>
<td>Controls whether the authentication node carries out additional verification steps when it receives the authorization code from the authorization server.</td>
</tr>
<tr>
<td></td>
<td>Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the <code>iss</code> response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the <code>client_id</code> response parameter.</td>
</tr>
<tr>
<td></td>
<td>The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (<code>iss</code>) that will be validated by the client.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong></td>
</tr>
<tr>
<td></td>
<td>Consult with the authorization server's documentation on what value it uses for the issuer field. For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.</td>
</tr>
<tr>
<td>Token Issuer</td>
<td>Corresponds to the expected issuer identifier value in the <code>iss</code> field of the ID token.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>https://accounts.google.com</code></td>
</tr>
</tbody>
</table>

**Example:**

The following example uses the Anonymous User Mapping authentication node to allow users who have performed social authentication using Google to access AM as an anonymous user if they do not have a matching existing profile.

**Google-AnonymousUser Tree With Anonymous User Mapping Node**

![Diagram](image-url)

**Social Ignore Profile Node**

The Social Ignore Profile authentication node specifies if a local user profile should be ignored. If tree evaluation passes through this node, after successful social authentication, AM issues an SSO token regardless of whether a user profile exists in the data store. The presence of a user profile is not checked.

**Properties:**

This node has no configurable properties.
Social Provider Handler Node

This node is used alongside the "Select Identity Provider Node" to enable use of the platform's Social Identity Provider Service (located in AM). It takes the provider selection from the Select Identity Provider node and attempts to authenticate the user with that provider. It then collects relevant profile information from the provider and returns the user to the login or registration flow, and transforms that profile information into attributes the platform can use. The default transformation script can be found and edited in AM, by navigating to your Realm dashboard, selecting Scripts, then opening the Normalized Profile to Managed User script.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transformation Script</td>
<td>A script that can transform a normalized social profile to object data.</td>
</tr>
<tr>
<td>Username Attribute</td>
<td>The attribute in IDM that contains the username for this object.</td>
</tr>
</tbody>
</table>

Write Federation Information Node

This node creates a persistent link between a remote IdP account and a local account in the SP, if none exists yet. If a transient link exists, it is persisted. Existing account links with different IdPs are not lost.

Use this node alongside the "SAML2 Authentication Node", and ensure that the NameID Format is persistent.

Properties:

This node has no configurable properties.

Example:

Connect the Write Federation Information node to the tree branch that collects and validates the end user's login information in the SP.
Identity Management Authentication Nodes

Use the following nodes to perform identity management during an authentication tree flow, such as mapping anonymous users to a session:

Accept Terms and Conditions Node

This node prompts the user to accept the currently active Terms and Conditions. It requires integration with IDM to function. Terms and Conditions are configured in IDM, either through the IDM Admin UI, or in the `selfservice.terms.json` configuration file. This node is used in a registration tree, or combined with the "Terms and Conditions Decision Node" in a progressive profile or login tree. For more information about how IDM manages Terms and Conditions, see Terms & Conditions in the IDM Integrator's Guide.

Note that there is no failure path for this node: they must accept the Terms and Conditions in order to proceed.
Properties:

This node has no configurable properties.

Example:

In a progressive profile tree, the Accept Terms and Conditions node is used after the "Terms and Conditions Decision Node". If the user has not accepted the latest version of the Terms and Conditions, they are taken to a page notifying them that proceeding indicates accepting the current Terms and Conditions. If the user clicks next, the acceptance response is stored in IDM.
Anonymous User Mapping Node

The Anonymous User Mapping node allows users to log in to your application or web site without providing credentials, by assuming the identity of a specified, existing user account. The default user for this purpose is named \texttt{anonymous}.

Typically, you would provide such users with very limited access, for example, anonymous users may have access to public downloads on your site.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anonymous User Name</td>
<td>Specifies the username of an account that represents anonymous users. This user must already exist in the realm.</td>
</tr>
</tbody>
</table>

Example:

The following example uses the Anonymous User Mapping authentication node to allow users who have performed social authentication using Google to access AM as an anonymous user if they do not have a matching existing profile.
Anonymous Session Upgrade Node

The Anonymous Session Upgrade node allows an anonymous session to be upgraded to a non-anonymous session by adding the Anonymous Session Upgrade node as the first node in any tree.

Properties:

This node has no configurable properties.

Example:

After using the "Anonymous User Mapping Node" to access AM as an anonymous user, the Anonymous Session Upgrade authentication node lets users upgrade their session to a non-anonymous one.
Attribute Collector Node

The Attribute Collector node is used to collect the values of attributes for use elsewhere in a tree, such as collecting user information to populate a new account in a registration tree. This node relies on integration with IDM, and supports three types of attributes: string, boolean, and number. The node configuration allows the admin to specify if the attributes are required to continue, and if they should be subject to validation through IDM’s policy filter.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attributes to Collect</td>
<td>A list of the attributes you wish to collect, based on the attributes found in the IDM schema for the chosen object type.</td>
</tr>
<tr>
<td>All Attributes Required</td>
<td>When enabled, all attributes collected in this node are required in order to continue.</td>
</tr>
<tr>
<td>Validate Input</td>
<td>When enabled, the content input in this node should be validated against IDM policy settings specified in the IDM schema.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

Attribute Present Decision Node

Checks if an attribute is present on an object, regardless of whether the field is private. Use this to verify an attribute is present, without needing to know the value of the attribute itself. A good example of this is during an update password flow, where you want to check if the account has a password (rather than no password and logging in through a social identity) before continuing. This node is similar to the "Attribute Value Decision Node" when that node is set to use the present operator, except it cannot return the value of the attribute, and can work on private attributes.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Present Attribute</td>
<td>The object attribute to verify is present in the IDM object. This can be an otherwise private attribute, such as password.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

Attribute Value Decision Node

Verifies that the user's specified attribute satisfies a specific condition. Use this node to check whether an attribute's expected value is equal to a collected attribute value, or to validate that a specified attribute has been collected (regardless of the value of that attribute). For example, if you wish to validate that a user filled out the country attribute when registering, set the comparison operation to PRESENT, and the comparison attribute to country. If you instead need to ensure the country attribute is set to the United States, set the comparison operation to EQUALS, the comparison attribute to country, and the comparison value to United States.
Use "Attribute Present Decision Node" instead when you need to check for the presence of a private attribute (such as, **password**).

This node requires integration with IDM to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comparison Operation</td>
<td>The operation to perform on the object attribute; <strong>PRESENT</strong> checks for existence of an attribute, <strong>EQUALS</strong> checks if the object's attribute value equals the configured comparison value.</td>
</tr>
<tr>
<td>Comparison Attribute</td>
<td>The object attribute to compare.</td>
</tr>
<tr>
<td>Comparison Value</td>
<td>This property is only relevant when using the <strong>EQUALS</strong> comparison operation, and is the value to compare the object's attribute value to.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

**Create Object Node**

The Create Object node is used to create a new object in IDM based on information collected during an auth tree flow, such as user registration. Any managed object attributes that are marked as required in IDM will need to be collected during the auth tree flow in order for the new object to be created. This node requires IDM integration to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Resource</td>
<td>The type of managed object in IDM that this node will create. This needs to match the identity resource for the current tree.</td>
</tr>
</tbody>
</table>

**Create Password Node**

The Create Password node allows users to create a password when provisioning an account.

The social identity provider will not provide a user's password. Use this node to provide a password to complete the user's credentials before provisioning an account.

The tree must provision an account after asking the user for a password, for example by using the **Provision Dynamic Account** authentication node. If an account is not provisioned the entered password will not be saved.

**Note**

You must not place any nodes that request additional input from the user between the Create Password node and the provisioning node, otherwise the password will be lost.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>minPasswordLength</td>
<td>Specifies the minimum number of characters the password must contain.</td>
</tr>
</tbody>
</table>

Example:

The following example uses the Create Password authentication node to allow users who have performed social authentication using Google to provide a password and provision an account, if they do not have a matching existing profile. They must enter a one-time password to verify they are the owner of the Google account.

![Google-DynamicAccountCreation Tree With Create Password Node](image)

Consent Collector Node

The Consent Collector node prompts the user to consent to share their profile data. A consent notice is listed for each IDM mapping that has consent enabled. If an IDM mapping is not created, or the mappings do not have privacy and consent enabled, no consent message will be shown to the user. This node is primarily used in progressive profile or registration flows. It requires integration with IDM to function.

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Mappings Required</td>
<td>If enabled, all mappings listed by this node require consent in order to move forward.</td>
</tr>
<tr>
<td>Privacy &amp; Consent Message</td>
<td>Localized message providing the privacy and consent notice. The key is the language (such as en or fr), and the value is the message to display.</td>
</tr>
</tbody>
</table>

### Display Username Node

This node is used to fetch a username based on a different identifying attribute (such as an email address), then display it on screen. To email the username to the user instead, use the "Identify Existing User Node" combined with a "Email Suspend Node" or "Email Template Node". The Display Username node requires IDM integration to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>The attribute used to identify the username in an IDM object.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM. Since this node is generally used for recovering a username, the identity attribute in this case should be some other attribute that is unique to a user object, such as the user's email address. You will receive an exception if there is more than one result for this attribute, so make sure the value of whatever attribute you select is unique for each user.</td>
</tr>
</tbody>
</table>

### Identify Existing User Node

This node verifies a user exists based on an identifying attribute, such as an email address, then makes the value of a specified attribute available in a tree's shared state. For example, use this node in a "Forgot Username" flow to fetch a username to email to the user. If you want to display the username on screen, use the "Display Username Node" instead. The Identify Existing User node requires IDM integration to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identifier</td>
<td>The attribute to collect from an IDM object.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM. Since this node is generally used for recovering a username, the identity attribute in this case should be some other attribute that is unique to a user object, such as the user's email address.</td>
</tr>
</tbody>
</table>

### KBA Decision Node

The KBA Decision node is used to check if the minimum number of KBA questions required by the system are defined for the user. This node relies on integration with IDM; the number of KBA
questions is determined by the `minimumAnswersToDefine` property in `selfservice.kba.json` in IDM. This node is mainly used for Progressive Profile completion.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

**KBA Definition Node**

The KBA Definition node collects KBA questions and answers from the user and saves them to the user object. This is used when creating or updating a user with Knowledge-Based Authentication enabled. For more information, see Configuring Security Questions in the *IDM Integrator's Guide*.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Purpose Message</td>
<td>A localised message describing the purpose of the data requested from the user.</td>
</tr>
</tbody>
</table>

**KBA Verification Node**

The KBA Verification node presents KBA questions to the user, collects answers to those questions, and verifies the input against the user's stored answers. This is used during self-service actions such as Forgot Password or Forgot Username, where additional authentication is needed. This node relies on integration with IDM; the number of KBA questions is determined by the `minimumAnswersToVerify` property in `selfservice.kba.json` in IDM.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>KBA Attribute</td>
<td>The IDM object attribute in which KBA questions and answers are stored.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

**Patch Object Node**

The Patch Object node is used to update attributes in an existing managed object in IDM. This is used in cases such as progressive profile completion, where you may wish to collect additional profile data from a user after they have logged in several times. This node requires integration with IDM to function.

Properties:
Property | Usage
---|---
Patch as Object | Allows patching as the object being updated. Enable this property to patch a user object as part of the user's current session, such as when updating their password.

Ignored Fields | Fields from the tree's shared state that should be ignored as part of patch. If this is empty, all fields in `sharedState` are attempted as part of the patch. Use this to keep your patch focused only on the fields you want to update.

Identity Resource | The type of managed object in IDM that this node will patch. This needs to match the identity resource for the current tree.

Identity Attribute | The attribute used to identify the object to update in IDM.

### Platform Password Node

Similar to the "Password Collector Node", this node prompts the user to enter their password. Instead of being transient, however, the input is stored in a configurable state attribute. Use this node instead of the Password Collector node when working with AM and IDM as an integrated platform. The Platform Password node requires IDM integration to function.

**Properties:**

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
| Validate Password | When enabled, this node checks the user's input against IDM's password policies, and returns any policy failures as errors. For example, if you submitted an invalid password on registration, the response from this node would include a list of failed policies:

```json
{
    "name": "failedPolicies",
    "value": [ 
        {
            "params": { "minLength": 8 },
            "policyRequirement": "MIN_LENGTH"
        },
        {
            "params": { "numCaps": 1 },
            "policyRequirement": "AT_LEAST_X_CAPITAL_LETTERS"
        },
        {
            "params": { "numNums": 1 },
            "policyRequirement": "AT_LEAST_X_NUMBERS"
        }
    ]
}
```

| Password Attribute | The attribute used to store a password in the IDM object.

### Platform Username Node

Similar to the "Username Collector Node", this node prompts the user to enter their username. The input is stored in a configurable state attribute. Use this node instead of the Username Collector node when working with AM and IDM as an integrated platform. The Platform Username node requires IDM integration to function.

**Properties:**
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Validate Username</td>
<td>When enabled, this node checks the user's input against IDM's username policies, and returns any policy failures as errors.</td>
</tr>
<tr>
<td>Username Attribute</td>
<td>The attribute used to store a username in the IDM object.</td>
</tr>
</tbody>
</table>

**Profile Completeness Decision Node**

The Profile Completeness Decision node is used in progressive profile flows. It checks how much of a user's profile has been filled out, where the completeness of a profile is expressed as a percentage of user-viewable, user-editable fields that aren't `null`. This node requires integration with IDM to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Completeness Threshold</td>
<td>Percentage of user-viewable and user-editable fields in a profile that need to be filled out for the node to pass. Expressed as a number between 0 and 100.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

**Query Filter Decision Node**

Checks if the contents of a user's profile matches a specified query filter. Use this to verify whether a particular field has been filled out, or that the contents of a field match a specific pattern. For instance, use this in progressive profile flows to check if marketing preferences are set on a user's profile. For more information on constructing effective query filters, see Construct Queries in the IDM Object Modeling Guide.

This node requires integration with IDM to function.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Query Filter</td>
<td>A query filter used to check the contents of an object.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object that will be queried in IDM.</td>
</tr>
</tbody>
</table>

**Required Attributes Present Node**

The Required Attributes Present node checks the specified identity resource in IDM (by default, `managed/user`), and determines if all attributes required to create the specified object exist within shared state of the tree. This node is meant for use with the platform, and requires integration with IDM to function.

Properties:
Select Identity Provider Node

This node is used in combination with the "Social Provider Handler Node" to enable use of the platform's Social Identity Provider Service (found in AM). It presents the user with a list of configured, enabled, social identity providers to use for authentication. It can also be configured to only show identity providers the user has already associated with their account, such as in account claiming flows, where a user wishes to associate a new social identity provider with an account that is being authenticated with social authentication.

The node has two possible outputs: social authentication, and local authentication. Local authentication can be turned off by disabling Include local authentication. In cases such as during account claiming, where the user has already authenticated once and is associating a new identity provider, the node will only display a local sign in option if it detects that the user's account has a password attribute present.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Include local authentication</td>
<td>Determines whether local authentication will be included as an available method for authenticating.</td>
</tr>
<tr>
<td>Offer only existing providers</td>
<td>Enable this when the social identity provider choices offered should be limited to those already associated with a user object. Use this when a user is authenticating using a new social identity provider, and an account associated with that user already exists (also known as &quot;account claiming&quot;).</td>
</tr>
<tr>
<td>Password attribute</td>
<td>The attribute in the user object that stores a user's password, for use during local authentication.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify an existing user. Required to support the offer of only existing providers.</td>
</tr>
</tbody>
</table>

Terms and Conditions Decision Node

The Terms and Conditions Decision node verifies the user has accepted the active set of Terms and Conditions. This node relies on integration with IDM to function. Terms and Conditions are configured in IDM, either through the IDM Admin UI, or in the selfservice.terms.json configuration file. Use this node when you want to verify the user has accepted your Terms and Conditions before proceeding (such as logging in, or in a progressive profile tree). This is often used with the "Accept Terms and Conditions Node".

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object to check in IDM.</td>
</tr>
</tbody>
</table>
Time Since Decision Node

Checks if a specified amount of time has passed since the user was registered. For example, if you wanted to prompt users to review your terms and conditions after the account is a week old, you could set the Elapsed Time property to 10080 minutes. After that time has elapsed, the next time the user logs in, they will be prompted to review your terms and conditions. This node is mainly used for Progressive Profile completion, and requires integration with IDM to work.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed Time</td>
<td>The amount of time since the user was created, in minutes, that needs to elapse before this node is triggered. This property also supports specifying basic time units. For example, when setting the property to 10080 minutes, writing 7 days or 1 week also works.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object to update in IDM.</td>
</tr>
</tbody>
</table>

Utility Authentication Nodes

Use the following nodes to perform various tasks during the authentication flow:

Agent Data Store Decision Node

The Agent Data Store Decision authentication node verifies that a provided agent ID and password match a web agent or Java agent profile configured in AM.

**Note**

Non-agent identities, such as users stored in configured identity repositories, cannot be verified by using the Agent Data Store Decision node. Instead, you should use the Data Store Decision Node.

The web or Java agent ID, and the password should be obtained by using the Zero Page Login Collector Node.

Tree evaluation continues along the True path if the credentials match those of a configured agent profile. Otherwise, the tree evaluation continues along the False path.

Properties:

This node has no configurable properties.
Choice Collector Node

The Choice Collector authentication node lets you define two or more options to present to the user when authenticating.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Choices</td>
<td>Enter two or more choice strings to display to the user.</td>
</tr>
<tr>
<td></td>
<td>To remove a choice, select its Delete icon (x). To delete all choices, select the Clear all button in the Choices field.</td>
</tr>
<tr>
<td>Default choice</td>
<td>Enter the value of the choice to be selected by default.</td>
</tr>
<tr>
<td>Prompt</td>
<td>Enter the prompt string to display to the user when presenting the choices.</td>
</tr>
</tbody>
</table>

Example:
Email Suspend Node

The Email Suspend node is used to generate and send an email to a user, such as an address verification email, based on an email template in IDM. The authentication tree will pause until the user clicks a link in the email to resume the tree flow. The link is generated by the Email Suspend node, and is passed along to IDM as part of the email object, in a property called `resumeURI`.

This node relies on integration with IDM; it uses the email service configured in IDM to send email. If you do not need the auth tree to pause and wait for a response from email, use the "Email Template Node" instead.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Template Name</td>
<td>The name of the IDM email template to be sent. Check IDM for the names of available email templates, or to create a new template.</td>
</tr>
<tr>
<td>Email Attribute</td>
<td>The IDM attribute storing the address to send the email to.</td>
</tr>
<tr>
<td>Email Suspend Message</td>
<td>The localized message to be returned once the tree is suspended. The default message is &quot;An email has been sent to your inbox.&quot;</td>
</tr>
<tr>
<td>Object Lookup</td>
<td>Determines whether the object should be looked up in IDM. If true, IDM is queried for an existing object. Otherwise, the object in the authentication tree's shared state is used. For example, if suspending a user registration flow before the user object is created in IDM, this should be set to false. If the registration flow has already created the new user object when the flow is suspended, then this should be set to true.</td>
</tr>
</tbody>
</table>
### Email Template Node

The Email Template node is used to generate and send an email to a user, such as a welcome email, based on an email template in IDM. This node relies on integration with IDM; it uses the email service configured in IDM to send email. If you need the auth tree to pause and wait for a response from email, use the "Email Suspend Node" instead.

**Note**

This node has two possible outcomes: "Email Sent" and "Email Not Sent", which can be used if you need different behavior depending on the outcome. According to OWASP authentication recommendations, the message to the user should be the same in both cases.

**Properties:**

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email Template Name</td>
<td>The name of the IDM email template to be sent. Check IDM for the names of available email templates, or to create a new template.</td>
</tr>
<tr>
<td>Email Attribute</td>
<td>The IDM attribute storing the address to send the email to.</td>
</tr>
<tr>
<td>Identity Attribute</td>
<td>The attribute used to identify the object in IDM.</td>
</tr>
</tbody>
</table>

### Failure URL Node

The Failure URL authentication node sets the URL to be redirected to when authentication fails.

**Note**

Specifying a failure URL in a tree overrides any gotoOnFail query string parameters.

For more information on how AM determines the redirection URL, and to configure the Validation Service to trust redirection URLs, see "Configuring Success and Failure Redirection URLs".

**Tip**

The URL is also saved into the sharedState object, under a property named failureUrl, which can be useful for custom node developers. For more information, see "Customizing Authentication Trees".

**Properties:**
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failure URL</td>
<td>Specify the full URL to be redirected to when authentication fails.</td>
</tr>
</tbody>
</table>

Get Session Data Node

The Get Session Data authentication node retrieves the value of a specified key from a user's session data, and stores it in the specified key in the tree's `sharedState` object.

The Get Session Data authentication node is only used during session upgrade—when the user has already successfully authenticated previously—and is now upgrading their session for additional access. For more information on upgrading a session, see "Session Upgrade" in the Sessions Guide.

The node will fail with an error if you attempt to get a property when the user does not have an existing session. Use a "Scripted Decision Node" to determine if an existing session is present.

+ Example Check for Existing Session Script

```javascript
if (typeof existingSession !== 'undefined')
{
    outcome = "hasSession";
}
else
{
    outcome = "noSession";
}
```

Example:
The following table includes example keys that may be available in an existing session, and sample data that they might contain:

### Get Session Data Example Keys and Values

<table>
<thead>
<tr>
<th>Key</th>
<th>Sample value</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMCtxId</td>
<td>e370cca2-02d6-41f9-a244-2b107206bd2a-122934</td>
</tr>
<tr>
<td>amlbcokie</td>
<td>01</td>
</tr>
<tr>
<td>authInstant</td>
<td>2018-04-04T09:19:05Z</td>
</tr>
<tr>
<td>AuthLevel</td>
<td>0</td>
</tr>
<tr>
<td>CharSet</td>
<td>UTF-8</td>
</tr>
<tr>
<td>clientType</td>
<td>genericHTML</td>
</tr>
<tr>
<td>FullLoginURL</td>
<td>/openam/UI/Login?realm=%2F</td>
</tr>
<tr>
<td>Host</td>
<td>198.51.100.1</td>
</tr>
<tr>
<td>HostName</td>
<td>openam.example.com</td>
</tr>
<tr>
<td>Locale</td>
<td>en_US</td>
</tr>
<tr>
<td>Organization</td>
<td>dc=openam,dc=forgerock,dc=org</td>
</tr>
<tr>
<td>Principal</td>
<td>uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org</td>
</tr>
<tr>
<td>Principals</td>
<td>amAdmin</td>
</tr>
<tr>
<td>Service</td>
<td>ldapService</td>
</tr>
<tr>
<td>successURL</td>
<td>/openam/console</td>
</tr>
<tr>
<td>sun.am.UniversalIdentifier</td>
<td>uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org</td>
</tr>
<tr>
<td>UserId</td>
<td>amAdmin</td>
</tr>
<tr>
<td>UserProfile</td>
<td>Required</td>
</tr>
<tr>
<td>UserToken</td>
<td>amAdmin</td>
</tr>
<tr>
<td>webhooks</td>
<td>myWebHook</td>
</tr>
</tbody>
</table>

Properties:
Property | Usage
--- | ---
Session Data Key | Specify the name of a key in the user's session data from which to retrieve the value.
Shared State Key | Specify the name of a key in the `sharedState` object in which to store the retrieved value.

Inner Tree Evaluator Node

The Inner Tree Evaluator authentication node allows the nesting and evaluation of authentication trees as children within a parent tree. There is no limit to the depth of nested trees.

Any information collected or set by the parent tree, for example, a username or the authentication level, is available to the child trees. Information collected by child trees is available to the parent once evaluation of the child is complete.

Tree evaluation continues along the `True` path if the child tree reached the Success exit point. Otherwise, the tree evaluation continues along the `False` path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tree name</td>
<td>Enter the name of the tree to evaluate.</td>
</tr>
</tbody>
</table>
Message Node

The Message authentication node allows you to present a custom, localized message to the user. Alongside the message, you can provide a localized positive, and negative response that the user can select to proceed.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
<td>Click the Add button, and then enter the locale of the message in the <strong>Key</strong> field, and the message to display to the user in the <strong>Value</strong> field. If the locale of the user's browser cannot be determined during authentication, the first message in the list is used.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>If the message property is left blank, the text <strong>Default message</strong> is displayed to the user.</td>
</tr>
<tr>
<td></td>
<td>To remove a message, select its Delete icon (_DIAGRAM?).</td>
</tr>
<tr>
<td>Positive answer</td>
<td>Specifying a positive answer will cause tree evaluation to continue along the <strong>True</strong> outcome path.</td>
</tr>
<tr>
<td></td>
<td>Click the Add button, and then enter the locale of the positive answer in the <strong>Key</strong> field, and the message to display to the user in the <strong>Value</strong> field.</td>
</tr>
<tr>
<td></td>
<td>If the locale of the user's browser cannot be determined during authentication, the first message in the list is used.</td>
</tr>
<tr>
<td></td>
<td>If the message property is left blank, the text <strong>Yes</strong> is displayed to the user.</td>
</tr>
<tr>
<td></td>
<td>To remove a message, select its Delete icon (_DIAGRAM?).</td>
</tr>
<tr>
<td>Negative answer</td>
<td>Specifying a negative answer will cause tree evaluation to continue along the <strong>False</strong> outcome path.</td>
</tr>
<tr>
<td></td>
<td>Click the Add button, and then enter the locale of the negative answer in the <strong>Key</strong> field, and the message to display to the user in the <strong>Value</strong> field.</td>
</tr>
<tr>
<td></td>
<td>If the locale of the user's browser cannot be determined during authentication, the first message in the list is used.</td>
</tr>
<tr>
<td></td>
<td>If the message property is left blank, the text <strong>No</strong> is displayed to the user.</td>
</tr>
<tr>
<td></td>
<td>To remove a message, select its Delete icon (_DIAGRAM?).</td>
</tr>
</tbody>
</table>

**Example:**

![Example Image](image-url)
Meter Node

The Meter authentication node increments a specified metric key each time tree evaluation passes through the node. For information on the Meter metric type, see "Monitoring Metric Types" in the Maintenance Guide. The metric is exposed in all available interfaces, as described in "Monitoring Instances" in the Maintenance Guide.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metric Key</td>
<td>Specify the name of a metric to increment when tree evaluation passes through the node.</td>
</tr>
</tbody>
</table>

Page Node

The Page authentication node combines multiple nodes that request input into a single page for display to the user. Drag and drop nodes on to the page node to combine them.

The outcome paths are determined by the last node in the page node. Only the last node in the page can have more than one outcome path.

Only nodes that use callbacks to request input can be added to a page node. Other nodes, such as the Data Store Decision Node and Push Sender Node must not be added to a page node.
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Header</td>
<td>Optional. Localized title for the page node and the nodes contained within it. Use this when components of an authentication flow need a title, such as breaking a registration into labelled sections.</td>
</tr>
<tr>
<td>Description</td>
<td>Optional. A localized description for the page node and the nodes contained within it. Use this when additional descriptive text is needed in an authentication flow.</td>
</tr>
<tr>
<td>Stage</td>
<td>Optional. This is used in UI development, to help identify what node or series of nodes are being returned so they can be rendered in the UI appropriately.</td>
</tr>
</tbody>
</table>

**Note**

The Page Node's optional properties are passed in the response, but the UI needs to support these properties before they will be visible to the end user.

Example:

The following example uses a page node containing a username collector, a password collector, and a choice collector:
The user is presented with all of the requests for input on a single page:

**User View of Example Tree with Page Node**
Polling Wait Node

The Polling Wait authentication node pauses progress of the authentication tree for a specified number of seconds, for example in order to wait for a response to a one-time password email or push notification.

Requests to the tree made during the wait period are sent a PollingWaitCallback callback and an authentication ID. For example, the following callback indicates a wait time of 10 seconds:

```json
{
    "authId": "eyJ0eXAiOiJK...u4WvZmiI",
    "callbacks": [
        {
            "type": "PollingWaitCallback",
            "output": [
                {
                    "name": "waitTime",
                    "value": "10000"
                },
                {
                    "name": "message",
                    "value": "Waiting for response..."
                }
            ]
        }
    ]
}
```

The client must wait 10 seconds before returning the callback data, including the authId. For example:

```bash
$ curl \
   --cookie "iPlanetDirectoryPro=AQIC5w...NTcy*" " \
   --request POST \
   --header "Content-Type: application/json" \
   --header "Accept-API-Version: resource=2.0, protocol=1.0" \
   --data '{
       "authId":"eyJ0eXAiOi...WLxJ-1d6ovYKHQ",
       "template":"",
       "stage":"AuthenticatorPush3",
       "header":"Authenticator Push",
       "callbacks":[
         {
             "type":"PollingWaitCallback",
             "output":[
                 {
                     "name":"waitTime",
                     "value":"10000"
                 }
             ]
         },
         {
             "type":"ConfirmationCallback",
             "output":[
                 {
                     "name":"prompt",
                     "value":""
                 }
             ]
         }
       ]
   }
```


For more information on authenticating using the REST API, see "Authenticating (REST)".

When using the UI for authentication, it automatically waits for the required amount of time and resubmits the page in order to continue tree evaluation. The message displayed whilst waiting is configurable by using the Waiting Message property.

Tree evaluation continues along the Done outcome path when the next request is received after the wait time has passed.

Enabling Spam detection adds a Spam outcome path to the node. Tree evaluation continues along the Spam outcome path if more than the specified number of requests are received during the wait time.

Enabling the user to exit without waiting adds an Exited outcome path to the node. Tree evaluation continues along the Exited outcome path if the user clicks the button that appears when the option is enabled. The message displayed on the exit button is configurable by using the Exit Message property.
Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Seconds To Wait</td>
<td>Specify the number of seconds to pause the authentication tree. Default: 8</td>
</tr>
<tr>
<td>Enable Spam Detection</td>
<td>Specify whether to track the number of responses received during the wait time, and continue tree evaluation along the Spam outcome path if the number specified in the Spam Tolerance property is exceeded.</td>
</tr>
<tr>
<td>Property</td>
<td>Usage</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default: Disabled</td>
<td>Specify the number of responses to allow during the wait time before continuing tree evaluation along the Spam outcome path. This property only applies if spam detection is enabled. Default: 3</td>
</tr>
<tr>
<td>Spat Tolerance</td>
<td>Specify the number of responses to allow during the wait time before continuing tree evaluation along the Spam outcome path. This property only applies if spam detection is enabled. Default: 3</td>
</tr>
<tr>
<td>Waiting Message</td>
<td>Specifies the optional message to display to the user. You can provide the message in multiple languages by specifying the locale in the KEY field, for example en-US. For information on valid locale strings, see JDK 11 Supported Locales. The locale selected for display is based on the user's locale settings in their browser. Messages provided in the node override the defaults provided by AM. For information about customizing and translating the default messages, see &quot;Internationalization&quot; in the Authentication Node Development Guide.</td>
</tr>
<tr>
<td>Exitable</td>
<td>Specify whether the user can exit the node during the wait period. Enabling this option adds a button with a configurable message to the page. Clicking the button causes tree evaluation to continue along the Exit message outcome path. Default: Disabled</td>
</tr>
<tr>
<td>Exit Message</td>
<td>Specifies the optional message to display to the user on the button used to exit the node before the wait period has elapsed. For example, Cancel or Lost phone? Use Recovery Code. This property only applies if the Exitable property is enabled. You can provide the message in multiple languages by specifying the locale in the KEY field, for example en-US. For information on valid locale strings, see JDK 11 Supported Locales. The locale selected for display is based on the user's locale settings in their browser. Messages provided in the node override the defaults provided by AM. For information about customizing and translating the default messages, see &quot;Internationalization&quot; in the Authentication Node Development Guide.</td>
</tr>
</tbody>
</table>

Register Logout Webhook Node

The Register Logout Webhook authentication node registers the specified webhook to trigger when a user's session ends. The webhook triggers when a user explicitly logs out, or the maximum idle time or expiry time of the session is reached.

The webhook is only registered if tree evaluation passes through the Register Logout Webhook node. You can register multiple webhooks during the authentication process, but they must be unique.

For more information on webhooks, see "Configuring Authentication Webhooks".

Properties:
## Remove Session Properties Node

The Remove Session Properties authentication node enables the removal of properties from the session. The session properties may have been set by a Set Session Properties node elsewhere in the tree.

If a specified key is not found in the list of session properties that will be added to the session upon successful authentication, no error is thrown and tree evaluation continues along the single outcome path.

If a specified key is found, the tree evaluation continues along the single outcome path after setting the value of the property to `null`.

### Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property Names</td>
<td>Enter one or more key names of properties to remove from the session.</td>
</tr>
</tbody>
</table>
Retry Limit Decision Node

The Retry Limit Decision authentication node allows the specified number of passes through to the Retry outcome path, before continuing tree evaluation along the Reject outcome path.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Retry limit</td>
<td>Specify the number of times to allow a retry.</td>
</tr>
<tr>
<td>Default: 3</td>
<td></td>
</tr>
</tbody>
</table>

Save Retry Limit to User

(Introduced in AM 7.0.2) Specify whether the number of failed login attempts persists between successful authentications. Possible values are:

- Enabled. The node saves the number of failed login attempts to the user's profile. New authentication journeys using the Retry Limit Decision node will use the stored value as the starting point for the retry limit.

AM resets the count after the user authenticates successfully with a tree that contains this node.

If AM cannot find the user's profile, the authentication journey will end with an error.

Important

After upgrading to AM 7.0.2 or later, you must update the identity store's schema manually before enabling this feature.

+ How Do I Apply the New Schema?

To update the identity store schema for the Retry Limit Decision Node, perform the following steps:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
</table>
|          | 1. Change directories to the path where you deployed the `openam.war` file. For example, `/path/to/tomcat/webapps/openam`.
|          | 2. Locate the `opendj_retry_limit_node_count.ldif` file in the `WEB-INF/template/ldif/opendj` path.
|          | 3. Update the identity store schema using the LDIF file. For example:
|          | ```
|          | $ /path/to/opendj/bin/ldapmodify \
|          |   --hostname 'id.example.com' \
|          |   --port 1636 \
|          |   --useSsl \
|          |   --usePkcs12TrustStore /path/to/opendj/config/keystore \
|          |   --trustStorePasswordFile /path/to/opendj/config/keystore.pin \
|          |   --continueOnError \
|          |   --bindDN uid=admin \
|          |   --bindPassword strongAdm1nPa55word \
|          |   /path/to/tomcat/webapps/openam/WEB-INF/template/ldif/opendj/ \
|          |   `opendj_retry_limit_node_count.ldif` 
|          | Now you are ready to enable the Save Retry Limit to User switch in the "Retry Limit Decision Node". |
|          | • Disabled. The node saves the number of failed login attempt in the tree's `nodeRetryLimitKey` shared state property, which is discarded when the authentication session ends. For security reasons, ForgeRock recommends that you enable this setting. Default: Disabled. |

Example:

**RetryLimit Tree**
Scripted Decision Node

The Scripted Decision authentication node allows execution of scripts during authentication. Tree evaluation continues along the path matching the result.

The script defines the possible outcome paths by setting one or more values of a string variable named `outcome`. For more information on creating scripts, see "Managing Scripts (Console)" in the Getting Started with Scripting.

Tree evaluation continues along the outcome path that matches the value of the `outcome` variable when script execution completes.

All of the inputs required by the script and the outputs produced by it must be declared in the node's configuration or the script may fail. Even if the definition is `null`, it still needs to be declared. Use the wildcard `*` to include any available inputs or outputs.

For information about the API available for use in the Scripted Decision Node, see "Scripted Decision Node API Functionality".

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Script</td>
<td>Select the script to execute from the drop-down field.</td>
</tr>
<tr>
<td>Outcomes</td>
<td>Enter the possible strings that can be assigned to the <code>outcome</code> variable by the script. These strings provide the possible outcome paths the tree can continue along.</td>
</tr>
<tr>
<td>Script Inputs</td>
<td>A list of state inputs required by the script. Defaults to <code>*</code>.</td>
</tr>
<tr>
<td>Script Outputs</td>
<td>A list of state outputs produced by the script. Defaults to <code>*</code>.</td>
</tr>
</tbody>
</table>
Set Session Properties Node

The Set Session Properties authentication node allows the addition of key:value properties to the user's session if authentication is successful.

**Tip**

You can access session properties using a variable in a webhook. For more information, see "Configuring Authentication Webhooks".

Tree evaluation continues along the single outcome path after setting the specified properties in the session.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
<td>To add a session property, select the Add button, enter a key name and a value, and then select the plus icon. Repeat the steps to add multiple properties.</td>
</tr>
</tbody>
</table>

Success URL Node

The Success URL authentication node sets the URL to be redirected to when authentication succeeds.

**Note**

Specifying a success URL in a tree overrides any goto query string parameters.

For more information on how AM determines the redirection URL, and to configure the Validation Service to trust redirection URLs, see "Configuring Success and Failure Redirection URLs".
Tip

The URL is also saved into the sharedState object, under a property named successUrl, which can be useful for custom node developers. For more information, see "Customizing Authentication Trees".

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success URL</td>
<td>Specify the full URL to be redirected to when the authentication succeeds.</td>
</tr>
</tbody>
</table>

Timer Start Node

The Timer Start authentication node starts a named timer metric, which can be stopped elsewhere in the tree by using the Timer Stop Node.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time Property</td>
<td>Specify a property name into which to store the current time. Specify the same value in any instances of the Timer Stop Node that measure the time elapsed since tree evaluation passed through this node.</td>
</tr>
</tbody>
</table>
Timer Stop Node

The Timer Stop authentication node records the time elapsed since tree evaluation passed through the specified Timer Start Node in the specified metric name. For information on the Timer metric type, see "Monitoring Metric Types" in the Maintenance Guide.

Note that the time stored in the specified Start Time Property property is not reset by the Timer Stop Node, so other Timer Stop Nodes in the tree can also calculate the time elapsed since tree evaluation passed through the same Timer Start Node.

The metric is exposed in all available interfaces, as described in "Monitoring Instances" in the Maintenance Guide.

Properties:

<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start Time Property</td>
<td>Specify the property name containing the time from which to calculate the elapsed time.</td>
</tr>
<tr>
<td>Metric Key</td>
<td>Specify the name of a metric in which to store the calculated elapsed time.</td>
</tr>
</tbody>
</table>

Thing Authentication Nodes

Use the following nodes to perform various tasks related to authenticating IoT things:

Authenticate Thing Node

This node authenticates a thing. A thing represents an IoT device, service, or the Thing Gateway. Before using this node, ensure that the IoT Service is configured for the realm.
Important

Support for this node is provided by the Thing SDK.

It collects a proof-of-possession JWT from the request and checks the following:

• That the claims are valid.

• That the thing is of a valid type.

• That an identity with the same ID as the name of the JWT subject exists.

• That the identity contains a confirmation key that matches the JWT's kid.

If all checks are successful and AM can verify the JWT's signature with the confirmation key, the tree continues through the Success path, and adds the username and the verified claims to the authentication tree's shared state.

When using the resulting session, the thing's request must be signed, and AM must be able to validate the signature using the confirmation key in the thing's identity profile.

If the identity does not exist, or AM cannot match the identity with the confirmation key, the tree continues through the Requires Registration outcome. If any other check fails, the tree continues through the Failure outcome.

Properties:

This node has no configurable properties.

Examples:

The following example shows how to authenticate a thing when the identity already exists in the identity store and when its profile contains a confirmation key:

Authenticating a Thing Without Registration
The following example shows how to authenticate a thing when the identity does not exist, or when it needs to refresh its confirmation key:

**Authenticating a Thing With Registration**

![Diagram of Authenticating a Thing With Registration]

Register Thing Node

This node registers a thing. A thing represents an IoT device, service, or the Thing Gateway. Before using this node, ensure that the IoT Service is configured for the realm.

**Important**

Support for this node is provided by the Thing SDK.

The node collects a proof-of-possession JWT from the request, and verifies the contained X.509 certificate against the key mapped to the `am.services.iot.cert.verification` secret ID.

If the certificate is valid, the node verifies the JWT's signature with the public key provided in the certificate and uses the claims in the JWT to create an identity for the thing and register (or rotate) a confirmation key for it. Then, the tree continues through the **Success** outcome.

If the node cannot verify the certificate with the key mapped to the secret ID, or if it cannot verify the JWT's signature, the tree continues through the **Failure** outcome.

For an example on how to use this node, see the "Authenticate Thing Node".

Properties:
<table>
<thead>
<tr>
<th>Property</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify Certificate Subject</td>
<td>Specifies whether to verify that the subject provided in the JWT is the same as the one specified in the CN or UID fields of the X.509 certificate. Default: Enabled</td>
</tr>
<tr>
<td>Create Identity</td>
<td>Specifies whether AM will create an ID for the thing if one does not exist. Default: Disabled</td>
</tr>
<tr>
<td>Rotate Confirmation Key</td>
<td>Specifies whether multiple confirmation keys can be registered for a thing. Disable this setting to allow one key per thing. Default: Disabled</td>
</tr>
<tr>
<td>Claim to Attribute Mapping</td>
<td>When Create Identity is enabled, maps verified claims in the JWT to attributes in the new identity. The key of the map is the claim name, and the value is the name of the attribute in the identity store.</td>
</tr>
<tr>
<td>Overwrite Attributes</td>
<td>Specifies whether the node will overwrite the value for an existing profile attribute when a claim with a different value is provided in the JWT. Default: Disabled</td>
</tr>
</tbody>
</table>
Scripted Decision Node API Functionality

In addition to the functionality provided by "Accessing HTTP Services" in the Getting Started with Scripting and "Debug Logging" in the Getting Started with Scripting, scripted decision nodes can access request headers, the authentication session's shared state, and information provided during session upgrade.

Scripted decision nodes can also use callbacks to provide or request additional information during the authentication process.

Accessing Request Header Data

Scripted Decision Node scripts can access the headers provided by the login request by using the methods of the requestHeaders object.

Note that the script has access to a copy of the headers. Changing their values does not affect the request itself.

The following table lists the methods of the requestHeaders object:

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requestHeaders.</td>
<td>Header Name</td>
<td>String[]</td>
<td>Return the array of string values of the named request header, or null if</td>
</tr>
<tr>
<td>get</td>
<td>(type: String)</td>
<td></td>
<td>the property is not set. Note that header names are case-sensitive.</td>
</tr>
</tbody>
</table>

For example:

```javascript
var headerName = "user-agent";
if (requestHeaders.get(headerName).get(0).indexOf("Chrome") != -1) {
  outcome = "true";
} else {
  outcome = "false";
}
```

Accessing Shared State Data

Scripted Decision Node scripts can get access to the shared state within the tree by using the sharedState and transientState objects.

The following table lists the available methods:
### Shared State Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sharedState.get</td>
<td>Property Name (type: String)</td>
<td>String</td>
<td>Return the string value of the named shared state property, or null if the property is not set. Note that property names are case-sensitive.</td>
</tr>
<tr>
<td>transientState.get</td>
<td>Property Name (type: String)</td>
<td>String</td>
<td>Return the string value of the named transient state property, or null if the property is not set. Note that property names are case-sensitive.</td>
</tr>
</tbody>
</table>

For example, use the following code to get the current authentication level:

```javascript
var currentAuthLevel = sharedState.get("authLevel");
```

For example, use the following code to get the value of a previously supplied password:

```javascript
var givenPassword = transientState.get("password");
```

### Accessing Profile Data

Scripted decision nodes can access profile data through the methods of the `idRepository` object.

### Profile Data Methods

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idRepository.getAttribute</td>
<td>User Name (type: String) Attribute Name (type: String)</td>
<td>Set</td>
<td>Return the values of the named attribute for the named user.</td>
</tr>
<tr>
<td>idRepository.setAttribute</td>
<td>User Name (type: String) Attribute Name (type: String) Attribute Values (type: Array)</td>
<td>Void</td>
<td>Set the named attribute as specified by the attribute value for the named user, and persist the result in the user's profile.</td>
</tr>
<tr>
<td>idRepository.addAttribute</td>
<td>User Name (type: String) Attribute Name (type: String) Attribute Value (type: String)</td>
<td>Void</td>
<td>Add an attribute value to the list of attribute values associated with the attribute name for a particular user.</td>
</tr>
</tbody>
</table>

### Setting Session Properties

Scripted Decision Node scripts can create session properties by using the `Action` API, as follows:
JavaScript

```javascript
var fr = JavaImporter(
    org.forgerock.openam.auth.node.api.Action
);

with (fr) {
    action = Action.goTo("true").putSessionProperty("mySessionProperty","myPropertyValue").build();
}
```

Groovy

```groovy
import org.forgerock.openam.auth.node.api.Action

action =
    new Action.ActionBuilder("true").putSessionProperty("mySessionProperty","myPropertyValue").build();
```

**Note**

Add the property name to the Whitelisted Session Property Names list in the Session Property Whitelist Service; otherwise, it will not be added to sessions. For more information on this service, see "Session Property Whitelist Service" in the *Reference*.

Add the script to a scripted decision node in your authentication tree. Users that authenticate successfully using that tree will have the property added to their session, as shown in the following output when introspecting a session in the *Sessions Guide*:

```
{
    "username": "15249a65-8f9a-4063-9586-a2465963cee4",
    "universalId": "id=15249a65-8f9a-4063-9586-a2465963bee4,ou=user,o=alpha,ou=services,ou=am-config",
    "realm": "/alpha",
    "latestAccessTime": "2020-10-22T15:01:14Z",
    "maxIdleExpirationTime": "2020-10-22T15:31:14Z",
    "maxSessionExpirationTime": "2020-10-22T17:01:13Z",
    "properties": {
        "AMCtxId": "dffed74d-f203-469c-9ed2-34738915baea-5255",
        "mySessionProperty": "myPropertyValue"
    }
}
```

## Accessing Existing Session Properties

Scripted Decision Node scripts can access any existing session properties during a session upgrade request, by using the `existingSession` object.

The following table lists the methods of the `existingSession` object:

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>existingSession.get</code></td>
<td><code>Property Name</code> (type: String)</td>
<td>String</td>
<td>Return the string value of the named existing session property, or <code>null</code> if the property is not set. Note that property names are case-sensitive.</td>
</tr>
</tbody>
</table>
Using Callbacks

The scripted decision node can use callbacks to provide or request additional information during the authentication process.

For example, the following scripts use the `NameCallback` callback to request a "Nickname" value from the user, and adds the returned value to the `sharedState` map for use elsewhere in the authentication tree:

**Groovy**

```groovy
import org.forgerock.openam.auth.node.api.*;
import javax.security.auth.callback.NameCallback;

if (callbacks.isEmpty()) {
    action = Action.send(new NameCallback("Enter Your Nickname")).build();
} else {
    sharedState.put("Nickname", callbacks.get(0).getName());
    action = Action.goTo("true").build();
}
```

**JavaScript**

```javascript
import org.forgerock.openam.auth.node.api.*;
import javax.security.auth.callback.NameCallback;

if (callbacks.isEmpty()) {
    action = Action.send(new NameCallback("Enter Your Nickname")).build();
} else {
    sharedState.put("Nickname", callbacks.get(0).getName());
    action = Action.goTo("true").build();
}
```
Adding Audit Information

The scripted decision node can add information to audit log entries, by using the `auditEntryDetail` object.

AM appends the value of the object, which can be either plain text, or a JSON object, to the authentication audit logs.

For example, the following Groovy script adds the user's email address to the `authentication.audit.json` audit log file:

```groovy
var currentUser = sharedState.get("username");
var attributeToRead = "mail";

auditEntryDetail="Extra Audit: " + currentUser + " email address: " +
idRepository.getAttribute(currentUser,attributeToRead).iterator().next().toString();
outcome = "true";
```

The code above adds the information to the `auditInfo` element, for example:

```
For more information about auditing, see "Setting Up Audit Logging" in the Security Guide.

Authentication Module Properties

This section provides a reference to configuration properties for AM authentication modules.

Active Directory Module Properties

**amster** service name: ActiveDirectoryModule

**ssoadm** service name: sunAMAuthADService

Primary Active Directory Server

Secondary Active Directory Server

Specify the primary and secondary Active Directory server(s). AM attempts to contact the primary server(s) first. If no primary server is available, then AM attempts to contact the secondary server(s).

When authenticating users from a directory server that is remote to AM, set the primary server values, and optionally the secondary server values. Primary servers have priority over secondary servers.
To allow users to change passwords through AM, Active Directory requires that you connect over SSL. The default port for LDAP is 389. If you are connecting to Active Directory over SSL, the default port for LDAP/SSL is 636.

For SSL or TLS security, enable the SSL/TLS Access to Active Directory Server property. Make sure that AM can trust the Active Directory certificate when using this option.

**ssoadm** attributes are: primary is `iplanet-am-auth-ldap-server`; secondary is `iplanet-am-auth-ldap-server2`.

Both properties may take a single value in the form of `server:port`, or more than one value in the form of `openam_full_server_name | server:port`; thus, allowing more than one primary or secondary remote server, respectively.

Assuming a multi-data center environment, AM determines priority within the primary and secondary remote servers as follows:

- Every LDAP server that is mapped to the current AM instance has highest priority.
  
  For example, if you are connected to `openam1.example.com` and `ldap1.example.com` is mapped to that AM instance, then AM uses `ldap1.example.com`.

- Every LDAP server that was not specifically mapped to a given AM instance has the next highest priority.

  For example, if you have another LDAP server, `ldap2.example.com`, that is not connected to a specific AM server and if `ldap1.example.com` is unavailable, AM connects to the next highest priority LDAP server, `ldap2.example.com`.

- LDAP servers that are mapped to different AM instances have the lowest priority.

  For example, if `ldap3.example.com` is connected to `openam3.example.com` and `ldap1.example.com` and `ldap2.example.com` are unavailable, then `openam1.example.com` connects to `ldap3.example.com`.

**DN to Start User Search**

Specifies the base DN from which AM searches for users to authenticate.

LDAP data is organized hierarchically, a bit like a file system on Windows or UNIX. More specific DNs likely result in better performance. When configuring the module for a particular part of the organization, you can perhaps start searches from a specific organizational unit, such as `OU=sales, DC=example, DC=com`.

If multiple entries exist with identical search attribute values, make this value specific enough to return only one entry.

**amster** attribute: `userSearchStartDN`

**ssoadm** attribute: `iplanet-am-auth-ldap-base-dn`
Bind User DN, Bind User Password

Specify the user and password to authenticate to Active Directory.

If AM stores attributes in Active Directory, for example to manage account lockout, or if Active Directory requires that AM authenticate in order to read users' attributes, then AM needs the DN and password to authenticate to Active Directory.

If the administrator authentication chain (default: ldapService) has been configured to include only the Active Directory module, then make sure that the password is correct before you logout. If it is incorrect, you will be locked out. If you do get locked out, you can login with the superuser DN, which by default is uid=amAdmin,ou=People,AM-deploy-base, where AM-deploy-base was set during AM configuration.

**ssoadm** attributes: iplanet-am-auth-ldap-bind-dn and iplanet-am-auth-ldap-bind-passwd

Attribute Used to Retrieve User Profile

Attributes Used to Search for a User to be Authenticated

User Search Filter

Search Scope

LDAP searches for user entries with attribute values matching the filter you provide. For example, if you search under CN=Users,DC=example,DC=com with a filter "(MAIL=bjensen@example.com)", then the directory returns the entry that has MAIL=bjensen@example.com. In this example the attribute used to search for a user is mail. Multiple attribute values mean the user can authenticate with any one of the values. For example, if you have both uid and mail, then Barbara Jensen can authenticate with either bjensen or bjensen@example.com.

The User Search Filter text box provides a more complex filter. For example, if you search on mail and add User Search Filter (objectClass=inetOrgPerson), then AM uses the resulting search filter 

&mail=address (objectClass=inetOrgPerson), where address is the mail address provided by the user.

This controls how and the level of the directory that will be searched. You can set the search to run at a high level or against a specific area:

- **OBJECT** will search only for the entry specified as the DN to Start User Search.
- **ONELEVEL** will search only the entries that are directly children of that object.
- **SUBTREE** will search the entry specified and every entry under it.


LDAP Connection Mode

If you want to initiate secure communications to data stores using SSL or StartTLS, AM must be able to trust Active Directory certificates, either because the Active Directory certificates were signed by a CA whose certificate is already included in the trust store used by the container where AM runs, or because you imported the certificates into the trust store.
**ssoadm** attribute: `openam-auth-ldap-connection-mode`  
Possible values: LDAP, LDAPS, and StartTLS

**Return User DN to DataStore**

When enabled, and AM uses Active Directory as the user store, the module returns the DN rather than the User ID, so the bind for authentication can be completed without a search to retrieve the DN.

**amster** attribute: `returnUserDN`  
**ssoadm** attribute: `iplanet-am-auth-ldap-return-user-dn`

**User Creation Attributes**

Maps internal attribute names used by AM to external attribute names from Active Directory for dynamic profile creation. Values are of the format `internal_attr1|external_attr1`.

**amster** attribute: `profileAttributeMappings`  
**ssoadm** attribute: `iplanet-am-ldap-user-creation-attr-list`

**Trust All Server Certificates**

When enabled, the module trusts all server certificates, including self-signed certificates.

**amster** attribute: `trustAllServerCertificates`  
**ssoadm** attribute: `iplanet-am-auth-ldap-ssl-trust-all`

**LDAP Connection Heartbeat Interval**

Specifies how often AM should send a heartbeat request to the directory server to ensure that the connection does not remain idle. Some network administrators configure firewalls and load balancers to drop connections that are idle for too long. You can turn this off by setting the value to 0 or to a negative number. To set the units for the interval, use LDAP Connection Heartbeat Time Unit.

Default: 1

**amster** attribute: `connectionHeartbeatInterval`  
**ssoadm** attribute: `openam-auth-ldap-heartbeat-interval`

**LDAP Connection Heartbeat Time Unit**

Specifies the time unit corresponding to LDAP Connection Heartbeat Interval. Possible values are SECONDS, MINUTES, and HOURS.

**amster** attribute: `connectionHeartbeatTimeUnit`
**ssoadm** attribute: openam-auth-ldap-heartbeat-timeunit

**LDAP operations timeout**

Defines the timeout in milliseconds that AM should wait for a response from the directory server.

Default: 0 (means no timeout)

**amster** attribute: operationTimeout

**ssoadm** attribute: openam-auth-ldap-operation-timeout

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: authenticationLevel

**ssoadm** attribute: sunAMAuthADAuthLevel

**Adaptive Risk Authentication Module Properties**

**amster** service name: AdaptiveRiskModule

**ssoadm** service name: sunAMAuthAdaptiveService

**General**

The following properties are available under the General tab:

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: authenticationLevel

**ssoadm** attribute: openam-auth-adaptive-auth-level

**Risk Threshold**

Sets the risk threshold score. If the sum of the scores is greater than the threshold, the Adaptive Risk module fails.

Default: 1

**amster** attribute: riskThreshold

**ssoadm** attribute: openam-auth-adaptive-auth-threshold
Failed Authentications

The following properties are available under the Failed Authentications tab:

**Failed Authentication Check**

When enabled, checks the user profile for authentication failures since the last successful login. This check therefore requires AM to have access to the user profile, and Account Lockout to be enabled (otherwise, AM does not record authentication failures).

**amster** attribute: `failedAuthenticationCheckEnabled`

**ssoadm** attribute: `openam-auth-adaptive-failure-check`

**Score**

Sets the value to add to the total score if the user fails the Failed Authentication Check. Default: 1

**amster** attribute: `failureScore`

**ssoadm** attribute: `openam-auth-adaptive-failure-score`

**Invert Result**

When enabled, adds the score to the total score if the user passes the Failed Authentication Check.

**amster** attribute: `invertFailureScore`

**ssoadm** attribute: `openam-auth-adaptive-failure-invert`

**IP Address Range**

The following properties are available under the IP Address Range tab:

**IP Range Check**

When enabled, checks whether the client IP address is within one of the specified IP Ranges.

**amster** attribute: `ipRangeCheckEnabled`

**ssoadm** attribute: `openam-auth-adaptive-ip-range-check`

**IP Range**

For IPv4, specifies a list of IP ranges either in CIDR-style notation (`x.x.x.x/YY`) or as a range from one address to another (`x.x.x.y.y.y.y`, meaning from `x.x.x.x` to `y.y.y.y`).

amster attribute: ipRange

ssoadm attribute: openam-auth-adaptive-ip-range-range

Score

Sets the value to add to the total score if the user fails the IP Range Check.

amster attribute: ipRangeScore

ssoadm attribute: openam-auth-adaptive-ip-range-score

Invert Result

When enabled, adds the Score to the total score if the user passes the IP Range Check.

amster attribute: invertIPRangeScoreEnabled

ssoadm attribute: openam-auth-adaptive-ip-range-invert

IP Address History

The following properties are available under the IP Address History tab:

IP History Check

When enabled, checks whether the client IP address matches one of the known values stored on the profile attribute you specify. This check therefore requires that AM have access to the user profile.

amster attribute: ipHistoryCheckEnabled

ssoadm attribute: openam-auth-adaptive-ip-history-check

History size

Specifies how many IP address values to retain on the profile attribute you specify.

Default: 5

amster attribute: ipHistoryCount

ssoadm attribute: openam-auth-ip-adaptive-history-count

Profile Attribute Name

Specifies the name of the user profile attribute in which to store known IP addresses. Ensure the specified attribute exists in your user data store; the iphistory attribute does not exist by default, and it is not created when performing AM schema updates.
Default: `iphistory`

**amster** attribute: `ipHistoryProfileAttribute`

**ssoadm** attribute: `openam-auth-adaptive-ip-history-attribute`

### Save Successful IP Address

When enabled, saves new client IP addresses to the known IP address list following successful authentication.

**amster** attribute: `saveSuccessfulIP`

**ssoadm** attribute: `openam-auth-adaptive-ip-history-save`

### Score

Sets the value to add to the total score if the user fails the IP History Check.

Default: 1

**amster** attribute: `ipHistoryScore`

**ssoadm** attribute: `openam-auth-adaptive-ip-history-score`

### Invert Result

When enabled, adds the Score to the total score if the user passes the IP History Check.

**amster** attribute: `invertIPHistoryScore`

**ssoadm** attribute: `openam-auth-adaptive-ip-history-invert`

### Known Cookie

The following properties are available under the Known Cookie tab:

#### Cookie Value Check

When enabled, checks whether the client browser request has the specified cookie and optional cookie value.

**amster** attribute: `knownCookieCheckEnabled`

**ssoadm** attribute: `openam-auth-adaptive-known-cookie-check`

#### Cookie Name

Specifies the name of the cookie for which AM checks when you enable the Cookie Value Check.

**amster** attribute: `knownCookieName`
**Cookie Value**

Specifies the value of the cookie for which AM checks. If no value is specified, AM does not check the cookie value.

**Save Cookie Value on Successful Login**

When enabled, saves the cookie as specified in the client's browser following successful authentication. If no Cookie Value is specified, the value is set to 1.

**Score**

Sets the value to add to the total score if user passes the Cookie Value Check.

Default: 1

**Invert Result**

When enabled, adds the Score to the total score if the user passes the Cookie Value Check.

**Device Cookie**

The following properties are available under the Device Cookie tab:

**Device Registration Cookie Check**

When enabled, the cookie check passes if the client request contains the cookie specified in Cookie Name.
Cookie Name

Specifies the name of the cookie for the Device Registration Cookie Check.

Default: Device

**amster** attribute: `deviceCookieName`

**ssoadm** attribute: `openam-auth-adaptive-device-cookie-name`

Save Device Registration on Successful Login

When enabled, saves the specified cookie with a hashed device identifier value in the client's browser following successful authentication.

**amster** attribute: `saveDeviceCookieValueOnSuccessfulLogin`

**ssoadm** attribute: `openam-auth-adaptive-device-cookie-save`

Score

Sets the value to add to the total score if the user fails the Device Registration Cookie Check.

Default: 1

**amster** attribute: `deviceCookieScore`

**ssoadm** attribute: `openam-auth-adaptive-device-cookie-score`

Invert Result

When enabled, adds the Score to the total score if the user passes the Device Registration Cookie Check.

**amster** attribute: `invertDeviceCookieScore`

**ssoadm** attribute: `openam-auth-adaptive-device-cookie-invert`

Time Since Last Login

The following properties are available under the Time Since Last Login tab:

**Time since Last login Check**

When enabled, checks whether the client browser request has the specified cookie that holds the encrypted last login time, and check that the last login time is more recent than a maximum number of days you specify.

**amster** attribute: `timeSinceLastLoginCheckEnabled`
**Cookie Name**

Specifies the name of the cookie holding the encrypted last login time value.

- **amster** attribute: `timeSinceLastLoginCookieName`
- **ssoadm** attribute: `openam-auth-adaptive-time-since-last-login-cookie-name`

**Max Time since Last login**

Specifies a threshold age of the last login time in days. If the client's last login time is more recent than the number of days specified, then the client successfully passes the check.

- **amster** attribute: `maxTimeSinceLastLogin`
- **ssoadm** attribute: `openam-auth-adaptive-time-since-last-login-value`

**Save time of Successful Login**

When enabled, saves the specified cookie with the current time encrypted as the last login value in the client's browser following successful authentication.

- **amster** attribute: `saveLastLoginTimeOnSuccessfulLogin`
- **ssoadm** attribute: `openam-auth-adaptive-time-since-last-login-save`

**Score**

Sets the value to add to the total score if the user fails the Time Since Last Login Check.

Default: 1

- **amster** attribute: `timeSinceLastLoginScore`
- **ssoadm** attribute: `openam-auth-adaptive-time-since-last-login-score`

**Invert Result**

When enabled, adds the Score to the total score if the user passes the Time Since Last Login Check.

- **amster** attribute: `invertTimeSinceLastLoginScore`
- **ssoadm** attribute: `openam-auth-adaptive-time-since-last-login-invert`

**Profile Attribute**

The following properties are available under the Profile Attribute tab:
Profile Risk Attribute check
When enabled, checks whether the user profile contains the specified attribute and value.

**amster** attribute: `profileRiskAttributeCheckEnabled`

**ssoadm** attribute: `openam-auth-adaptive-risk-attribute-check`

Attribute Name
Specifies the attribute to check on the user profile for the specified value.

**amster** attribute: `profileRiskAttributeName`

**ssoadm** attribute: `openam-auth-adaptive-risk-attribute-name`

Attribute Value
Specifies the value to match on the profile attribute. If the attribute is multi-valued, a single match is sufficient to pass the check.

**amster** attribute: `profileRiskAttributeValue`

**ssoadm** attribute: `openam-auth-adaptive-risk-attribute-value`

Score
Sets the value to add to the total score if the user fails the Profile Risk Attribute Check.
Default: 1

**amster** attribute: `profileRiskAttributeScore`

**ssoadm** attribute: `openam-auth-adaptive-risk-attribute-score`

Invert Result
When enabled, adds the Score to the total score if the user passes the Profile Risk Attribute Check.

**amster** attribute: `invertProfileRiskAttributeScore`

**ssoadm** attribute: `openam-auth-adaptive-risk-attribute-invert`

Geo Location
The following properties are available under the Geo Location tab:

**Geolocation Country Code Check**
When enabled, checks whether the client IP address location matches a country specified in the Valid Country Codes list.
ssoadm attribute: forgerock-am-auth-adaptive-geo-location-check

Geolocation Database Location

Path to GeoIP data file used to convert IP addresses to country locations. The geolocation database is not packaged with AM. You can download the GeoIP Country database from MaxMind. Use the binary .mmdb file format, rather than .csv. You can use the GeoLite Country database for testing.

amster attribute: geolocationDatabaseLocation

ssoadm attribute: openam-auth-adaptive-geo-location-database

Valid Country Codes

Specifies the list of country codes to match. Use | to separate multiple values.

ssoadm attribute: openam-auth-adaptive-geo-location-values

Score

Value to add to the total score if the user fails the Geolocation Country Code Check.

Default: 1

amster attribute: geolocationScore

ssoadm attribute: openam-auth-adaptive-geo-location-score

Invert Result

When enabled, adds the Score to the total score if the user passes the Geolocation Country Code Check.

amster attribute: invertGeolocationScore

ssoadm attribute: openam-auth-adaptive-geo-location-invert

Request Header

The following properties are available under the Request Header tab:

Request Header Check

When enabled, checks whether the client browser request has the specified header with the correct value.

amster attribute: requestHeaderCheckEnabled

ssoadm attribute: openam-auth-adaptive-req-header-check
Request Header Name

Specifies the name of the request header for the Request Header Check.

**amster** attribute: `requestHeaderName`

**ssoadm** attribute: `openam-auth-adaptive-req-header-name`

Request Header Value

Specifies the value of the request header for the Request Header Check.

**amster** attribute: `requestHeaderValue`

**ssoadm** attribute: `openam-auth-adaptive-req-header-value`

Score

Value to add to the total score if the user fails the Request Header Check.

Default: 1

**amster** attribute: `requestHeaderScore`

**ssoadm** attribute: `openam-auth-adaptive-req-header-score`

Invert Result

When enabled, adds the Score to the total score if the user passes the Request Header Check.

**amster** attribute: `invertRequestHeaderScore`

**ssoadm** attribute: `openam-auth-adaptive-req-header-invert`

Anonymous Authentication Module Properties

**amster** service name: `AnonymousModule`

**ssoadm** service name: `iPlanetAMAuthAnonymousService`

Valid Anonymous Users

Specifies the list of valid anonymous user IDs that can log in without submitting a password.

**amster** attribute: `validAnonymousUsers`

**ssoadm** attribute: `iplanet-am-auth-anonymous-users-list`

When user accesses the default module instance login URL, then the module prompts the user to enter a valid anonymous user name.
The default module instance login URL is defined as follows:

```
protocol://hostname:port/deploy_URI/XUI/?module=Anonymous&org=org_name#login
```

**Default Anonymous User Name**

Specifies the user ID assigned by the module if the Valid Anonymous Users list is empty. The default value is `anonymous`. Note that the anonymous user must be defined in the realm.

- **amster** attribute: `defaultAnonymousUsername`
- **ssoadm** attribute: `iplanet-am-auth-anonymous-default-user-name`

**Case Sensitive User IDs**

When enabled, determines whether case matters for anonymous user IDs.

- **amster** attribute: `caseSensitiveUsernameMatchingEnabled`
- **ssoadm** attribute: `iplanet-am-auth-anonymous-case-sensitive`

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 (default) to any positive integer and is set for each authentication method. The higher number corresponds to a higher level of authentication. If you configured your authentication levels from a 0 to 5 scale, then an authentication level of 5 will require the highest level of authentication.

After a user has authenticated, AM stores the authentication level in the session token. When the user attempts to access a protected resource, the token is presented to the application. The application uses the token's value to determine if the user has the correct authentication level required to access the resource. If the user does not have the required authentication level, the application can prompt the user to authenticate with a higher authentication level.

- **amster** attribute: `authenticationLevel`
- **ssoadm** attribute: `iplanet-am-auth-anonymous-auth-level`

**Certificate Authentication Module Properties**

- **amster** service name: `CertificateModule`
- **ssoadm** service name: `iPlanetAMAAuthCertService`

**Match Certificate in LDAP**

When enabled, AM searches for a match for the user's certificate in the LDAP directory. If a match is found and not revoked according to a CRL or OCSP validation, then authentication succeeds.
amster attribute: matchCertificateInLdap

ssoadm attribute: iplanet-am-auth-cert-check-cert-in-ldap

Subject DN Attribute Used to Search LDAP for Certificates

Indicates which attribute and value in the certificate Subject DN is used to find the LDAP entry holding the certificate.

Default: CN

amster attribute: ldapCertificateAttribute

ssoadm attribute: iplanet-am-auth-cert-attr-check-ldap

Match Certificate to CRL

When enabled, AM checks whether the certificate has been revoked according to a CRL in the LDAP directory.

amster attribute: matchCertificateToCRL

ssoadm attribute: iplanet-am-auth-cert-check-crl

Issuer DN Attribute Used to Search LDAP for CRLs

Indicates which attribute and value in the certificate Issuer DN is used to find the CRL in the LDAP directory.

Default: CN

If only one attribute is specified, the LDAP search filter used to find the CRL based on the Subject DN of the CA certificate is \((\text{attr-name}=\text{attr-value-in-subject-DN})\).

For example, if the subject DN of the issuer certificate is \(\text{C=US, CN=Some CA, serialNumber=123456}\), and the attribute specified is \(\text{CN}\), then the LDAP search filter used to find the CRL is \((\text{CN=Some CA})\).

In order to distinguish among different CRLs for the same CA issuer, specify multiple attributes separated by commas (,) in the same order they occur in the subject DN. When multiple attribute names are provided in a comma-separated list, the LDAP search filter used is \((\text{cn}=\text{attr1=value-in-subject-DN}, \text{attr2=value-in-subject-DN}, ..., \text{attrN=value-in-subject-DN})\).

For example, if the subject DN of the issuer certificate is \(\text{C=US, CN=Some CA, serialNumber=123456}\), and the attributes specified are \(\text{CN, serialNumber}\), then the LDAP search filter used to find the CRL is \((\text{cn=CN=Some CA, serialNumber=123456})\).

amster attribute: crlMatchingCertificateAttribute

ssoadm attribute: iplanet-am-auth-cert-attr-check-crl
HTTP Parameters for CRL Update

Specifies parameters to be included in any HTTP CRL call to the CA that issued the certificate.

This property supports key pairs of values separated by commas, for example, `param1=value1, param2=value2`.

If the client or CA contains the Issuing Distribution Point Extension, AM uses this information to retrieve the CRL from the distribution point.

**amster attribute:** `crlHttpParameters`

**ssoadm attribute:** `iplanet-am-auth-cert-param-get-crl`

Match CA Certificate to CRL

When enabled, AM checks the CRL against the CA certificate to ensure it has not been compromised.

**amster attribute:** `matchCACertificateToCRL`

**ssoadm attribute:** `sunAMValidateCACert`

Cache CRLs in memory

(LDAP distribution points only) When enabled, AM caches CRLs.

**amster attribute:** `cacheCRLsInMemory`

**ssoadm attribute:** `openam-am-auth-cert-attr-cache-crl`

Update CA CRLs from CRLDistributionPoint

When enabled, AM updates the CRLs stored in the LDAP directory store.

**amster attribute:** `updateCRLsFromDistributionPoint`

**ssoadm attribute:** `openam-am-auth-cert-update-crl`

OCSP Validation

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

You must configure OSCP for AM under Configure > Server Defaults or Deployment > Servers > Server Name > Security.

**amster attribute:** `ocspValidationEnabled`

**ssoadm attribute:** `iplanet-am-auth-cert-check-ocsp`
LDAP Server Where Certificates are Stored

Identifies the LDAP server that holds users' certificates. The property has the format `ldap_server:port`, for example, `ldap1.example.com:636`. To configure a secure connection, enable the Use SSL/TLS for LDAP Access property.

AM servers can be associated with LDAP servers by writing multiple chains with the format `openam_server|ldapserver:port`, for example, `openam.example.com|ldap1.example.com:636`.

**amster attribute**: `certificateLdapServers`

**ssoadm attribute**: `iplanet-am-auth-cert-ldap-provider-url`

LDAP Search Start or Base DN

Valid base DN for the LDAP search, such as `dc=example,dc=com`. To associate AM servers with different search base DNs, use the format `openam_server|base_dn`, for example, `openam.example.com|dc=example,dc=com openam1.test.com|dc=test, dc=com`.

**amster attribute**: `ldapSearchStartDN`

**ssoadm attribute**: `iplanet-am-auth-cert-start-search-loc`

LDAP Server Authentication User, LDAP Server Authentication Password

If AM stores attributes in the LDAP directory, for example to manage account lockout, or if the LDAP directory requires that AM authenticate in order to read users' attributes, then AM needs the DN and password to authenticate to the LDAP directory.

**ssoadm attributes**: `iplanet-am-auth-cert-principal-user`, and `iplanet-am-auth-cert-principal-passwd`

Use SSL/TLS for LDAP Access

If you use SSL/TLS for LDAP access, AM must be able to trust the LDAP server certificate.

**amster attribute**: `sslEnabled`

**ssoadm attribute**: `iplanet-am-auth-cert-use-ssl`

Certificate Field Used to Access User Profile

If the user profile is in a different entry from the user certificate, then this can be different from subject DN attribute used to find the entry with the certificate. When you select other, provide an attribute name in the Other Certificate Field Used to Access User Profile text box.

**amster attribute**: `certificateAttributeToProfileMapping`

**ssoadm attribute**: `iplanet-am-auth-cert-user-profile-mapper`

Valid values: `subject DN`, `subject CN`, `subject UID`, `email address`, `other`, and `none`. 
Other Certificate Field Used to Access User Profile

This field is only used if the Certificate Field Used to Access User Profile attribute is set to other. This field allows a custom certificate field to be used as the basis of the user search.

**amster** attribute: `otherCertificateAttributeToProfileMapping`

**ssoadm** attribute: `iplanet-am-auth-cert-user-profile-mapper-other`

SubjectAltNameExt Value Type to Access User Profile

Specifies how to look up the user profile:

- Let the property default to `none` to give preference to the Certificate Field Used to Access User Profile or Other Certificate Field Used to Access User Profile attributes when looking up the user profile.

- Select `RFC822Name` if you want AM to look up the user profile from an RFC 822 style name.

- Select `UPN` if you want AM to look up the user profile as the User Principal Name attribute used in Active Directory.

**amster** attribute: `certificateAttributeProfileMappingExtension`

**ssoadm** attribute: `iplanet-am-auth-cert-user-profile-mapper-ext`

Trusted Remote Hosts

Defines a list of hosts trusted to send certificates to AM, such as load balancers doing SSL termination.

Valid values are `none`, `any`, and `IP_ADDR`, where `IP_ADDR` is one or more IP addresses of trusted hosts that can send client certificates to AM.

**amster** attribute: `trustedRemoteHosts`

**ssoadm** attribute: `iplanet-am-auth-cert-gw-cert-auth-enabled`

HTTP Header Name for Client Certificates

Specifies the name of the HTTP request header containing the certificate, which can be in one of the following formats:

- Raw PEM-encoded.
- PEM-encoded first, and then URL-encoded.

If Trusted Remote Hosts is set to `any` or specifies the IP address of the trusted host (for example, an SSL-terminated load balancer) that can supply client certificates to AM, the administrator must specify the header name in this attribute.
amster attribute: clientCertificateHttpHeaderName

ssoadm attribute: sunAMHttpParamName

Use only Certificate from HTTP request header

When enabled, AM always uses the client certificate from the HTTP header rather than the certificate the servlet container receives during the SSL handshake.

Default: false

ssoadm attribute: iplanet-am-auth-cert-gw-cert-preferred

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

amster attribute: authenticationLevel

ssoadm attribute: iplanet-am-auth-cert-auth-level

Data Store Authentication Module Properties

amster service name: DataStoreModule

ssoadm service name: sunAMAuthDataStoreService

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

amster attribute: authenticationLevel

ssoadm attribute: sunAMAuthDataStoreAuthLevel

Device ID (Match) Authentication Module Properties

amster service name: DeviceIdMatchModule

ssoadm service name: iPlanetAMAuthDeviceIdMatchService

Client-Side Script Enabled

Enable Device ID (Match) to send JavaScript in an authentication page to the device to collect data about the device by a self-submitting form.


**Client-Side Script, Server-Side Script**

Specify the client-side and server-side Javascript scripts to use with the Device Id (Match) module.

To view and modify the contents of the scripts, navigate to Realms > *Realm Name* > Scripts and select the name of the script.

If you change the client-side script, you must make a corresponding change in the server-side script to account for the specific addition or removal of an element.

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**Device ID (Save) Authentication Module Properties**

**Automatically store new profiles**

When enabled, AM assumes user consent to store new profiles. After successful HOTP confirmation, AM stores the new profile automatically.

**Maximum stored profile quantity**

Sets the maximum number of stored profiles on the user's record.
Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `iplanet-am-auth-device-id-save-auth-level`

Federation Authentication Module Properties

**amster** service name: `FederationModule`

**ssoadm** service name: `sunAMAuthFederationService`

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `sunAMAuthFederationAuthLevel`

Amster Authentication Module Properties

**amster** service name: `AmsterModule`

**ssoadm** service name: `iPlanetAMAuthAmsterService`

Authorized Keys

Specifies the location of the `authorized_keys` file that contains the private and public keys used to validate remote **amster** client connections.

The default location for the `authorized_keys` file is the `/path/to/openam/security/keys/amster/` directory. Its content is similar to an OpenSSH `authorized_keys` file.

**amster** attribute: `forgerock-am-auth-amster-authorized-keys`

Enabled

When enabled, allows **amster** clients to authenticate using PKI. When disabled, allows **amster** clients to authenticate using interactive login only.

**amster** attribute: `forgerock-am-auth-amster-enabled`

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.
amster attribute: forgerock-am-auth-amster-auth-level

ForgeRock Authenticator (OATH) Authentication Module Properties

amster service name: AuthenticatorOathModule

ssoadm service name: iPlanetAMAuthenticatorOATHService

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

ssoadm attribute: iplanet-am-auth-fr-oath-auth-level

One-Time Password Length

Sets the length of the OTP to six digits or longer. The default value is six.

amster attribute: passwordLength

ssoadm attribute: iplanet-am-auth-fr-oath-password-length

Minimum Secret Key Length

The minimum number of hexadecimal characters allowed for the secret key.

amster attribute: minimumSecretKeyLength

ssoadm attribute: iplanet-am-auth-fr-oath-min-secret-key-length

OATH Algorithm to Use

Select whether to use HOTP or TOTP. You can create an authentication chain to allow for a greater variety of devices. The default value is HOTP.

amster attribute: oathAlgorithm

ssoadm attribute: iplanet-am-auth-fr-oath-algorithm

HOTP Window Size

The window that the OTP device and the server counter can be out of sync. For example, if the window size is 100 and the server's last successful login was at counter value 2, then the server will accept an OTP from device counter 3 to 102. The default value is 100.

amster attribute: hotpWindowSize

ssoadm attribute: iplanet-am-auth-fr-oath-hotp-window-size
Add Checksum Digit

Adds a checksum digit at the end of the HOTP password to verify the OTP was generated correctly. This is in addition to the actual password length. Set this only if your device supports it. The default value is No.

**amster** attribute: `addChecksumToOtpEnabled`

**ssoadm** attribute: `iplanet-am-auth-fr-oath-add-checksum`

Truncation Offset

Advanced feature that is device-specific. Let this value default unless you know your device uses a truncation offset. The default value is -1.

**amster** attribute: `truncationOffset`

**ssoadm** attribute: `iplanet-am-auth-fr-oath-truncation-offset`

TOTP Time Step Interval

The time interval for which an OTP is valid. For example, if the time step interval is 30 seconds, a new OTP will be generated every 30 seconds, and an OTP will be valid for 30 seconds. The default value is 30 seconds.

**amster** attribute: `totpTimeStepInterval`

**ssoadm** attribute: `iplanet-am-auth-fr-oath-size-of-time-step`

TOTP Time Steps

The number of time step intervals that the system and the device can be off before password resynchronization is required. For example, if the number of TOTP time steps is 2 and the TOTP time step interval is 30 seconds, the server will allow an 89 second clock skew between the client and the server—two 30 second steps plus 29 seconds for the interval in which the OTP arrived. The default value is 2.

**amster** attribute: `totpTimeStepsInWindow`

**ssoadm** attribute: `iplanet-am-auth-fr-oath-steps-in-window`

One Time Password Max Retry

The number of times entry of the OTP may be attempted. Minimum is 1, maximum is 10.

Default: 3

**amster** attribute: `oauthOtpMaxRetry`

**ssoadm** attribute: `forgerock-oath-max-retry`
Maximum Allowed Clock Drift

The maximum acceptable clock skew before authentication fails. When this value is exceeded, the user must re-register the device.

- **amster** attribute: `totpMaximumClockDrift`
- **ssoadm** attribute: `openam-auth-fr-oath-maximum-clock-drift`

Name of the Issuer

A value that appears as an identifier on the user's device. Common choices are a company name, a web site, or an AM realm.

- **amster** attribute: `oathIssuerName`
- **ssoadm** attribute: `openam-auth-fr-oath-issuer-name`

ForgeRock Authenticator (Push) Authentication Module Properties

- **amster** service name: `AuthenticatorPushModule`
- **ssoadm** service name: `iPlanetAMAuthAuthenticatorPushService`

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

- **amster** attribute: `authenticationLevel`
- **ssoadm** attribute: `forgerock-am-auth-authenticatorpush-auth-level`

Return Message Timeout (ms)

The period of time (in milliseconds) within which a push notification should be replied to.

Default: **120000**

- **amster** attribute: `timeoutInMilliSeconds`
- **ssoadm** attribute: `forgerock-am-auth-push-message-response-timeout`

Login Message

Text content of the push message, which is used for the notification displayed on the registered device. The following variables can be used in the message:

`{{user}}`

Replaced with the username value of the account registered in the ForgeRock Authenticator app, for example *Demo*. 
{{issuer}}

Replaced with the issuer value of the account registered in the ForgeRock Authenticator app, for example *ForgeRock*.

Default: `Login attempt from {{user}} at {{issuer}}`

**amster** attribute: `pushMessage`

**ssoadm** attribute: `forgerock-am-auth-push-message`

---

**ForgeRock Authenticator (Push) Registration Authentication Module Properties**

**amster** service name: `AuthenticatorPushRegistrationModule`

**ssoadm** service name: `iPlanetAMAuthAuthenticatorPushRegistrationService`

### Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `forgerock-am-auth-push-reg-auth-level`

### Issuer Name

A value that appears as an identifier on the user's device. Common choices are a company name, a web site, or an AM realm.

**amster** attribute: `issuer`

**ssoadm** attribute: `forgerock-am-auth-push-reg-issuer`

### Registration Response Timeout (ms)

The period of time (in milliseconds) to wait for a response to the registration QR code. If no response is received during this time the QR code times out and the registration process fails.

Default: `120000`

**amster** attribute: `timeoutInMilliSeconds`

**ssoadm** attribute: `forgerock-am-auth-push-message-registration-response-timeout`

### Background Color

The background color in hex notation to display behind the issuer's logo within the ForgeRock Authenticator app.
Default: #519387

amster attribute: bgcolour

ssoadm attribute: forgerock-am-auth-hex-bgcolour

Image URL

The location of an image to download and display as the issuer's logo within the ForgeRock Authenticator app.

amster attribute: imgUrl

ssoadm attribute: forgerock-am-auth-img-url

App Store App URL

URL of the app to download on the App Store.

Default: https://itunes.apple.com/app/forgerock-authenticator/id1038442926 (the ForgeRock Authenticator app)

amster attribute: appleLink

ssoadm attribute: forgerock-am-auth-apple-link

Google Play URL

URL of the app to download on Google Play.


amster attribute: googleLink

ssoadm attribute: forgerock-am-auth-google-link

HOTP Authentication Module Properties

amster service name: HotpModule

ssoadm service name: sunAMAuthHOTPService

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

amster attribute: authenticationLevel

ssoadm attribute: sunAMAuthHOTPAuthLevel
SMS Gateway Implementation Class

Specifies the class the HOTP module uses to send SMS or email messages. Specify a class that implements the `com.sun.identity.authentication.modules.hotp.SMSGateway` interface to customize the SMS gateway implementation.

**amster** attribute: `smsGatewayClass`

**ssoadm** attribute: `sunAMAuthHOTPSMSGatewayImplClassName`

Mail Server Host Name

Specifies the hostname of the mail server supporting SMTP for electronic mail.

**amster** attribute: `smtpHostname`

**ssoadm** attribute: `sunAMAuthHOTPSMTPHostName`

Mail Server Host Port

Specifies the outgoing mail server port. The default port is 25, 465 (when connecting over SSL), or 587 (for StartTLS).

**amster** attribute: `smtpHostPort`

**ssoadm** attribute: `sunAMAuthHOTPSMTPHostPort`

Mail Server Authentication Username

Specifies the username for AM to connect to the mail server.

**amster** attribute: `smtpUsername`

**ssoadm** attribute: `sunAMAuthHOTPSMTPUserName`

Mail Server Authentication Password

Specifies the password for AM to connect to the mail server.

**amster** attribute: `smtpUserPassword`

**ssoadm** attribute: `sunAMAuthHOTPSMTPUserPassword`

Mail Server Secure Connection

Specifies whether to connect to the mail server securely. If enabled, AM must be able to trust the server certificate.

The possible values for this property are:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSL</td>
<td>Secure Connection</td>
</tr>
<tr>
<td>Non</td>
<td>Non-secure Connection</td>
</tr>
</tbody>
</table>
Start TLS

**amster** attribute: `smtpSslEnabled`

**ssoadm** attribute: `sunAMAuthHOTPSMTPSSLEnabled`

**Email From Address**

Specifies the **From:** address when sending a one-time password by mail.

**amster** attribute: `smtpFromAddress`

**ssoadm** attribute: `sunAMAuthHOTPSMTPFromAddress`

**One-Time Password Validity Length (in minutes)**

Specifies the amount of time, in minutes, the one-time passwords are valid after they are generated. The default is 5 minutes.

**amster** attribute: `otpValidityDuration`

**ssoadm** attribute: `sunAMAuthHOTPPasswordValidityDuration`

**One-Time Password Length**

Sets the length of one-time passwords.

**amster** attribute: `otpLength`

**ssoadm** attribute: `sunAMAuthHOTPPasswordLength`

Valid values: 6 and 8.

**One Time Password Max Retry**

The number of times entry of the OTP may be attempted. Minimum is 1, maximum is 10.

Default: 3

**amster** attribute: `oathOtpMaxRetry`

**ssoadm** attribute: `forgerock-oath-max-retry`

**One-Time Password Delivery**

Specifies whether to send the one-time password by SMS, by mail, or both.

**amster** attribute: `otpDeliveryMethod`

**ssoadm** attribute: `sunAMAuthHOTPPasswordDelivery`

Valid values: **SMS**, **E-mail**, and **SMS and E-mail**.
Mobile Phone Number Attribute Name

Provides the attribute name used for the text message. The default value is `telephoneNumber`.

**amster** attribute: `userProfileTelephoneAttribute`

**ssoadm** attribute: `openamTelephoneAttribute`

Mobile Carrier Attribute Name

Specifies a user profile attribute that contains a mobile carrier domain for sending SMS messages.

The uncustomized AM user profile does not have an attribute for the mobile carrier domain. You can:

- Customize the AM user profile by adding a new attribute to it. Then you can populate the new attribute with users' SMS messaging domains.

  All mobile carriers and bulk SMS messaging services have associated SMS messaging domains. For example, Verizon uses `vtext.com`, T-Mobile uses `tmomail.net`, and the TextMagic service uses `textmagic.com`. If you plan to send text messages internationally, determine whether the messaging service requires a country code.

- Leave the value for Mobile Carrier Attribute Name blank, and let AM default to sending SMS messages using `txt.att.net` for all users.

**amster** attribute: `mobileCarrierAttribute`

**ssoadm** attribute: `openamSMSCarrierAttribute`

Email Attribute Name

Provides the attribute name used to email the OTP. The default value is `mail` (email).

**amster** attribute: `userProfileEmailAttribute`

**ssoadm** attribute: `openamEmailAttribute`

Auto Send OTP Code

When enabled, configures the HOTP module to automatically generate an email or text message when users begin the login process.

**ssoadm** attribute: `sunAMAuthHOTPAutoClicking`

HTTP Basic Authentication Module Properties

**amster** service name: `HttpBasicModule`
ssoadm service name: iPlanetAMAuthHTTPBasicService

**Backend Module Name**

Specifies the module that checks the user credentials. The credentials are then supplied to either a data store or other identity repository module for authentication.

*amster* attribute: backendModuleName

ssoadm attribute: iplanet-am-auth-http-basic-module-configured

Valid values: LDAP and DataStore.

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

*amster* attribute: authenticationLevel

ssoadm attribute: iplanet-am-auth-httpbasic-auth-level

**JDBC Authentication Module Properties**

*amster* service name: JdbcModule

ssoadm service name: sunAMAuthJDBCService

**Connection Type**

Determines how the module obtains the connection to the database.

*amster* attribute: connectionType

ssoadm attribute: sunAMAuthJDBCConnectionType

Valid values: JNDI and JDBC.

**Connection Pool JNDI Name**

Specifies the URL of the connection pool for JNDI connections. Refer to your web container's documentation for instructions on setting up the connection pool.

*amster* attribute: connectionPoolJndiName

ssoadm attribute: sunAMAuthJDBCJndiName

**JDBC Driver**

Specifies the JDBC driver to use for JDBC connections.
Install a suitable Oracle or MySQL driver in the container where AM is installed, for example in the `/path/to/tomcat/webapps/openam/WEB-INF/lib` path. You can add it to the AM `.war` file when you deploy AM.

**amster** attribute: `jdbcDriver`

**ssoadm** attribute: `sunAMAuthJDBCDriver`

### JDBC URL

Specifies the URL to connect to the database when using a JDBC connection.

**amster** attribute: `jdbcUrl`

**ssoadm** attribute: `sunAMAuthJDBCUrl`

### Database Username, Database Password

Specifies the user name and password used to authenticate to the database when using a JDBC connection.

**ssoadm** attribute: `sunAMAuthJDBCUser` and `sunAMAuthJDBCPassword`

### Password Column Name

Specifies the database column name where passwords are stored.

**amster** attribute: `passwordColumn`

**ssoadm** attribute: `sunAMAuthJDBCPasswordColumn`

### Prepared Statement

Specifies the SQL query to return the password corresponding to the user to authenticate.

**amster** attribute: `passwordStatement`

**ssoadm** attribute: `sunAMAuthJDBCStatement`

### Class to Transform Password Syntax

Specifies the class that transforms the password retrieved to the same format as provided by the user.

The default class expects the password in cleartext. Custom classes must implement the `JDBCPasswordSyntaxTransform` interface.

**amster** attribute: `passwordTransformClass`

**ssoadm** attribute: `sunAMAuthJDBCPasswordSyntaxTransformPlugin`
Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `sunAMAuthJDBCAuthLevel`

---

**Note**

AM provides two properties, `iplanet-am-admin-console-invalid-chars` and `iplanet-am-auth-ldap-invalid-chars`, that store LDAP-related special characters that are not allowed in username searches.

When using JDBC databases, consider adding the '%' wildcard character to the `iplanet-am-admin-console-invalid-chars` and `iplanet-am-auth-ldap-invalid-chars` properties. By default, the '%' character is not included in the properties.

---

**LDAP Authentication Module Properties**

**amster** service name: `LdapModule`

**ssoadm** service name: `iPlanetAMAuthLDAPService`

**Primary LDAP Server**

**Secondary LDAP Server**

Directory servers generally use built-in data replication for high availability. Thus, a directory service likely consists of a pool of replicas to which AM can connect to retrieve and update directory data. You set up primary and secondary servers in case a replica is down due to maintenance or to a problem with a particular server.

Set one or more primary and optionally, one or more secondary directory server for each AM server. For the current AM server, specify each directory server as a `host:port` combination. For other AM servers in the deployment, you can specify each directory server as `servername|host:port`, where `servername` is the FQDN portion of the AM server from the list under Deployment > Servers, and `host:port` identifies the directory server.

For example, if the `servername` that is listed is `https://openam.example.com:8443/openam`, and the directory server is accessible at `opendj.example.com:1636`, you would enter `openam.example.com|opendj.example.com:1636`.

When authenticating users from a directory server that is remote to AM, set the primary server values, and optionally the secondary server values. Primary servers have priority over secondary servers.

**ssoadm** attributes are: primary is `iplanet-am-auth-ldap-server`; secondary is `iplanet-am-auth-ldap-server2`.

Both properties take more than one value; thus, allowing more than one primary or secondary remote server, respectively. Assuming a multi-data center environment, AM determines priority within the primary and secondary remote servers, respectively, as follows:

- Every LDAP server that is mapped to the current AM instance has highest priority.

  For example, if you are connected to openam1.example.com and ldap1.example.com is mapped to that AM instance, then AM uses ldap1.example.com.

- Every LDAP server that was not specifically mapped to a given AM instance has the next highest priority.

  For example, if you have another LDAP server, ldap2.example.com, that is not connected to a specific AM server and if ldap1.example.com is unavailable, AM connects to the next highest priority LDAP server, ldap2.example.com.

- LDAP servers that are mapped to different AM instances have the lowest priority.

  For example, if ldap3.example.com is connected to openam3.example.com and ldap1.example.com and ldap2.example.com are unavailable, then openam1.example.com connects to ldap3.example.com.

If you want to use SSL or StartTLS to initiate a secure connection to a data store, then scroll down to enable SSL/TLS Access to LDAP Server. Make sure that AM can trust the server's certificates when using this option.

**ssoadm attributes:** openam-auth-ldap-connection-mode

Possible values: LDAP, LDAPS, and StartTLS

**DN to Start User Search**

LDAP data is organized hierarchically, a bit like a file system on Windows or UNIX. More specific DNs likely result in better search performance. When configuring the module for a particular part of the organization, you can perhaps start searches from a specific organizational unit, such as ou=sales,dc=example,dc=com.

If multiple entries exist with identical search attribute values, make this value specific enough to return only one entry.

**ssoadm attribute:** iplanet-am-auth-ldap-base-dn

**Bind User DN, Bind User Password**

If AM stores attributes in the directory, for example to manage account lockout, or if the directory requires that AM authenticate in order to read users' attributes, then AM needs the DN and password to authenticate to the directory.

The default is uid=admin. Make sure that password is correct before you log out. If it is incorrect, you will be locked out. If this should occur, you can login with the superuser DN, which by default
is uid=amAdmin,ou=People,AM-deploy-base, where AM-deploy-base is the value you set during AM configuration.

**ssoadm** attributes: iplanet-am-auth-ldap-bind-dn, iplanet-am-auth-ldap-bind-passwd

**Attribute Used to Retrieve User Profile**

**Attributes Used to Search for a User to be Authenticated**

**User Search Filter**

**Search Scope**

LDAP searches for user entries return entries with attribute values matching the filter you provide. For example, if you search under ou=people,dc=example,dc=com with a filter "(mail=bjensen@example.com)", then the directory returns the entry that has mail=bjensen@example.com. In this example the attribute used to search for a user is mail. Multiple attribute values mean the user can authenticate with any one of the values. For example, if you have both uid and mail, then Barbara Jensen can authenticate with either bjensen or bjensen@example.com.

Should you require a more complex filter for performance, you add that to the User Search Filter text box. For example, if you search on mail and add User Search Filter (objectClass/inetOrgPerson), then AM uses the resulting search filter (&(mail=address)(objectClass/inetOrgPerson)), where address is the mail address provided by the user.

Scope OBJECT means search only the entry specified as the DN to Start User Search, whereas ONELEVEL means search only the entries that are directly children of that object. SUBTREE means search the entry specified and every entry under it.


**LDAP Connection Mode**

If you want use SSL or StartTLS to initiate a secure connection to a data store, AM must be able to trust LDAP certificates, either because the certificates were signed by a CA whose certificate is already included in the trust store used by the container where AM runs, or because you imported the certificates into the trust store.

**ssoadm** attribute: openam-auth-ldap-connection-mode

Possible values: LDAP, LDAPS, and StartTLS

**Return User DN to DataStore**

When enabled, and AM uses the directory service as the user store, the module returns the DN, rather than the User ID. From the DN value, AM uses the RDN to search for the user profile. For example, if a returned DN value is uid=demo,ou=people,dc=openam,dc=example,dc=org, AM uses uid=demo to search the data store.

**amster** attribute: returnUserDN

**ssoadm** attribute: iplanet-am-auth-ldap-return-user-dn
User Creation Attributes

This list lets you map (external) attribute names from the LDAP directory server to (internal) attribute names used by AM.

**amster** attribute: profileAttributeMappings

**ssoadm** attribute: iplanet-am-ldap-user-creation-attr-list

Minimum Password Length

Specifies the minimum acceptable password length.

**amster** attribute: minimumPasswordLength

**ssoadm** attribute: iplanet-am-auth-ldap-min-password-length

LDAP Behera Password Policy Support

When enabled, support interoperability with servers that implement the Internet-Draft, Password Policy for LDAP Directories.

Support for this Internet-Draft is limited to the LDAP authentication module. Other components of AM, such as the password change functionality in the /idm/EndUser page, do not support the Internet-Draft. In general, outside of the LDAP authentication module, AM binds to the directory server as an administrator, such as Directory Manager. When AM binds to the directory server as an administrator rather than as an end user, many features of the Internet-Draft password policies do not apply.

**amster** attribute: beheraPasswordPolicySupportEnabled

**ssoadm** attribute: iplanet-am-auth-ldap-behera-password-policy-enabled

Trust All Server Certificates

When enabled, blindly trust server certificates, including self-signed test certificates.

**amster** attribute: trustAllServerCertificates

**ssoadm** attribute: iplanet-am-auth-ldap-ssl-trust-all

LDAP Connection Heartbeat Interval

Specifies how often AM should send a heartbeat request to the directory server to ensure that the connection does not remain idle. Some network administrators configure firewalls and load balancers to drop connections that are idle for too long. You can turn this off by setting the value to 0 or to a negative number. To set the units for the interval use LDAP Connection Heartbeat Time Unit.

Default: 1
amster attribute: connectionHeartbeatInterval

ssoadm attribute: openam-auth-ldap-heartbeat-interval

**LDAP Connection Heartbeat Time Unit**

Specifies the time unit corresponding to LDAP Connection Heartbeat Interval.

Default: minute

amster attribute: connectionHeartbeatTimeUnit

ssoadm attribute: openam-auth-ldap-heartbeat-timeunit

**LDAP operations timeout**

Defines the timeout in milliseconds that AM should wait for a response from the directory server.

Default: 0 (means no timeout)

amster attribute: operationTimeout

ssoadm attribute: openam-auth-ldap-operation-timeout

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

amster attribute: authenticationLevel

ssoadm attribute: iplanet-am-auth-ldap-auth-level

**Legacy OAuth 2.0/OpenID Connect Authentication Module Properties**

**Important**

This authentication module is labelled as legacy. Equivalent functionality is provided by the following authentication modules:

- Social Authentication Module Properties - OAuth 2.0
- Social Authentication Module Properties - OpenID Connect 1.0

The Legacy OAuth 2.0/OpenID Connect Authentication Module will only be available in AM when upgrading from a previous version that was making use of the module in a chain. It is not available in new, clean installations since AM 5.5.

The default settings are for Facebook.
amster service name: OAuth2Module

ssoadm service name: sunAMAuthOAuthService

Client id

Specifies the OAuth 2.0 `client_id` parameter as described in section 2.2 of RFC 6749.

amster attribute: clientId

ssoadm attribute: iplanet-am-auth-oauth-client-id

Client Secret

Specifies the OAuth 2.0 `client_secret` parameter as described in section 2.3 of RFC 6749.

amster attribute: clientSecret

ssoadm attribute: iplanet-am-auth-oauth-client-secret

Authentication Endpoint URL

Specifies the URL to the endpoint handling OAuth 2.0 authentication as described in section 3.1 of RFC 6749.


amster attribute: authenticationEndpointUrl

ssoadm attribute: iplanet-am-auth-oauth-auth-service

Access Token Endpoint URL

Specifies the URL to the endpoint handling access tokens as described in section 3.2 of RFC 6749.

Default: https://graph.facebook.com/oauth/access_token.

amster attribute: accessTokenEndpointUrl

ssoadm attribute: iplanet-am-auth-oauth-token-service

User Profile Service URL

Specifies the user profile URL that returns profile information in JSON format.

Default: https://graph.facebook.com/me.

amster attribute: userProfileServiceUrl

ssoadm attribute: iplanet-am-auth-oauth-user-profile-service
Scope

Specifies a space-delimited list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework. The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

Some authorization servers use non-standard separators for scopes. Facebook, for example, takes a comma-separated list.

Default: email,read_stream (Facebook example)

amster attribute: scope

ssoadm attribute: iplanet-am-auth-oauth-scope

OAuth2 Access Token Profile Service Parameter name

Specifies the name of the parameter that contains the access token value when accessing the profile service.

Default: access_token.

amster attribute: accessTokenParameterName

ssoadm attribute: iplanet-am-auth-oauth-user-profile-param

Proxy URL

Sets the URL to the /oauth2c/OAuthProxy.jsp file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

Default: @SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp.

amster attribute: ssoProxyUrl

ssoadm attribute: iplanet-am-auth-oauth-sso-proxy-url

Account Provider

Specifies the name of the class that implements the account provider.

Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider

amster attribute: accountProviderClass

ssoadm attribute: org-forgerock-auth-oauth-account-provider

Account Mapper

Specifies the name of the class that implements the attribute mapping for the account search.
For Google implementations, use `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper`.

For Facebook implementations, use `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`.

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`

**amster attribute**: `accountMapperClass`

**ssoadm attribute**: `org-forgerock-auth-oauth-account-mapper`

### Account Mapper Configuration

Specifies the attribute configuration used to map the account of the user authenticated in the OAuth 2.0 provider to the local data store in AM. Valid values are in the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
   "sub" : "12345",
   "name" : {
      "first_name" : "Demo",
      "last_name" : "User"
   }
}
```

You can create a mapper such as:

```
name.first_name=cn
```

Default: `email=mail` and `id=facebook-id`.

**amster attribute**: `accountMapperConfiguration`

**ssoadm attribute**: `org-forgerock-auth-oauth-account-mapper-configuration`

### Attribute Mapper

Specifies the list of fully qualified class names for implementations that map attributes from the OAuth 2.0 authorization server or OpenID Connect provider to AM profile attributes.

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`

Provided implementations are:

```
org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper (can only be used when using the openid scope)

Tip

You can provide string constructor parameters by appending pipe (|) separated values.

For example, the org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper class can take two constructor parameters: a comma-separated list of attributes and a prefix to apply to their values. Specify these as follows:

org.forgerock.openam.authentication.modules.oidc.JsonAttributeMapper

amster attribute: attributeMappingClasses
ssoadm attribute: org-forgerock-auth-oauth-attribute-mapper

Attribute Mapper Configuration

Map of OAuth 2.0 provider user account attributes to local user profile attributes, with values in the form provider-attr=local-attr.

Tip

When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```
{
  "sub" : "12345",
  "name" : {
    "first_name" : "Demo",
    "last_name" : "User"
  }
}
```

You can create a mapper such as:

```
name.first_name=cn
```

Default: first_name=givenname, last_name=sn, name=cn, email@mail, id=facebook-id, first_name=facebook-fname, last_name=facebook-lname, email=facebook-email.

amster attribute: attributeMapperConfiguration
ssoadm attribute: org-forgerock-auth-oauth-attribute-mapper-configuration

Save attributes in the session

When enabled, saves the attributes in the Attribute Mapper Configuration field to the AM session.
amster attribute: saveAttributesInSession

ssoadm attribute: org-forgerock-auth-oauth-save-attributes-to-session-flag

Email attribute in OAuth2 Response

Specifies the attribute identifying the authenticated user's email address in the response from the profile service in the OAuth 2.0 provider. This setting is used to send an email message with an activation code for accounts created dynamically.

amster attribute: oauth2EmailAttribute

ssoadm attribute: org-forgerock-auth-oauth-mail-attribute

Create account if it does not exist

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.

When the OAuth 2.0/OpenID Connect client is configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the OAuth 2.0/OpenID Connect client authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide here in the OAuth 2.0/OpenID Connect client configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.

amster attribute: createAccount

ssoadm attribute: org-forgerock-auth-oauth-createaccount-flag

Prompt for password setting and activation code

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

amster attribute: promptForPassword

ssoadm attribute: org-forgerock-auth-oauth-prompt-password-flag

Map to anonymous user

When enabled, maps the OAuth 2.0 authenticated user to the specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to the anonymous user.

amster attribute: mapToAnonymousUser
**Anonymous User**

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: `anonymous`.

**OAuth 2.0 Provider logout service**

Specifies the optional URL of the OAuth 2.0 provider's logout service, if required.

**Logout options**

Specifies whether not to log the user out without prompting from the OAuth 2.0 provider on logout, to log the user out without prompting, or to prompt the user regarding whether to log out from the OAuth 2.0 provider.

Valid values are:

- `prompt`, to ask the user whether or not to log out from the OAuth 2.0 provider.
- `logout`, to log the user out of the OAuth 2.0 provider without prompting.
- `donotlogout`, to keep the user logged in to the OAuth 2.0 provider. There is no prompt to the user.

Default: `prompt`.

**Mail Server Gateway implementation class**

Specifies the class used by the module to send email. A custom subclass of `org.forgerock.openam.authentication.modules.oauth2.EmailGateway` class can be provided.

Default: `org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl`
**ssoadm** attribute: `org-forgerock-auth-oauth-email-gwy-impl`

**SMTP host**

Specifies the host name of the mail server.

Default: `localhost`.

**amster** attribute: `smtpHostName`

**ssoadm** attribute: `org-forgerock-auth-oauth-smtp-hostname`

**SMTP port**

Specifies the SMTP port number for the mail server.

Default: `25`.

**amster** attribute: `smtpHostPort`

**ssoadm** attribute: `org-forgerock-auth-oauth-smtp-port`

**SMTP User Name, SMTP User Password**

Specifies the username and password AM uses to authenticate to the mail server.


**SMTP SSL Enabled**

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

**amster** attribute: `smtpSslEnabled`

**ssoadm** attribute: `org-forgerock-auth-oauth-smtp-ssl_enabled`

**SMTP From address**

Specifies the address of the email sender, such as `no-reply@example.com`.

Default: `info@forgerock.com`.

**amster** attribute: `smtpFromAddress`

**ssoadm** attribute: `org-forgerock-auth-oauth-smtp-email-from`

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.
Default: 0.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `iplanet-am-auth-oauth-auth-level`

### OpenID Connect validation configuration type

Validates the ID token from the OpenID Connect provider. The module needs either a URL to get the public keys for the provider or the symmetric key for an ID token signed with a HMAC-based algorithm.

By default, the configuration type is `.well-known/openid-configuration_url`. This means the module should retrieve the keys based on information in the OpenID Connect provider configuration document.

You can instead configure the authentication module to validate the ID token signature with the client secret key you provide, or to validate the ID token with the keys retrieved from the URL to the OpenID Connect provider's JSON web key set.

/oauth2/realms/root/.well-known/openid-configuration_url (Default)

Retrieve the provider keys based on the information provided in the OpenID Connect Provider Configuration Document.

Specify the URL to the document as the discovery URL.

**client_secret**

Use the client secret that you specify as the key to validate the ID token signature according to the HMAC by using the client secret to the decrypt the hash, and then checking that the hash matches the hash of the ID token JWT.

**jwk_url**

Retrieve the provider's JSON web key set as the URL that you specify.

**amster** attribute: `cryptoContextType`

**ssoadm** attribute: `openam-auth-openidconnect-crypto-context-type`

### OpenID Connect validation configuration value

Edit this field depending on the Configuration type you specified in the OpenId Connect validation configuration type field.

**amster** attribute: `cryptoContextValue`

**ssoadm** attribute: `openam-auth-openidconnect-crypto-context-value`
### Token Issuer

Required when the `openid` scope is included. Value must match the `iss` field in the issued ID token. For example, `accounts.google.com`.

The issuer value MUST be provided when OAuth 2.0 Mix-Up Mitigation is enabled. For more information, see "OAuth 2.0 Mix-Up Mitigation".

**amster** attribute: `idTokenIssuer`

**ssoadm** attribute: `openam-auth-openidconnect-issuer-name`

---

**Note**

Old uses of `DefaultAccountMapper` are automatically upgraded to the equivalent default implementations.

The following table shows endpoint URLs for AM when configured as an OAuth 2.0 provider. For details, see the OAuth 2.0 Guide. The default endpoints are for Facebook as the OAuth 2.0 provider. In addition to the endpoint URLs you can set other fields, like scope and attribute mapping, depending on the provider you use:

<table>
<thead>
<tr>
<th>AM Field</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorization Endpoint URL</td>
<td><code>/oauth2/authorize</code> under the deployment URL.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>https://openam.example.com:8443/openam/oauth2/realms/root/authorize</code></td>
</tr>
<tr>
<td>Access Token Endpoint URL</td>
<td><code>/oauth2/access_token</code> under the deployment URL.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>https://openam.example.com:8443/openam/oauth2/realms/root/access_token</code></td>
</tr>
<tr>
<td>User Profile Service URL</td>
<td><code>/oauth2/tokeninfo</code> under the deployment URL.</td>
</tr>
<tr>
<td></td>
<td>Example: <code>https://openam.example.com:8443/openam/oauth2/realms/root/tokeninfo</code></td>
</tr>
</tbody>
</table>

---

This AM endpoint can take additional parameters. In particular, you must specify the realm if the AM OAuth 2.0 provider is configured for a subrealm rather than the Top Level Realm.

When making a REST API call, specify the realm in the path component of the endpoint. You must specify the entire hierarchy of the realm, starting at the Top Level Realm. Prefix each realm in the hierarchy with the `realms/` keyword. For example `/realms/root/realms/customers/realms/europe`.

For example, if the OAuth 2.0 provider is configured for the subrealm `customers` within the Top Level Realm, then the authentication endpoint URL is as follows: `https://openam.example.com:8443/openam/oauth2/realms/root/realms/customers/authorize`.

The `/oauth2/authorize` endpoint can also take `module` and `service` parameters. Use either as described in "Authenticating (Browser)", where `module` specifies the authentication module instance to use or `service` specifies the authentication chain to use when authenticating the resource owner.
OAuth 2.0 Mix-Up Mitigation

AM has added a new property to the OAuth 2.0 authentication module, `openam-auth-oauth-mix-up-mitigation-enabled`. This OAuth 2.0 Mix-Up Mitigation property controls whether the OAuth 2.0 authentication module carries out additional verification steps when it receives the authorization code from the authorization server. This setting should be only enabled when the authorization server also supports OAuth 2.0 Mix-Up Mitigation.

**OAuth 2.0 Mix-Up Mitigation Enabled**

Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter.

For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.

**Note**

At the time of this release, Facebook, Google, and Microsoft identity providers do not support this draft.

**Note**

Consult with the authorization server's documentation on what value it uses for the issuer field.

**amster** attribute: `mixUpMitigation`

**ssoadm** attribute: `openam-auth-oauth-mix-up-mitigation-enabled`

On the AM console, the field Token Issuer must be provided when the OAuth 2.0 Mix-Up Mitigation feature is enabled. The authorization code response will contain an issuer value (`iss`) that will be validated by the client. When the module is an OAuth2-only module (that is, OIDC is not used), the issuer value needs to be explicitly set in the Token Issuer field, so that the validation can succeed.

**Note**

Consult with the authorization server's documentation on what value it uses for the issuer field.

**MSISDN Authentication Module Properties**

**amster** service name: `MsisdnModule`

**ssoadm** service name: `sunAMAuthMSISDNService`

**Trusted Gateway IP Address**

Specifies a list of IP addresses of trusted clients that can access MSISDN modules. Either restrict the clients allowed to access the MSISDN module by adding each IPv4 or IPv6 address here, or leave the list empty to allow all clients to access the module. If you specify the value `none`, no clients are allowed access.
amster attribute: trustedGatewayIPAddresses

ssoadm attribute: sunAMAuthMSISDNTrustedGatewayList

MSISDN Number Search Parameter Name

Specifies a list of parameter names that identify which parameters to search in the request header or cookie header for the MSISDN number. For example, if you define x-Cookie-Param, AM_NUMBER, and COOKIE-ID, the MSISDN authentication service checks those parameters for the MSISDN number.

amster attribute: msisdnParameterNames

ssoadm attribute: sunAMAuthMSISDNParameterNameList

LDAP Server and Port

Specifies the LDAP server FQDN and its port in the format ldap_server:port. AM servers can be paired with LDAP servers and ports by adding entries with the format AM_server|ldap_server:port, for example, openam.example.com|ldap1.example.com:649.

To use SSL or TLS for security, enable the SSL/TLS Access to LDAP property. Make sure that AM can trust the servers' certificates when using this option.

amster attribute: ldapProviderUrl

ssoadm attribute: sunAMAuthMSISDNLdapProviderUrl

LDAP Start Search DN

Specifies the DN of the entry where the search for the user's MSISDN number should start. AM servers can be paired with search base DNs by adding entries with the format AM_server|base_dn. For example, openam.example.com|dc=openam,dc=forgerock,dc=com.

amster attribute: baseSearchDN

ssoadm attribute: sunAMAuthMSISDNBaseDn

Attribute To Use To Search LDAP

Specifies the name of the attribute in the user's profile that contains the MSISDN number to search for the user. The default is sunIdentityMSISDNNumber.

amster attribute: userProfileMsisdnAttribute

ssoadm attribute: sunAMAuthMSISDNUserSearchAttribute

LDAP Server Authentication User, LDAP Server Authentication Password

Specifies the bind DN and password of the service account AM uses to authenticate to the directory server. The default is uid=admin.
ssoadm attribute: sunAMAuthMSISDNPrincipalUser and sunAMAuthMSISDNPrincipalPasswd.

SSL/TLS for LDAP Access

When enabled, AM uses LDAPS or StartTLS to connect to the directory server. If you choose to enable SSL or TLS, then make sure that AM can trust the servers' certificates.

amster attribute: ldapSslEnabled
ssoadm attribute: sunAMAuthMSISDNUseSsl

MSISDN Header Search Attribute

Specifies which elements are searched for the MSISDN number. The possible values are:

searchCookie
    To search the cookie.

searchRequest
    To search the request header.

searchParam
    To search the request parameters.

amster attribute: msisdnRequestSearchLocations
ssoadm attribute: sunAMAuthMSISDNHeaderSearch

LDAP Attribute Used to Retrieve User Profile

Specify the LDAP attribute that is used during a search to return the user profile for MSISDN authentication service. The default is uid.

amster attribute: msisdnUserNamingAttribute
ssoadm attribute: sunAMAuthMSISDNUserNamingAttribute

Return User DN to DataStore

When enabled, this option allows the authentication module to return the DN instead of the User ID. AM thus does not need to perform an additional search with the user ID to find the user's entry.

Enable this option only when the AM directory is the same as the directory configured for MSISDN searches.

amster attribute: returnUserDN
ssoadm attribute: sunAMAuthMSISDNReturnUserDN
## Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `sunAMAuthMSISDNAuthLevel`

### OATH Authentication Module Properties

**amster** service name: `OathModule`

**ssoadm** service name: `iPlanetAMAuthOATHService`

## Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `iplanet-am-auth-oath-auth-level`

### One Time Password Length

Sets the length of the OTP to six digits or longer. The default value is six.

**amster** attribute: `passwordLength`

**ssoadm** attribute: `iplanet-am-auth-oath-password-length`

### Minimum Secret Key Length

The minimum number of hexadecimal characters allowed for the secret key.

**amster** attribute: `minimumSecretKeyLength`

**ssoadm** attribute: `iplanet-am-auth-oath-min-secret-key-length`

### Secret Key Attribute Name

The name of the attribute where the key will be stored in the user profile.

**amster** attribute: `secretKeyAttribute`

**ssoadm** attribute: `iplanet-am-auth-oath-secret-key-attribute`

### OATH Algorithm to Use

Select whether to use HOTP or TOTP. You can create an authentication chain to allow for a greater variety of devices. The default value is HOTP.
amster attribute: oathAlgorithm

ssoadm attribute: iplanet-am-auth-oath-algorithm

HOTP Window Size

The window that the OTP device and the server counter can be out of sync. For example, if the window size is 100 and the server's last successful login was at counter value 2, then the server will accept an OTP from device counter 3 to 102. The default value is 100.

amster attribute: hotpWindowSize

ssoadm attribute: iplanet-am-auth-oath-hotp-window-size

Note

For information on resetting the HOTP counter, see "Resetting Registered Devices by using REST".

Counter Attribute Name

The name of the HOTP attribute where the counter will be stored in the user profile.

amster attribute: hotpCounterAttribute

ssoadm attribute: iplanet-am-auth-oath-hotp-counter-attribute

Add Checksum Digit

Adds a checksum digit at the end of the HOTP password to verify the OTP was generated correctly. This is in addition to the actual password length. Set this only if your device supports it. The default value is No.

amster attribute: addChecksum

ssoadm attribute: iplanet-am-auth-oath-add-checksum

Truncation Offset

Advanced feature that is device-specific. Let this value default unless you know your device uses a truncation offset. The default value is -1.

amster attribute: truncationOffset

ssoadm attribute: iplanet-am-auth-oath-truncation-offset

TOTP Time Step Interval

The time interval for which an OTP is valid. For example, if the time step interval is 30 seconds, a new OTP will be generated every 30 seconds, and an OTP will be valid for 30 seconds. The default value is 30 seconds.
amster attribute: `timeStepSize`

ssoadm attribute: `iplanet-am-auth-oath-size-of-time-step`

**One Time Password Max Retry**

The number of times entry of the OTP may be attempted. Minimum is 1, maximum is 10.

Default: 3

amster attribute: `oathOtpMaxRetry`

ssoadm attribute: `forgerock-oath-max-retry`

**TOTP Time Steps**

The number of time step intervals that the system and the device can be off before password resynchronization is required. For example, if the number of TOTP time steps is 2 and the TOTP time step interval is 30 seconds, the server will allow an 89 second clock skew between the client and the server—two 30 second steps plus 29 seconds for the interval in which the OTP arrived. The default value is 2.

amster attribute: `stepsInWindow`

ssoadm attribute: `iplanet-am-auth-oath-steps-in-window`

**Last Login Time Attribute**

The name of the attribute where both HOTP and TOTP authentication will store information on when a person last logged in.

amster attribute: `lastLoginTimeAttribute`

ssoadm attribute: `iplanet-am-auth-oath-last-login-time-attribute-name`

**The Shared Secret Provider Class**

The class that processes the user profile attribute where the user's secret key is stored. The name of this attribute is specified in the Secret Key Attribute Name property.

Default: `org.forgerock.openam.authentication.modules.oath.plugins.DefaultSharedSecretProvider`

ssoadm attribute: `forgerock-oath-sharedsecret-implementation-class`

**Clock Drift Attribute Name**

The user profile attribute where the clock drift is stored. If this field is not specified, then AM does not check for clock drift.

ssoadm attribute: `forgerock-oath-observed-clock-drift-attribute-name`
Maximum Allowed Clock Drift

The maximum acceptable clock drift before authentication fails. If this value is exceeded, the user must register their device again.

The Maximum Allowed Clock Drift value should be greater than the TOTP Time Steps value.

**ssoadm** attribute: `forgerock-oath-maximum-clock-drift`

OpenID Connect id_token bearer Authentication Module Properties

The default settings are for Google's provider.

**amster** service name: `SocialAuthOpenIDModule`

**ssoadm** service name: `amAuthOpenIdConnect`

Account provider class

The account provider provides the means to search for and create OpenID Connect users given a set of attributes.

Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

**amster** attribute: `accountProviderClass`

**ssoadm** attribute: `openam-auth-openidconnect-account-provider-class`

OpenID Connect validation configuration type

In order to validate the ID token from the OpenID Connect provider, the module needs either a URL to get the public keys for the provider, or the symmetric key for an ID token signed with a HMAC-based algorithm; AM ignores keys specified in JWT headers, such as `jku` and `jwe`.

By default, the configuration type is `.well-known/openid-configuration_url`. This means the module should retrieve the keys based on information in the OpenID Connect Provider Configuration Document.

You can instead configure the authentication module to validate the ID token signature with the client secret key you provide, or to validate the ID token with the keys retrieved from the URL to the OpenID Connect provider's JSON web key set.

`.well-known/openid-configuration_url` *(Default)*

Retrieve the provider keys based on the information provided in the OpenID Connect Provider Configuration Document.

Specify the URL to the document as the discovery URL.
client_secret

Use the client secret that you specify as the key to validate the ID token signature according to the HMAC, using the client secret to decrypt the hash and then checking that the hash matches the hash of the ID token JWT.

jwk_url

Retrieve the provider's JSON web key set at the URL that you specify.

amster attribute: cryptoContextType

ssoadm attribute: openam-auth-openidconnect-crypto-context-type

OpenID Connect validation configuration value

Specifies the discovery URL, JWK or the client secret corresponding to the configuration type selected in the OpenID Connect validation configuration type property.

amster attribute: cryptoContextValue

ssoadm attribute: openam-auth-openidconnect-crypto-context-value

Name of header referencing the ID Token

Specifies the name of the HTTP request header to search for the ID token.

Default: oidc_id_token

amster attribute: idTokenHeaderName

ssoadm attribute: openam-auth-openidconnect-header-name

Name of OpenID Connect ID Token Issuer

Corresponds to the expected issue identifier value in the iss field of the ID token.

Default: accounts.google.com

amster attribute: idTokenIssuer

ssoadm attribute: openam-auth-openidconnect-issuer-name

Mapping of jwt attributes to local LDAP attributes

Maps OpenID Connect ID token claims to local user profile attributes, allowing the module to retrieve the user profile based on the ID token.

In OpenID Connect, an ID token is represented as a JSON Web Token (JWT). The ID Token section of the OpenID Connect Core 1.0 specification defines a number of claims included in the ID token for all flows. Additional claims depend on the scopes requested of the OpenID Connect provider.
For each item in the map, the key is the ID token field name and the value is the local user profile attribute name.

Default: mail=email, uid=sub

**ssoadm** attribute: openam-auth-openidconnect-jwt-to-local-attribute-mappings

**Audience name**

Specifies a case-sensitive audience name for this OpenID Connect authentication module. Used to check that the ID token received is intended for this module as an audience.

Default: example

**amster** attribute: audienceName

**ssoadm** attribute: openam-auth-openidconnect-audience-name

**List of accepted authorized parties**

Specifies a list of case-sensitive strings and/or URIs from which this authentication module accepts ID tokens. This list is checked against the authorized party claim of the ID token.

Default: AuthorizedPartyExample http://www.example.com/authorized/party

**amster** attribute: acceptedAuthorizedParties

**ssoadm** attribute: openam-auth-openidconnect-accepted-authorized-parties

**Principal Mapper class**

Specifies the class that implements the mapping of the OpenID Connect end user to an AM account. The default principal mapper uses the mapping of local attributes to ID token attributes to find a user profile.

Default: org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper

**amster** attribute: principalMapperClass

**ssoadm** attribute: openam-auth-openidconnect-principal-mapper-class

**Persistent Cookie Authentication Module Properties**

**amster** service name: PersistentCookieModule

**ssoadm** service name: iPlanetAMAuthPersistentCookieService

**Idle Timeout**

Specifies the maximum idle time between requests in hours. If that time is exceeded, the cookie is no longer valid.
ssoadm attribute: openam-auth-persistent-cookie-idle-time

Max Life

Specifies the maximum life of the cookie in hours.

ssoadm attribute: openam-auth-persistent-cookie-max-life

Enforce Client IP

When enabled, enforces that the persistent cookie can only be used from the same client IP to which the cookie was issued.

ssoadm attribute: openam-auth-persistent-cookie-enforce-ip

Use Secure Cookie

When enabled, adds the "Secure" attribute to the persistent cookie.

ssoadm attribute: openam-auth-persistent-cookie-secure-cookie

Use HTTP Only Cookie

When enabled, adds the HttpOnly attribute to the persistent cookie.

ssoadm attribute: openam-auth-persistent-cookie-http-only-cookie

RADIUS Authentication Module Properties

amster service name: RadiusModule

ssoadm service name: iPlanetAMAuthRadiusService

Primary Radius Servers, Secondary Radius Servers

Specify one or more primary and secondary RADIUS servers.

When configuring RADIUS servers, specify their IP address or FQDN. Configuring multiple servers allows you to map a RADIUS server to a specific AM instance in the form of $AM_instance | RADIUS_server$, where the AM instance is also specified by its IP address or FQDN.

Tip

Ensure each RADIUS server listens to the port specified in the Port Number field.

When authenticating users from a directory server that is remote to AM, set the primary values and, optionally, the secondary server values. Assuming a multi-data center environment, AM determines priority within the primary and secondary remote servers, respectively, as follows:

- Every RADIUS server that is mapped to the current AM instance has highest priority.
• Every RADIUS server that was not specifically mapped to a given AM instance has the next highest priority.

• RADIUS servers that are mapped to different AM instances have the lowest priority.

**Note**
AM does not use round-robin load balancing to set priority. AM uses an active-passive algorithm, determining the highest priority to the first available server within the primary server list. If no primary servers are available, AM uses the secondary remote server.

**ssoadm** attribute: `primary is iplanet-am-auth-radius-server1; secondary is iplanet-am-auth-radius-server2`

**Shared Secret**
Specify the shared secret for RADIUS authentication. The shared secret should be as secure as a well-chosen password.

**amster** attribute: `sharedSecret`

**ssoadm** attribute: `iplanet-am-auth-radius-secret`

**Port Number**
Specify the RADIUS server port.

Default is 1645.

**amster** attribute: `serverPortNumber`

**ssoadm** attribute: `iplanet-am-auth-radius-server-port`

**Timeout**
Specify how many seconds to wait for the RADIUS server to respond. The default value is 3 seconds.

**amster** attribute: `serverTimeout`

**ssoadm** attribute: `iplanet-am-auth-radius-timeout`

**Health Check Interval**
Used for failover. Specify how often AM performs a health check on a previously unavailable RADIUS server by sending an invalid authentication request.

Default: 5 minutes

**amster** attribute: `healthCheckInterval`
ssoadm attribute: openam-auth-radius-healthcheck-interval

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

amster attribute: authenticationLevel

ssoadm attribute: iplanet-am-auth-radius-auth-level

SAE Authentication Module Properties

amster service name: SaeModule

ssoadm service name: sunAMAuthSAEService

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

ssoadm service name: sunAMAuthSAEAuthLevel

SAML2 Authentication Module Properties

amster service name: Saml2Module

ssoadm service name: iPlanetAMAuthSAML2Service

Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

ssoadm attribute: iplanet-am-auth-saml2-auth-level

IDP Entity ID

Specifies the identity provider (IDP) for authentication requests to this module. Specify the name of a SAML v2.0 entity provider that is defined in the SAML2 authentication module's realm.

You can find configured entity providers in the AM console under Federation. The Realm column identifies the realm in which an entity provider has been configured.

amster attribute: entityId

ssoadm attribute: forgerock-am-auth-saml2-entity-name
SP MetaAlias

Specifies the local alias for the service provider (SP).

For service providers configured in the Top Level Realm, use the format /SP Name.

For service providers configured in subrealms, use the format /Realm Name/SP Name.

To find the local aliases for entity providers in the AM console, navigate to Realms > Realm Name > Applications > Federation > Entity Providers > Entity Provider Name > Services.

amster attribute: metaAlias

ssoadm attribute: forgerock-am-auth-saml2-meta-alias

Allow IDP to Create NameID

Specifies whether the IDP should create a new identifier for the authenticating user if none exists.

A value of true permits the IDP to create an identifier for the authenticating user if none exists. A value of false indicates a request to constrain the IDP from creating an identifier.

For detailed information, see the section on the AllowCreate property in SAML Version 2.0 Errata 05.

Default: true

amster attribute: allowCreate

ssoadm attribute: forgerock-am-auth-saml2-allow-create

Linking Authentication Chain

Specifies an authentication chain that is invoked when a user requires authentication to the SP.

Authentication to the SP is required when the authentication module running on the SP is unable to determine the user's identity based on the assertion received from the IDP. In this case, the linking authentication chain is invoked to allow the end user to link their remote and local accounts.

amster attribute: loginChain

ssoadm attribute: forgerock-am-auth-saml2-login-chain

Comparison Type

Specifies a comparison method to evaluate authentication context classes or statements. The value specified in this property overrides the value set in the SP configuration under Realms > Realm Name > Applications > Federation > Entity Providers > Service Provider Name > Assertion Content > Authentication Context > Comparison Type.
Valid comparison methods are **exact**, **minimum**, **maximum**, or **better**.

For more information about the comparison methods, see the section on the `<RequestedAuthnContext>` element in Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.

Default: **exact**

**amster** attribute: authComparison

**ssoadm** attribute: forgerock-am-auth-saml2-auth-comparison

### Authentication Context Class Reference

Specifies one or more URIs for authentication context classes to be included in the SAML request. Authentication context classes are unique identifiers for an authentication mechanism. The SAML v2.0 protocol supports a standard set of authentication context classes, defined in Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0. In addition to the standard authentication context classes, you can specify customized authentication context classes.

Any authentication context class that you specify in this field must be supported for the service provider. To determine which authentication context classes are supported, locate the list of authentication context classes that are available to the SP under Realms > Realm Name > Applications > Federation > Entity Providers > Service Provider Name > Assertion Content > Authentication Context, and then review the values in the Supported column.

When specifying multiple authentication context classes, use the | character to separate the classes.


**amster** attribute: authnContextClassRef

**ssoadm** attribute: forgerock-am-auth-saml2-authn-context-class-ref

### Authentication Context Declaration Reference

Specifies one or more URIs that identify authentication context declarations. This field is optional.

When specifying multiple URIs, use the | character to separate the URIs.

For more information, see the section on the `<RequestedAuthnContext>` element in Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0.

**amster** attribute: authnContextDeclRef
ssoadm attribute: forgerock-am-auth-saml2-authn-context-decl-ref

**Request Binding**

Specifies the format used to send the authentication request from the SP to the IDP.

Valid values are [HTTP-Redirect](#) and [HTTP-POST](#).

Default: [HTTP-Redirect](#)


**Response Binding**

Specifies the format used to send the response from the IDP to the SP.

A value of [HTTP-POST](#) indicates that the HTTP POST binding with a self-submitting form should be used in assertion processing. A value of [HTTP-Artifact](#) indicates that the HTTP Artifact binding should be used.

Default: [HTTP-Artifact](#)


**Force IDP Authentication**

Specifies whether the IDP should force authentication or can reuse existing security contexts.

A value of *true* indicates that the IDP should force authentication. A value of *false* indicates that the IDP can reuse existing security contexts.

amster attribute: forceAuthn

ssoadm attribute: forgerock-am-auth-saml2-force-authn

**Passive Authentication**

Specifies whether the IDP should use passive authentication or not. Passive authentication requires the IDP to only use authentication methods that do not require user interaction. For example, authenticating using an X.509 certificate.

A value of *true* indicates that the IDP should authenticate passively. A value of *false* indicates that the IDP should not authenticate passively.

amster attribute: isPassive

ssoadm attribute: forgerock-am-auth-saml2-is-passive
NameID Format

Specifies a SAML name ID format to be requested in the SAML authentication request.

Default: urn:oasis:names:tc:SAML:2.0:nameid-format:persistent

- **amster** attribute: `nameIdFormat`
- **ssoadm** attribute: `forgerock-am-auth-saml2-name-id-format`

Single Logout Enabled

Specifies whether AM should attempt to log out of the user's IDP session during session logout.

When enabling SAML v2.0 single logout, you must also configure the post-authentication processing class for the authentication chain containing the SAML2 authentication module to `org.forgerock.openam.authentication.modules.saml2.SAML2PostAuthenticationPlugin`.

For more information about configuring single logout when implementing SAML v2.0 federation using the SAML2 authentication module, see "Configuring SLO in Integrated Mode (Chains)" in the SAML v2.0 Guide.

Default: `false`

- **amster** attribute: `sloEnabled`
- **ssoadm** attribute: `forgerock-am-auth-saml2-slo-enabled`

Single Logout URL

Specifies the URL to which the user is forwarded after successful IDP logout. Configure this property only if you have enabled SAML v2.0 single logout by selecting the Single Logout Enabled check box.

- **amster** attribute: `sloRelay`
- **ssoadm** attribute: `forgerock-am-auth-saml2-slo-relay`

Scripted Authentication Module Properties

- **amster** service name: `scripted`
- **ssoadm** service name: `iPlanetAMAuthScriptedService`

Use the following settings at the realm level when configuring an individual scripted authentication module, in the AM console under Realms > Realm Name > Authentication > Modules.

Client-Side Script Enabled

When enabled, the module includes the specified client-side script in the login page to be executed on the user-agent prior to the server-side script.
amster attribute: `clientScriptEnabled`

**Client-Side Script**

Specifies the ID of the script to include in the login page. This script is run on the user-agent prior to the server-side script. This script must be written in a language the user-agent can interpret, such as JavaScript, even if the server-side script is written in Groovy.

To create, view, or modify the content of the scripts, navigate to Realms > Realm Name > Scripts.

amster attribute: `clientScript`

Server Side Script

Specifies the ID of the script to run in AM after the client-side script has completed.

To create, view, or modify the content of the scripts, navigate to Realms > Realm Name > Scripts.

amster attribute: `serverScript`

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the scripted authentication module.

The value can range from 0 to any positive integer.

amster attribute: `authenticationLevel`

In the AM console, navigate to Configure > Global Services > Scripting > Secondary Configurations > Server-Side Script Type, > Secondary Configurations > EngineConfiguration.

On the EngineConfiguration page, configure the following settings for the scripting engine of the selected type:

**Server-side Script Timeout**

Specifies the maximum execution time any individual script should take on the server (in seconds). AM terminates scripts which take longer to run than this value.

ssoadm attribute: `serverTimeout`
Core thread pool size

Specifies the initial number of threads in the thread pool from which scripts operate. AM will ensure the pool contains at least this many threads.

_ssoadm_ attribute: _coreThreads_

Maximum thread pool size

Specifies the maximum number of threads in the thread pool from which scripts operate. If no free thread is available in the pool, AM creates new threads in the pool for script execution up to the configured maximum. It is recommended to set the maximum number of threads to 300.

_ssoadm_ attribute: _maxThreads_

Thread pool queue size

Specifies the number of threads to use for buffering script execution requests when the maximum thread pool size is reached.

For short, CPU-bound scripts, consider a small pool size and larger queue length. For I/O-bound scripts, for example, REST calls, consider a larger maximum pool size and a smaller queue.

Not hot-swappable: restart server for changes to take effect.

_ssoadm_ attribute: _queueSize_

Thread idle timeout (seconds)

Specifies the length of time (in seconds) for a thread to be idle before AM terminates created threads. If the current pool size contains the number of threads set in _Core thread pool size_, then idle threads will not be terminated, maintaining the initial pool size.

_ssoadm_ attribute: _idleTimeout_

Java class whitelist

Specifies the list of class name patterns allowed to be invoked by the script. Every class accessed by the script must match at least one of these patterns.

You can specify the class name as-is or use a regular expression.

_ssoadm_ attribute: _whiteList_

Java class blacklist

Specifies the list of class name patterns that are NOT allowed to be invoked by the script. The blacklist is applied AFTER the whitelist to exclude those classes. Access to a class specified in both the whitelist and the blacklist will be denied.

You can specify the class name to exclude as-is or use a regular expression.
**Use system SecurityManager**

When enabled, AM makes a call to the `System.getSecurityManager().checkPackageAccess(...)` method for each class that is accessed. The method throws `SecurityException` if the calling thread is not allowed to access the package.

**Note**

This feature only takes effect if the security manager is enabled for the JVM.

**SecurID Authentication Module Properties**

**Important**

To use the SecurID authentication module, you must first build an AM `.war` file that includes the supporting library. For more information, see "Enabling RSA SecurID Support" in the *Installation Guide*.

**amster** service name: `securid`

**ssoadm** service name: `iPlanetAMAuthSecurIDService`

**ACE/Server Configuration Path**

Specify the directory where the SecurID ACE/Server `sdconf.rec` file is located, which by default is expected under the AM configuration directory, such as `/path/to/openam/config/auth/ace/data`. The directory must exist before AM can use SecurID authentication.

**amster** attribute: `serverConfigPath`

**ssoadm** attribute: `iplanet-am-auth-securid-server-config-path`

**Authentication Level**

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `iplanet-am-auth-securid-auth-level`

**Social Authentication Module Properties - Instagram**

**amster** service name: `SocialAuthInstagramModule`
**ssoadm** service name: *iPlanetAMAuthSocialAuthInstagramService*

**Core**

The following properties are available under the Core tab:

**Authentication Level**

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

Default: 0

**amster** data attribute: *authenticationLevel*

**Social Provider**

Specifies the name of the social provider for which this module is being set up.

Default: *Instagram*

**amster** data attribute: *provider*

**Client Id**

Specifies the *client_id* parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

**Tip**

To register an application with Instagram and obtain an OAuth 2.0 *client_id* and *client_secret*, visit [https://www.instagram.com/developer/](https://www.instagram.com/developer/).

**amster** attribute: *clientId*

**Client Secret**

Specifies the *client_secret* parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).

**amster** attribute: *clientSecret*

**Authentication Endpoint URL**

Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).

Default: [https://api.instagram.com/oauth/authorize](https://api.instagram.com/oauth/authorize)

**amster** attribute: *authorizeEndpoint*
Access Token Endpoint URL

Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

Default: https://api.instagram.com/oauth/access_token

**amster attribute**: `tokenEndpoint`

User Profile Service URL

Specifies the user profile URL that returns profile information in JSON format.

Default: https://api.instagram.com/v1/users/self

**amster attribute**: `userInfoEndpoint`

Scope

Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

Default: `basic`

**amster attribute**: `scope`

Scope Delimiter

Specifies the delimiter used to separate scope values.

Some authorization servers use non-standard separators for scopes. Facebook, for example, uses commas.

Default: space character

**amster attribute**: `scopeDelimiter`

Subject Property

Specifies the attribute the social provider uses to identify a user.

Default: `id`

**amster attribute**: `subjectProperty`

Use Basic Auth

Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.

Valid values are:
• true
• false
Default: false

**amster** attribute: **usesBasicAuth**

### Proxy URL

Specifies the URL to the `/oauth2c/OAuthProxy.jsp` file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

Default: `@SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp`

Example: `https://openam.example.com:8443/openam/oauth2c/OAuthProxy.jsp`

**amster** attribute: **ssoProxyUrl**

### OAuth 2.0 Provider Logout Service

Specifies the URL of the social provider's logout service.

To enable logout of the social authentication provider when logging out of AM, you must add `org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin` to the Authentication Post Processing Classes property. To add the class, navigate to Authentication > Settings > Post Authentication Processing.

Default: `https://instagram.com/accounts/logout`

**amster** attribute: **logoutServiceUrl**

### Logout Options

Specifies the social provider logout actions to take when logging out of AM.

Valid options are:

- **prompt**
  
  Asks the user whether or not to log out from the social provider.

- **logout**
  
  Logs the user out of the social provider without prompting.

- **donotlogout**
  
  Keeps the user logged in to the social provider. There is no prompt to the user.

Default: **prompt**
amster attribute: logoutBehaviour

Account Provisioning

The following properties are available under the Account Provisioning tab:

Use IDM as Registration Service

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the Reference.

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
- **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

Default: False

amster attribute: enableRegistrationService

Create account if it does not exist

When enabled, AM creates an account for the user if the user profile does not exist.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.

Valid values are:

- **true**
- **false**

Default: true

amster attribute: createAccount

Account Provider

Specifies the name of the class that implements the account provider.

Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider

amster attribute: accountProviderClass

Account Mapper

Specifies the name of the class that implements the attribute mapping for the account search.
Tip
You can provide string constructor parameters by appending pipe-separated () values.

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|instagram-amster`

**accountMapperClass**

Account Mapper Configuration

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form `provider-attr=local-attr`.

Tip
When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:

```java
name.first_name=cn
```

Default: `id=uid`

**accountMapperConfiguration**

Attribute Mapper

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` interface.

Provided implementations are:

- `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
- `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` - can only be used when using the `openid` scope
Tip
You can provide string constructor parameters by appending pipe-separated (|) values.

For example, the org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

```
org.forgerock.openam.authentication.modules.oidc.JsonAttributeMapper|uid|instagram-
```

Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|instagram-

amster attribute: attributeMappingClasses

Attribute Mapper Configuration

Specifies a map of social provider user account attributes to local user profile attributes with values in the form `provider-attr=local-attr`.

Tip
When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```
{
    "sub": "12345",
    "name": {
        "first_name": "Demo",
        "last_name": "User"
    }
}
```

You can create a mapper such as:

```
name.first_name=cn
```

Default:

```
id=uid
full_name=sn
username=cn
username=givenName
```

amster attribute: attributeMapperConfiguration

Map to anonymous user

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.
Valid values are:

- true
- false

Default: false

**attribute:** mapToAnonymousUser

**Anonymous User**

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: anonymous

**attribute:** anonymousUserName

**Save attributes in the session**

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:

- true
- false

Default: true

**attribute:** saveAttributesInSession

**Social Authentication Module Properties - OAuth 2.0**

**service name:** SocialAuthOAuth2Module

**ssoadm service name:** iPlanetAMAuthSocialAuthOAuth2Service

**Core**

The following properties are available under the Core tab:

**Authentication Level**

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.
Default: 0

**amster** data attribute: `authenticationLevel`

**Social Provider**

Specifies the name of the social provider for which this module is being set up.

Example: Google

**amster** data attribute: `provider`

**Client Id**

Specifies the `client_id` parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

**amster** attribute: `clientId`

**Client Secret**

Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).

**amster** attribute: `clientSecret`

**Authentication Endpoint URL**

Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).

Example: `https://accounts.google.com/o/oauth2/v2/auth`

**amster** attribute: `authorizeEndpoint`

**Access Token Endpoint URL**

Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

Example: `https://www.googleapis.com/oauth2/v4/token`

**amster** attribute: `tokenEndpoint`

**User Profile Service URL**

Specifies the user profile URL that returns profile information in JSON format.

Example: `https://www.googleapis.com/oauth2/v3/userinfo`

**amster** attribute: `userInfoEndpoint`
Scope

Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

**amster attribute:** `scope`

Scope Delimiter

Specifies the delimiter used to separate scope values.

Some authorization servers use non-standard separators for scopes. Facebook, for example, uses commas.

**amster attribute:** `scopeDelimiter`

Subject Property

Specifies the attribute the social provider uses to identify a user.

Example: `sub`

**amster attribute:** `subjectProperty`

Use Basic Auth

Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.

Valid values are:

- `true`
- `false`

Default: `true`

**amster attribute:** `usesBasicAuth`

Proxy URL

Specifies the URL to the `/oauth2c/OAuthProxy.jsp` file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

Default: `@SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp`

Example: `https://openam.example.com:8443/openam/oauth2c/OAuthProxy.jsp`

**amster attribute:** `ssoProxyUrl`
OAuth 2.0 Provider Logout Service

Specifies the URL of the social provider's logout service.

To enable logout of the social authentication provider when logging out of AM, you must add org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin to the Authentication Post Processing Classes property. To add the class, navigate to Authentication > Settings > Post Authentication Processing.

`amster` attribute: `logoutServiceUrl`

Logout Options

Specifies the social provider logout actions to take when logging out of AM.

Valid options are:

- `prompt`
  
  Asks the user whether or not to log out from the social provider.

- `logout`
  
  Logs the user out of the social provider without prompting.

- `donotlogout`
  
  Keeps the user logged in to the social provider. There is no prompt to the user.

Default: `prompt`

`amster` attribute: `logoutBehaviour`

Token Issuer

Corresponds to the expected issue identifier value in the `iss` field of the ID token.

Example: `https://accounts.google.com`

`amster` attribute: `issuerName`

OAuth 2.0 Mix-Up Mitigation Enabled

Controls whether the OAuth 2.0 authentication module carries out additional verification steps when it receives the authorization code from the authorization server.

Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the `iss` response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the `client_id` response parameter.
The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (iss) that will be validated by the client.

**Note**
Consult with the authorization server's documentation on what value it uses for the issuer field.

For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.

**amster** attribute: `mixUpMitigation`

**Account Provisioning**

The following properties are available under the Account Provisioning tab:

**Use IDM as Registration Service**

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the Reference

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
- **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

Default: **False**

**amster** attribute: `enableRegistrationService`

**Create account if it does not exist**

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.

**Important**
When configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide in the module configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.
Valid values are:

- `true`
- `false`

Default: `true`

**amster attribute: createAccount**

### Account Provider

Specifies the name of the class that implements the account provider.

Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

**amster attribute: accountProviderClass**

### Account Mapper

Specifies the name of the class that implements the attribute mapping for the account search.

Example: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-

**amster attribute: accountMapperClass**

### Account Mapper Configuration

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
   "sub" : "12345",
   "name" : {
      "first_name" : "Demo",
      "last_name" : "User"
   }
}
```

You can create a mapper such as:

```text
name.first_name=cn
```

**amster attribute: accountMapperConfiguration**
Attribute Mapper

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` interface.

Provided implementations are:

- `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
- `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` - can only be used when using the `openid` scope

**Tip**

You can provide string constructor parameters by appending pipe-separated () values.

For example, the `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

```java
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|*|google-
```

**amster** attribute: `attributeMappingClasses`

Attribute Mapper Configuration

Specifies a map of social provider user account attributes to local user profile attributes with values in the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
  "sub" : "12345",
  "name" : {
    "first_name" : "Demo",
    "last_name" : "User"
  }
}
```

You can create a mapper such as:

```java
name.first_name=cn
```

**amster** attribute: `attributeMapperConfiguration`
Prompt for password setting and activation code

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

Valid values are:

- true
- false

Default: false

**amster attribute:** promptPasswordFlag

Map to anonymous user

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.

Valid values are:

- true
- false

Default: false

**amster attribute:** mapToAnonymousUser

Anonymous User

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonyomus user, if enabled.

Default: anonymous

**amster attribute:** anonymousUserName

Save attributes in the session

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:

- true
- false
Default: true

**amster attribute:** saveAttributesInSession

### Email

The following properties are available under the Email tab:

#### Email attribute in the Response

Specifies the attribute identifying the authenticated user’s email address in the response from the profile service in the social provider. This setting is used to send an email message with an activation code for accounts created dynamically.

**amster attribute:** emailAttribute

#### Mail Server Gateway implementation class

Specifies the class used by the module to send email. A custom subclass of `org.forgerock.openam.authentication.modules.oauth2.EmailGateway` class can be provided.

Default: `org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl`

**amster attribute:** emailGateway

#### SMTP host

Specifies the host name of the mail server.

Default: localhost

**amster attribute:** smtpHost

#### SMTP port

Specifies the SMTP port number for the mail server.

Default: 25

**amster attribute:** smtpPort

#### SMTP User Name

Specifies the username AM uses to authenticate to the mail server.

**amster attribute:** smtpUsername

#### SMTP User Password

Specifies the password AM uses to authenticate to the mail server.
amster attribute: smtpPassword

SMTP SSL Enabled

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

Valid values are:

- true
- false

Default: false

amster attribute: smtpSslEnabled

SMTP From address

Specifies the address of the email sender, such as no-reply@example.com.

amster attribute: smtpFromAddress

Social Authentication Module Properties - OpenID Connect 1.0

The example settings are for Google.

amster service name: SocialAuthOpenIDModule

ssoadm service name: iPlanetAMAuthSocialAuthOpenIDService

Core

The following properties are available under the Core tab:

Social Provider

Specifies the name of the social provider for which this module is being set up.

Example: Google

amster data attribute: provider

Client Id

Specifies the client_id parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

amster attribute: clientId
Client Secret

Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).

**amster** attribute: `clientSecret`

Authentication Level

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

Default: 0

**amster** data attribute: `authenticationLevel`

Authentication Endpoint URL

Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).

Example: `https://accounts.google.com/o/oauth2/v2/auth`

**amster** attribute: `authorizeEndpoint`

Access Token Endpoint URL

Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

Example: `https://www.googleapis.com/oauth2/v4/token`

**amster** attribute: `tokenEndpoint`

User Profile Service URL

Specifies the user profile URL that returns profile information in JSON format.

Example: `https://www.googleapis.com/oauth2/v3/userinfo`

**amster** attribute: `userInfoEndpoint`

Scope

Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

Default: `openid`

**amster** attribute: `scope`
Scope Delimiter

Specifies the delimiter used to separate scope values.

Some authorization servers use non-standard separators for scopes. Facebook, for example, uses commas.

**amster attribute:** `scopeDelimiter`

Subject Property

Specifies the attribute the social provider uses to identify a user.

Example: `sub`

**amster attribute:** `subjectProperty`

Use Basic Auth

Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.

Valid values are:

- `true`
- `false`

Default: `true`

**amster attribute:** `usesBasicAuth`

Proxy URL

Specifies the URL to the `/oauth2c/OAuthProxy.jsp` file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

Default: `@SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp`

Example: `https://openam.example.com:8443/openam/oauth2c/OAuthProxy.jsp`

**amster attribute:** `ssoProxyUrl`

OAuth 2.0 Provider Logout Service

Specifies the URL of the social provider's logout service.

To enable logout of the social authentication provider when logging out of AM, you must add `org.forgerock.openam.authentication.modules.oauth2.OAuth2PostAuthnPlugin` to the Authentication Post Processing Classes property. To add the class, navigate to Authentication > Settings > Post Authentication Processing.
amster attribute: logoutServiceUrl

Logout Options

 Specifies the social provider logout actions to take when logging out of AM.
 Valid options are:

- prompt
  Asks the user whether or not to log out from the social provider.

- logout
  Logs the user out of the social provider without prompting.

- donotlogout
  Keeps the user logged in to the social provider. There is no prompt to the user.

Default: prompt

amster attribute: logoutBehaviour

Token Issuer

Corresponds to the expected issue identifier value in the iss field of the ID token.

Example: https://accounts.google.com

amster attribute: issuerName

OAuth 2.0 Mix-Up Mitigation Enabled

Controls whether the OAuth 2.0 authentication module carries out additional verification steps when it receives the authorization code from the authorization server.

Specifies that the client must compare the issuer identifier of the authorization server upon registration with the issuer value returned in the iss response parameter. If they do not match, the client must abort the authorization process. The client must also confirm that the authorization server's response is intended for the client by comparing the client's client identifier to the value of the client_id response parameter.

The Token Issuer property must be entered when the OAuth 2.0 Mix-Up Mitigation feature is enabled, so that the validation can succeed. The authorization code response will contain an issuer value (iss) that will be validated by the client.

Note
Consult with the authorization server's documentation on what value it uses for the issuer field.

For more information, see section 4 of OAuth 2.0 Mix-Up Mitigation Draft.
amster attribute: mixUpMitigation

OpenID Connect

The following properties are available under the OpenID Connect tab:

OpenID Connect validation configuration type

In order to validate the ID token from the OpenID Connect provider, the module needs either a URL to get the public keys for the provider, or the symmetric key for an ID token signed with a HMAC-based algorithm.

By default, the configuration type is `.well-known/openid-configuration_url`. This means the module should retrieve the keys based on information in the OpenID Connect Provider Configuration Document.

You can instead configure the authentication module to validate the ID token signature with the client secret key you provide, or to validate the ID token with the keys retrieved from the URL to the OpenID Connect provider's JSON web key set.

`.well-known/openid-configuration_url` (Default)

Retrieve the provider keys based on the information provided in the OpenID Connect Provider Configuration Document.

Specify the URL to the document in the OpenID Connect validation configuration value property

client_secret

Use the client secret that you specify in the Client Secret property (not the OpenID Connect validation configuration value property, which is ignored) as the key to validate the ID token signature according to the HMAC, using the client secret to the decrypt the hash and then checking that the hash matches the hash of the ID token JWT.

jwk_url

Retrieve the provider's JSON web key set at the URL that you specify in the OpenID Connect validation configuration value property.

amster attribute: cryptoContextType

OpenID Connect validation configuration value

Specifies the full URL to the discovery or JWK location, corresponding to the configuration type selected in the OpenID Connect validation configuration type property.

Example: https://accounts.google.com/.well-known/openid-configuration

amster attribute: cryptoContextValue
Account Provisioning

The following properties are available under the Account Provisioning tab:

**Use IDM as Registration Service**

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the *Reference*.

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
- **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

Default: *False*

**amster attribute**: `enableRegistrationService`

**Create account if it does not exist**

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.

**Important**

When configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide in the module configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.

Valid values are:

- **true**
- **false**

Default: *true*

**amster attribute**: `createAccount`

**Account Provider**

Specifies the name of the class that implements the account provider.
Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

**amster attribute:** `accountProviderClass`

**Account Mapper**

Specifies the name of the class that implements the attribute mapping for the account search.

**Tip**

You can provide string constructor parameters by appending pipe-separated (`|`) values.

Example: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|google-amster`

**amster attribute:** `accountMapperClass`

**Account Mapper Configuration**

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:

`name.first_name=cn`

**amster attribute:** `accountMapperConfiguration`

**Attribute Mapper**

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` interface.

Provided implementations are:
- `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`

- `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` - can only be used when using the `openid` scope

**Tip**

You can provide string constructor parameters by appending pipe-separated (`|`) values.

For example, the `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

```
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|*|google-
```

**Attribute Mapper Configuration**

Specifies a map of social provider user account attributes to local user profile attributes with values in the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```
{
  "sub" : "12345",
  "name" : {
    "first_name" : "Demo",
    "last_name" : "User"
  }
}
```

You can create a mapper such as:

```
name.first_name=cn
```

**Prompt for password setting and activation code**

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

Valid values are:

- `true`
false
Default: false

**amster attribute: promptPasswordFlag**

Map to anonymous user

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.

Valid values are:

- true
- false

Default: false

**amster attribute: mapToAnonymousUser**

Anonymous User

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: anonymous

**amster attribute: anonymousUserName**

Save attributes in the session

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:

- true
- false

Default: true

**amster attribute: saveAttributesInSession**

Email

The following properties are available under the Email tab:
Email attribute in the Response

Specifies the attribute identifying the authenticated user's email address in the response from the profile service in the social provider. This setting is used to send an email message with an activation code for accounts created dynamically.

**amster attribute:** `emailAttribute`

Mail Server Gateway implementation class

Specifies the class used by the module to send email. A custom subclass of `org.forgerock.openam.authentication.modules.oauth2.EmailGateway` class can be provided.

Default: `org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl`

**amster attribute:** `emailGateway`

SMTP host

Specifies the host name of the mail server.

Default: `localhost`

**amster attribute:** `smtpHost`

SMTP port

Specifies the SMTP port number for the mail server.

Default: `25`

**amster attribute:** `smtpPort`

SMTP User Name

Specifies the username AM uses to authenticate to the mail server.

**amster attribute:** `smtpUsername`

SMTP User Password

Specifies the password AM uses to authenticate to the mail server.

**amster attribute:** `smtpPassword`

SMTP SSL Enabled

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

Valid values are:
• true
• false

Default: false

**amster** attribute: `smtpSslEnabled`

**SMTP From address**

Specifies the address of the email sender, such as `no-reply@example.com`.

**amster** attribute: `smtpFromAddress`

---

**Social Authentication Module Properties - VKontakte**

**amster** service name: `SocialAuthVKontakteModule`

**ssoadm** service name: `iPlanetAMAuthSocialAuthVKService`

---

**Core**

The following properties are available under the Core tab:

**Social Provider**

Specifies the name of the social provider for which this module is being set up.

Default: `VKontakte`

**amster** data attribute: `provider`

**Client Id**

Specifies the `client_id` parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

**Tip**

To register an application with VKontakte and obtain an OAuth 2.0 `client_id` and `client_secret`, visit https://vk.com/apps?act=manage.

**amster** attribute: `clientId`

**Client Secret**

Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).
amster attribute: clientSecret

**Authentication Level**

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

Default: 0

amster data attribute: authenticationLevel

**Authentication Endpoint URL**

Specifies the URL to the endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).

Default: https://oauth.vk.com/authorize

amster attribute: authorizeEndpoint

**Access Token Endpoint URL**

Specifies the URL to the social provider's endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

Default: https://oauth.vk.com/access_token

amster attribute: tokenEndpoint

**User Profile Service URL**

Specifies the user profile URL that returns profile information in JSON format.

Default: https://api.vk.com/method/users.get

amster attribute: userInfoEndpoint

**Scope**

Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

amster attribute: scope

**Proxy URL**

Specifies the URL to the /oauth2c/OAuthProxy.jsp file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.
Default: @SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp

Example: https://openam.example.com:8443/openam/oauth2c/OAuthProxy.jsp

**amster attribute: ssoProxyUrl**

**Subject Property**

Specifies the attribute the social provider uses to identify a user.

Default: id

**amster attribute: subjectProperty**

**Account Provisioning**

The following properties are available under the Account Provisioning tab:

**Account Provider**

Specifies the name of the class that implements the account provider.

Default: org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider

**amster attribute: accountProviderClass**

**Use IDM as Registration Service**

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the Reference.

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
  - **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

Default: False

**amster attribute: enableRegistrationService**

**Create account if it does not exist**

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.
Important

When configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide in the module configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.

Valid values are:

- true
- false

Default: true

amster attribute: createAccount

Account Mapper

Specifies the name of the class that implements the attribute mapping for the account search.

Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|vkontakte-
amster attribute: accountMapperClass

Account Mapper Configuration

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form provider-attr=local-attr.

Tip

When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:

```ini
name.first_name=cn
```

Default: uid=uid
amster attribute: `accountMapperConfiguration`

**Attribute Mapper**

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` interface.

Provided implementations are:

- `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
- `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` - can only be used when using the `openid` scope

**Tip**

You can provide string constructor parameters by appending pipe-separated (|) values.

For example, the `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

`org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|uid|vkontakte-`

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|uid|vkontakte-`

amster attribute: `attributeMappingClasses`

**Attribute Mapper Configuration**

Specifies a map of social provider user account attributes to local user profile attributes with values in the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:
name.first_name=cn

Default:

uid=uid
givenName=full_name
first_name=cn
last_name=sn
email=mail

amster attribute: attributeMapperConfiguration

Prompt for password setting and activation code

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

Valid values are:

• true
• false

Default: false

amster attribute: promptPasswordFlag

Map to anonymous user

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.

Valid values are:

• true
• false

Default: false

amster attribute: mapToAnonymousUser

Anonymous User

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: anonymous
amster attribute: anonymousUserName

Save attributes in the session

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:

• true
• false

Default: true

amster attribute: saveAttributesInSession

Email

The following properties are available under the Email tab:

Email attribute in the Response

Specifies the attribute identifying the authenticated user's email address in the response from the profile service in the social provider. This setting is used to send an email message with an activation code for accounts created dynamically.

amster attribute: emailAttribute

Mail Server Gateway implementation class

Specifies the class used by the module to send email. A custom subclass of org.forgerock.openam.authentication.modules.oauth2.EmailGateway class can be provided.

Default: org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl

amster attribute: emailGateway

SMTP host

Specifies the host name of the mail server.

Default: localhost

amster attribute: smtpHost

SMTP port

Specifies the SMTP port number for the mail server.
Default: 25

**amster** attribute: `smtpPort`

**SMTP User Name**

Specifies the username AM uses to authenticate to the mail server.

**amster** attribute: `smtpUsername`

**SMTP User Password**

Specifies the password AM uses to authenticate to the mail server.

**amster** attribute: `smtpPassword`

**SMTP SSL Enabled**

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

Valid values are:

- `true`
- `false`

Default: `false`

**amster** attribute: `smtpSslEnabled`

**SMTP From address**

Specifies the address of the email sender, such as `no-reply@example.com`.

Default: `info@forgerock.com`

**amster** attribute: `smtpFromAddress`

---

**Social Authentication Module Properties - WeChat**

**amster** service name: `SocialAuthWeChatModule`

**ssoadm** service name: `iPlanetAMAuthSocialAuthWeChatService`

**Core**

The following properties are available under the Core tab:
Authentication Level

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

Default: 0

**amster** data attribute: `authenticationLevel`

Social Provider

Specifies the name of the social provider for which this module is being set up.

Default: WeChat

**amster** data attribute: `provider`

Client Id

Specifies the `client_id` parameter as described in section 2.2 of The OAuth 2.0 Authorization Framework (RFC 6749).

**Tip**

To register an application with WeChat and obtain an OAuth 2.0 `client_id` and `client_secret`, visit https://open.weixin.qq.com/cgi-bin/frame?t=home/web_tmpl.

**amster** attribute: `clientId`

Client Secret

Specifies the `client_secret` parameter as described in section 2.3 of The OAuth 2.0 Authorization Framework (RFC 6749).

**amster** attribute: `clientSecret`

Authentication Endpoint URL

Specifies the URL to the social provider's endpoint handling authentication as described in section 3.1 of The OAuth 2.0 Authorization Framework (RFC 6749).

Default: https://open.weixin.qq.com/connect/qrconnect

**amster** attribute: `authorizeEndpoint`

Access Token Endpoint URL

Specifies the URL to the endpoint handling access tokens as described in section 3.2 of The OAuth 2.0 Authorization Framework (RFC 6749).
Default: https://api.weixin.qq.com/sns/oauth2/access_token

**amster attribute:** `tokenEndpoint`

### User Profile Service URL

Specifies the user profile URL that returns profile information in JSON format.

Default: https://api.weixin.qq.com/sns/userinfo

**amster attribute:** `userInfoEndpoint`

### Scope

Specifies a list of user profile attributes that the client application requires, according to *The OAuth 2.0 Authorization Framework (RFC 6749)*. The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

**amster attribute:** `scope`

### ScopeDelimiter

Specifies the delimiter used to separate scope values.

Some authorization servers use non-standard separators for scopes. Facebook, for example, uses commas.

Default: space character

**amster attribute:** `scopeDelimiter`

### Subject Property

Specifies the attribute the social provider uses to identify a user.

Default: `openid`

**amster attribute:** `subjectProperty`

### Use Basic Auth

Specifies that the client uses HTTP Basic authentication when authenticating to the social provider.

Valid values are:

- **true**
- **false**

Default: false
**amster** attribute: `usesBasicAuth`

### Proxy URL

Specifies the URL to the `/oauth2c/OAuthProxy.jsp` file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

**Default:** `@SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp`

**Example:** `https://openam.example.com:8443/openam/oauth2c/OAuthProxy.jsp`

**amster** attribute: `ssoProxyUrl`

### Account Provisioning

The following properties are available under the Account Provisioning tab:

#### Use IDM as Registration Service

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the *Reference*.

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
- **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

**Default:** `False`

**amster** attribute: `enableRegistrationService`

#### Create account if it does not exist

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.

**Important**

When configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide in the module configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.
Valid values are:

- true
- false

Default: true

**amster attribute:** createAccount

**Account Provider**

Specifies the name of the class that implements the account provider.

Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

**amster attribute:** accountProviderClass

**Account Mapper**

Specifies the name of the class that implements the attribute mapping for the account search.

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|wechat`

**amster attribute:** accountMapperClass

**Account Mapper Configuration**

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:

`name.first_name=cn`

Default: openid=uid
Attribute Mapper

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper interface.

Provided implementations are:

- org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper
- org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper - can only be used when using the openid scope

For example, the org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|*|wechat-

Default: org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|wechat-

Attribute Mapper Configuration

Specifies a map of social provider user account attributes to local user profile attributes with values in the form provider-attr=local-attr.

Tip

When using the org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
    "sub" : "12345",
    "name" : {
        "first_name" : "Demo",
        "last_name" : "User"
    }
}
```

You can create a mapper such as:
**Prompt for password setting and activation code**

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

Valid values are:

- **true**
- **false**

Default: **false**

**Map to anonymous user**

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.

Valid values are:

- **true**
- **false**

Default: **false**

**Anonymous User**

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: **anonymous**
amster attribute: anonymousUserName

Save attributes in the session

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:

- true
- false

Default: true

amster attribute: saveAttributesInSession

Email

The following properties are available under the Email tab:

Email attribute in the Response

Specifies the attribute identifying the authenticated user's email address in the response from the profile service in the social provider. This setting is used to send an email message with an activation code for accounts created dynamically.

amster attribute: emailAttribute

Mail Server Gateway implementation class

Specifies the class used by the module to send email. A custom subclass of org.forgerock.openam.authentication.modules.oauth2.EmailGateway class can be provided.

Default: org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl

amster attribute: emailGateway

SMTP host

Specifies the host name of the mail server.

Default: localhost

amster attribute: smtpHost

SMTP port

Specifies the SMTP port number for the mail server.
Default: 25

**amster** attribute: `smtpPort`

### SMTP User Name

Specifies the username AM uses to authenticate to the mail server.

**amster** attribute: `smtpUsername`

### SMTP User Password

Specifies the password AM uses to authenticate to the mail server.

**amster** attribute: `smtpPassword`

### SMTP SSL Enabled

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

Valid values are:

- **true**
- **false**

Default: **false**

**amster** attribute: `smtpSslEnabled`

### SMTP From address

Specifies the address of the email sender, such as `no-reply@example.com`.

Default: `info@forgerock.com`

**amster** attribute: `smtpFromAddress`

## Social Authentication Module Properties - WeChat Mobile

**amster** service name: `SocialAuthWeChatMobileModule`

**ssoadm** service name: `iPlanetAMAuthSocialAuthWeChatMobileService`

## Core

The following properties are available under the Core tab:
Authentication Level

Specifies the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

Default: 0

amster data attribute: authenticationLevel

Social Provider

Specifies the name of the social provider for which this module is being set up.

Default: WeChat

amster data attribute: provider

User Profile Service URL

Specifies the user profile URL that returns profile information in JSON format.

Default: https://api.weixin.qq.com/sns/userinfo

amster attribute: userInfoEndpoint

Scope

Specifies a list of user profile attributes that the client application requires, according to The OAuth 2.0 Authorization Framework (RFC 6749). The list depends on the permissions that the resource owner, such as the end user, grants to the client application.

Default: snsapi_userinfo

amster attribute: scope

Subject Property

Specifies the attribute the social provider uses to identify a user.

Default: openid

amster attribute: subjectProperty

Proxy URL

Specifies the URL to the /oauth2c/OAuthProxy.jsp file, which provides AM with GET to POST proxying capabilities. Change this URL only if an external server performs the GET to POST proxying.

Default: @SERVER_PROTO@://@SERVER_HOST@:@SERVER_PORT@/@SERVER_URI@/oauth2c/OAuthProxy.jsp
Account Provisioning

The following properties are available under the Account Provisioning tab:

Use IDM as Registration Service

Whether to use IDM as an external registration service to complete registration for new users. You must configure and enable the IDM Provisioning service to use this option. See "IDM Provisioning" in the Reference.

AM passes IDM these parameters:

- **clientToken**: Signed, encrypted JWT of the OAuth 2.0 authentication state.
- **returnParams**: Encoded URL parameters, required to be returned to AM to resume authentication after registration in IDM is complete.

Default: *False*

**amster attribute**: `enableRegistrationService`

Create account if it does not exist

When enabled, AM creates an account for the user if the user profile does not exist. If the Prompt for password setting and activation code attribute is enabled, AM prompts the user for a password and activation code before creating the account.

**Important**

When configured to create new accounts, the SMTP settings must also be valid. As part of account creation, the authentication module sends the resource owner an email with an account activation code. To send the mail, AM uses the SMTP settings you provide in the module configuration.

When disabled, a user without a profile may still log into AM if the Ignore Profile attribute is set in the authentication service of the realm, or if the account is mapped to an anonymous account.

Valid values are:

- **true**
- **false**

Default: *true*

**amster attribute**: `createAccount`
Account Provider

Specifies the name of the class that implements the account provider.

Default: `org.forgerock.openam.authentication.modules.common.mapping.DefaultAccountProvider`

**amster** attribute: `accountProviderClass`

Account Mapper

Specifies the name of the class that implements the attribute mapping for the account search.

Default: `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` | `*|wechat-amster`

**amster** attribute: `accountMapperClass`

Account Mapper Configuration

Specifies the attribute configuration used to map the account of the user authenticated in the social provider to the local data store in AM. Valid values take the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```json
{
  "sub" : "12345",
  "name" : {
    "first_name" : "Demo",
    "last_name" : "User"
  }
}
```

You can create a mapper such as:

`name.first_name=cn`

Default: `openid=uid`

**amster** attribute: `accountMapperConfiguration`

Attribute Mapper

Specifies the list of fully qualified class names for implementations that map attributes from the social provider to AM profile attributes.

You can provide a custom attribute mapper. A custom attribute mapper must implement the `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` interface.
Provided implementations are:

- `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper`
- `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` - can only be used when using the `openid` scope

**Tip**

You can provide string constructor parameters by appending pipe-separated (|) values.

For example, the `org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper` class can take two constructor parameters: a comma-separated list of attributes, and a prefix to apply to their values. Specify these as follows:

```
org.forgerock.openam.authentication.modules.oidc.JwtAttributeMapper|*|wechat-
```

**Default:**

```
org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper|*|wechat-amster attribute: attributeMappingClasses
```

**Attribute Mapper Configuration**

Specifies a map of social provider user account attributes to local user profile attributes with values in the form `provider-attr=local-attr`.

**Tip**

When using the `org.forgerock.openam.authentication.modules.common.mapping.JsonAttributeMapper` class, you can parse JSON objects in mappings, by using dot notation.

For example, given a JSON payload of:

```
{  
  "sub" : "12345",  
  "name" : {  
    "first_name" : "Demo",  
    "last_name" : "User"  
  }  
}
```

You can create a mapper such as:

```
name.first_name=cn
```

**Default:**

```
openid=uid  
nickname=sn  
nickname=cn  
nickname=givenName
```
amster attribute: attributeMapperConfiguration

Prompt for password setting and activation code

When enabled, the user must set a password before AM creates an account dynamically. An activation code is also sent to the user's email address. Both the password and the code are required before the account is created.

Valid values are:

- true
- false

Default: false

amster attribute: promptPasswordFlag

Map to anonymous user

When enabled, maps the social provider authenticated user to a specified anonymous user. If the Create account if it does not exist property is enabled, AM creates an account for the authenticated user instead of mapping the account to an anonymous user.

Valid values are:

- true
- false

Default: false

amster attribute: mapToAnonymousUser

Anonymous User

Specifies an anonymous user that exists in the current realm. The Map to anonymous user property maps authorized users without a profile to this anonymous user, if enabled.

Default: anonymous

amster attribute: anonymousUserName

Save attributes in the session

When enabled, saves the values of attributes specified in the Attribute Mapper Configuration property in the AM session.

Valid values are:
• true
• false
Default: true

**amster attribute:** saveAttributesInSession

**Email**

The following properties are available under the Email tab:

**Email attribute in the Response**

Specifies the attribute identifying the authenticated user's email address in the response from the profile service in the social provider. This setting is used to send an email message with an activation code for accounts created dynamically.

**amster attribute:** emailAttribute

**Mail Server Gateway implementation class**

Specifies the class used by the module to send email. A custom subclass of `org.forgerock.openam.authentication.modules.oauth2.EmailGateway` class can be provided.

Default: `org.forgerock.openam.authentication.modules.oauth2.DefaultEmailGatewayImpl`

**amster attribute:** emailGateway

**SMTP host**

Specifies the host name of the mail server.

Default: `localhost`

**amster attribute:** smtpHost

**SMTP port**

Specifies the SMTP port number for the mail server.

Default: 25

**amster attribute:** smtpPort

**SMTP User Name**

Specifies the username AM uses to authenticate to the mail server.

**amster attribute:** smtpUsername
SMTP User Password

Specifies the password AM uses to authenticate to the mail server.

**amster attribute:** `smtpPassword`

SMTP SSL Enabled

When enabled, connects to the mail server over SSL. AM must be able to trust the SMTP server certificate.

Valid values are:

- `true`
- `false`

Default: `false`

**amster attribute:** `smtpSslEnabled`

SMTP From address

Specifies the address of the email sender, such as `no-reply@example.com`.

Default: `info@forgerock.com`

**amster attribute:** `smtpFromAddress`

Windows Desktop SSO Authentication Module Properties

**amster service name:** `WindowsDesktopSsoModule`

**ssoadm service name:** `iPlanetAMAuthWindowsDesktopSSOService`

**Tip**

Before configuring the authentication module, create an Active Directory account and a `keytab` file.

Service Principal

Specifies the Kerberos principal for authentication in the format `HTTP/host.domain@DC-DOMAIN-NAME`, where `host.domain` corresponds to the host and domain names of the AM instance and `DC-DOMAIN-NAME` is the domain name of the Kerberos realm (the FQDN of the Active Directory domain). `DC-DOMAIN-NAME` can differ from the domain name for AM.

In multi-server deployments, configure `host.domain` as the load balancer FQDN or IP address in front of the AM instances. For example, `HTTP/openamLB.example.com@KERBEROSREALM.INTERNAL.COM`. 
For more information, see the KB article *How do I set up the WDSSO authentication module in AM in a load-balanced environment?*.

**amster** attribute: `principalName`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-principal-name`

### Keytab File Name

Specifies the full path of the keytab file for the Service Principal. You generate the keytab file using the Windows `ktpass` utility.

**amster** attribute: `keytabFileName`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-keytab-file`

### Kerberos Realm

Specifies the Kerberos Key Distribution Center realm. For the Windows Kerberos service, this is the domain controller server domain name.

**amster** attribute: `kerberosRealm`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-kerberos-realm`

### Kerberos Server Name

Specifies the fully qualified domain name of the Kerberos Key Distribution Center server, such as that of the domain controller server.

**amster** attribute: `kerberosServerName`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-kdc`

### Return Principal with Domain Name

When enabled, AM automatically returns the Kerberos principal with the domain controller's domain name during authentication.

**amster** attribute: `returnPrincipalWithDomainName`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-returnRealm`

### Authentication Level

Sets the authentication level used to indicate the level of security associated with the module. The value can range from 0 to any positive integer.

**amster** attribute: `authenticationLevel`

**ssoadm** attribute: `iplanet-am-auth-windowsdesktopsso-auth-level`
Trusted Kerberos realms

List of trusted Kerberos realms for user Kerberos tickets. If realms are configured, then Kerberos tickets are only accepted if the realm part of the user principal name of the user's Kerberos ticket matches a realm from the list.

**amster** attribute: trustedKerberosRealms

**ssoadm** attribute: iplanet-am-auth-windowsdesksopssokerberos-realms-trusted

**isInitiator**

Configuration used for the JDK Kerberos LoginModule (Krb5LoginModule), which authenticates users using Kerberos principals. Possible values are true for initiator credentials, and false for acceptor credentials.

Default value: true

**amster** attribute: kerberosServiceIsinitiator

**ssoadm** attribute: iplanet-am-auth-windowsdesksopssokerberos-isinitiator

Search for the user in the realm

Validates the user against the configured data stores. If the user from the Kerberos token is not found, authentication will fail. If an authentication chain is set, the user is able to authenticate through another module. This search uses the **Alias Search Attribute Name** from the core realm attributes. See User Profile for more information about this property.

**amster** attribute: lookupUserInRealm

**ssoadm** attribute: iplanet-am-auth-windowsdesksopssolookupUserInRealm

Authenticating to Windows Desktop SSO Using REST

When authenticating with Windows Desktop SSO, add an Authorization header containing the string Basic, followed by a base64-encoded string of the username, a colon character, and the password. For example, if the credentials demo:Ch4ng31t are base64-encoded, the resulting string is ZGVtbzpDaDRuZzMxdA==.

```
$ curl \
  --request POST \
  --header "Content-Type: application/json" \ 
  --header "Accept-API-Version: resource=2.0, protocol=1.0" \ 
  --header "X-OpenAM-Username: demo" \ 
  --header "X-OpenAM-Password: Ch4ng31t" \ 
  --header "Authorization: Basic ZGVtbzpDaDRuZzMxdA==" \ 
  'https://openam.example.com:8443/openam/json/realms/root/authenticate'
{
  "tokenId":"AQIC5w...NTcy*",
  "successUrl":"/openam/console",
  "realm":"/
}
```
Authentication Modules Configuration Reference

The AM console provides two places where you can configure authentication modules:

1. Under Configure > Authentication, you configure default properties for global authentication modules.

2. Under Realms > Realm Name > Authentication > Modules, you configure modules for your realm.

The configuration of individual modules depend on its function. The configuration of an Active Directory instead of the LDAP authentication module requires connection information and details about where to search for users. In contrast, the configuration of the HOTP module for OTP authentication requires data about the password length and the mail server or SMS gateway to send the password during authentication.

Account Active Check Module

Lets you determine whether an account is marked as active, or locked.

By default, AM checks if a user account is active or locked after processing an entire authentication chain. This means users with locked accounts may be asked to perform unnecessary authentication steps, such as providing a one-time password, before authentication fails.

Use the Account Active Check module to check for active or locked status immediately after determining the user account; for example, after a DataStore or LDAP module. If the account is locked, the chain will fail early, without processing modules that appear after the Account Active Check module.

For more information, see "Configuring Account Lockout" in the Security Guide.

Active Directory Authentication Module

AM connects to Active Directory over Lightweight Directory Access Protocol (LDAP). AM provides separate Active Directory and LDAP modules to support the use of both Active Directory and another directory service in an authentication chain.

For detailed information about this module's configuration properties, see "Active Directory Module Properties".

Adaptive Risk Authentication Module

The Adaptive Risk module is designed to assess risk during authentication, so that AM can determine whether to require the user to complete further authentication steps. After configuring the Adaptive Risk module, insert it in your authentication chain with criteria set to Sufficient as shown in the following example:
In the example authentication chain shown, AM has users authenticate first using the LDAP module providing a user ID and password combination. Upon success, AM calls the Adaptive Risk module. The Adaptive Risk module assesses the risk based on your configured parameters. If the Adaptive Risk module calculates a total score below the threshold you set, the module returns success, and AM finishes authentication processing without requiring further credentials. Otherwise, the Adaptive Risk module evaluates the score to be above the risk threshold, and returns failure. AM then calls the HOTP module, requiring the user to authenticate with a one-time password delivered to her by email or by SMS to her mobile phone.
When you configure the Adaptive Risk module to save cookies and profile attributes after successful authentication, AM performs the save as post-authentication processing, only after the entire authentication chain returns success. You must set up AM to save the data as part of post-authentication processing by editing the authentication chain to add `org.forgerock.openam.authentication.modules.adaptive.AdaptivePostAuthenticationPlugin` to the list of post-authentication plugins.

When the Adaptive Risk module relies on the client IP address, and AM lies behind a load balancer or proxy layer, configure the load balancer or proxy to send the address by using the `X-Forwarded-For` header, and configure AM to consume and forward the header as necessary. For details, see "Handling HTTP Request Headers" in the Setup Guide.

For detailed information about this module's configuration properties, see "Adaptive Risk Authentication Module Properties".

Anonymous Authentication Module

This module lets you configure and track anonymous users, who can log in to your application or web site without login credentials. Typically, you would provide such users with very limited access, for example, an anonymous user may have access to public downloads on your site. When the user attempts to access resources that require more protection, the module can force further authentication for those resources.

For detailed information about this module's configuration properties, see "Anonymous Authentication Module Properties".

Certificate Authentication Module

X.509 digital certificates can enable secure authentication without the need for user names and passwords or other credentials. Certificate authentication can be used to manage authentication by applications. If all certificates are signed by a recognized Certificate Authority (CA), then you might not need additional configuration. If you need to look up public keys of AM clients, this module can also look up public keys in an LDAP directory server.

When you store certificates and certificate revocation lists (CRL) in an LDAP directory service, you must configure:

- How to access the directory service.
- How to look up the certificates and CRLs, based on the fields in the certificates that AM clients present to authenticate.

Access to the LDAP server and how to search for users is similar to LDAP module configuration as in "LDAP Authentication Module". The primary difference is that, unlike for LDAP configuration, AM retrieves the user identifier from a field in the certificate that the client application presents, then uses that identifier to search for the LDAP directory entry that holds the certificate, which should match the certificate presented. For example, if the Subject field of a typical certificate has a DN
C=FR, O=Example Corp, CN=Barbara Jensen, and Barbara Jensen's entry in the directory has \textit{cn=Barbara Jensen}, then you can use \textit{CN=Barbara Jensen} from the Subject DN to search for the entry with \textit{cn=Barbara Jensen} in the directory.

For detailed information about this module's configuration properties, see "Certificate Authentication Module Properties".

Data Store Authentication Module

The Data Store authentication module allows a login using the identity repository of the realm to authenticate users. The Data Store module removes the requirement to write an authentication plugin module, load, and then configure the authentication module if you need to authenticate against the same data store repository. Additionally, you do not need to write a custom authentication module where flatfile authentication is needed for the corresponding repository in that realm.

The Data Store module is generic. It does not implement data store-specific capabilities, such as the password policy and password reset features provided by LDAP modules. Therefore, the Data Store module returns failure when such capabilities are invoked.

For detailed information about this module's configuration properties, see "Data Store Authentication Module Properties".

Device ID (Match) Authentication Module

The Device ID (Match) module provides device fingerprinting functionality for risk-based authentication. The Device ID (Match) module collects the unique characteristics of a remote user's computing device and compares them to characteristics on a saved device profile. The module computes any variances between the collected characteristics to those stored on the saved device profile and assigns penalty points for each difference.

For detailed information about this module's configuration properties, see "Device ID (Match) Authentication Module Properties".

In general, you can configure and gather the following device characteristics:

- User agents associated with the configuration of a web browser
- Installed fonts
- Plugins installed for the web browser
- Resolution and color depth associated with a display
- Timezone or geolocation of a device

For example, when a user who typically authenticates to AM using Firefox and then logs on using Chrome, the Device ID (Match) module notes the difference and assigns penalty points to this
change in behavior. If the module detects additional differences in behavior, such as browser fonts, geolocation, and so forth, then additional points are assessed and calculated.

If the total number of penalty points exceeds a pre-configured threshold value, the Device ID (Match) module fails and control is determined by how you configured your authentication chain. If you include the HOTP module in your authentication chain, and if the Device ID (Match) module fails after the maximum number of penalty points have been exceeded, then the authentication chain issues a HOTP request to the user, requiring the user to identify themselves using two-factor authentication.

**Important**

By default, the maximum penalty points is set to 0, which you can adjust in the server-side script.

The Device ID (Match) module comes pre-configured with default client-side and server-side JavaScript code, supplying the logic necessary to fingerprint the user agent and computer. Scripting allows you to customize the code, providing more control over the device fingerprint elements that you would like to collect. While AM scripting supports both the JavaScript (default) and Groovy languages, only server-side scripts can be written in either language. The client-side scripts must be written in the JavaScript language.

**Caution**

The Device ID (Match) module’s default JavaScript client-side and server-side scripts are fully functional. If you change the client-side script, you must also make a corresponding change to the server-side script. For a safer option, if you want to change the behavior of the module, you can make a copy of the scripts, customize the behavior, and update the Device ID (Match) modules to use the new scripts.

The Device ID (Match) module does not stand on its own within an authentication chain and requires additional modules. For example, you can have any module that identifies the user (for example, DataStore, Active Directory or others), Device ID (Match), any module that provides two-factor authentication, for example the ForgeRock Authenticator (OATH) or ForgeRock Authenticator (Push) authentication modules, and Device ID (Save) within your authentication chain.

As an example, you can configure the following modules with the specified criteria:

1. **DataStore - Requisite.** The Device ID (Match) module requires user authentication information to validate the username. You can also use other modules that identify the username, such as LDAP, Active Directory, or RADIUS.

2. **Device ID (Match) - Sufficient.** The Device ID (Match) runs the client-side script, which invokes the device fingerprint collectors, captures the data, and converts it into a JSON string. It then auto-submits the data in a JSP page to the server-side scripting engine.

The server-side script calculates the penalty points based on differences between the client device and stored device profile, and whether the client device successfully "matches" the stored profile. If a match is successful, AM determines that the client's device has the required attributes for a successful authentication.
If the device does not have a match, then the module fails and falls through to the HOTP module for further processing.

3. **HOTP - Requisite.** If the user's device does not match a stored profile, AM presents the user with a HMAC One-Time Password (HOTP) screen either by SMS or email, prompting the user to enter a password.

   You can also use any other module that provides two-factor authentication.

   After the HOTP has successfully validated the user, the Device ID (Save) module gathers additional data from the user. For specific information about the HOTP module, see "HOTP Authentication Module".

4. **Device ID (Save) - Required.** The Device ID (Save) module provides configuration options to enable an auto-save feature on the device profile as well as set a maximum number of stored device profiles on the user entry or record. Once the maximum number of stored device profiles is reached, AM deletes the old data from the user record as new ones are added. User records could thus contain both old and new device profiles.

   If the auto-save feature is not enabled, AM presents the user with a screen to save the new device profile.

   The module also takes the device print and creates a JSON object that includes the ID, name, last selected date, selection counter, and device print. For specific information about the Device ID (Save) module, see "Device ID (Save) Module".

   **Note**

   If a user has multiple device profiles, the profile that is the closest match to the current client details is used for the comparison result.

   **To Configure the Device ID (Match) Authentication Module**

   1. Log into the AM console as an administrator.

   2. On the Realms page, click the realm from which you want to work.

   3. Click Authentication > Modules.

   4. To add the Device ID (Match) module, do the following substeps:

   a. Click Add Module.

   b. In the Module Name box, enter `Device-ID-Match`.

   c. In the Type box, select `Device Id (Match)`, and then click Create.

   d. Click Save Changes.
5. To make adjustments to the default scripts, click Scripts drop-down list, and then click Device ID (Match) - Client Side.

6. To make corresponding changes to the server-side script, click Scripts drop-down list, and then click Device Id (Match) - Server Side. For more information, see "Managing Scripts (Console)" in the Getting Started with Scripting.

**To Configure an Authentication Chain With a Device ID (Match) Authentication Module**

1. Log into the AM console as an administrator.

2. On the Realms page, click the realm from which you want to work.

3. Click Authentication > Chains.

4. On the Authentication Chains page, do the following steps:
   a. Click Add Chain. In the Chain Name box, enter a descriptive label for your authentication chain, and then click Create.
   b. Click Add Module.
   c. On the New Module dialog, select the authentication module, select the criteria, and then click Ok to save your changes. Repeat the last two steps to enter each module to your chain.

   For example, you can enter the following modules and criteria:
Device ID Chain

<table>
<thead>
<tr>
<th>Module</th>
<th>Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>DataStore</td>
<td>REQUISITE</td>
</tr>
<tr>
<td>Device-ID-Match</td>
<td>SUFFICIENT</td>
</tr>
<tr>
<td>HOTP</td>
<td>REQUISITE</td>
</tr>
<tr>
<td>Device-ID-Save</td>
<td>REQUIRED</td>
</tr>
</tbody>
</table>

It is assumed that you have added the Device Id (Match) and Device Id (Save) modules. If you have not added these modules, see "To Configure the Device ID (Match) Authentication Module" and "To Configure the Device ID (Save) Authentication Module".

5. Review your authentication chain, and then click Save Changes.

What the User Sees During Authentication

When the user logs on to the AM console, AM determines if the user's device differs from that of the stored profile. If the differences exceed the maximum number of penalty points or a device profile has not yet been stored, AM sends an "Enter OTP" page, requiring the user to enter a one-time password, which is sent to the user via email or SMS. The user also has the option to request a one-time password.

Next, because the Device ID (Save) module is present, AM presents the user with a "Add to Trusted Devices?" page, asking if the user wants to add the device to the list of trusted device profiles. If the user clicks "Yes", AM prompts the user to enter a descriptive name for the trusted device.

Next, AM presents the user with the User Profile page, where the user can click the Dashboard link at top to access the My Applications and Authentication Devices page. Once on the Dashboard, the user can view the list of trusted devices or remove the device by clicking the Delete Device link.

Device ID (Save) Module

The Device ID (Save) module saves a user's device profile. The module can either save the profile upon request, requiring the user to provide a name for the device and explicitly save it, or it can save the profile automatically. If a user has multiple device profiles, the profile that is the closest match to the current client details is used for the comparison result.

For detailed information about this module's configuration properties, see "Device ID (Save) Authentication Module Properties".

Within its configured authentication chain, the Device ID (Save) module also takes the device print and creates a JSON object that consists of the ID, name, last selected date, selection counter, and device print itself.
To Configure the Device ID (Save) Authentication Module

1. Log into the AM console as an administrator.
2. Click the realm from which you want to work.
3. Click Authentication > Modules.
4. To add the Device ID (Save) module, click Add Module.
5. In the Module Name box, enter Device-ID-Save.
6. In the Type box, select Device Id (Save), and then click Create.
7. To configure the Device-Id (Save) module, do the following:
   a. Click the Automatically store new profiles checkbox. If this box is left unchecked, the user will be prompted to give consent to store new profiles.
   b. In the Maximum stored profile quantity box, enter the max number of stored profiles. Any profile that exceeds this number will not be stored.
   c. In the Authentication Level box, enter a number corresponding to the authentication level of the module.
   d. Click Save Changes.
Federation Authentication Module

The Federation authentication module is used by a service provider to create a user session after validating single sign-on protocol messages. This authentication module is used by the SAML, SAMLv2, ID-FF, and WS-Federation protocols.

For detailed information about this module's configuration properties, see "Federation Authentication Module Properties".

ForgeRock Authenticator (OATH) Authentication Module

The ForgeRock Authenticator (OATH) module provides a more secure method for users to access their accounts with the help of a device such as a mobile phone.

For detailed information about this module's configuration properties, see "Creating Chains for One-Time Password Authentication".

**Note**

AM provides two authentication modules that support OATH:

- The ForgeRock Authenticator (OATH) authentication module, which is optimized for use with the ForgeRock Authenticator app and provides device profile encryption.

- The OATH authentication module, which is a raw OATH implementation requiring more configuration for users and the AM administrator.

We recommend using the ForgeRock Authenticator (OATH) authentication module when possible.

Also, the ForgeRock Authenticator (OATH), HOTP, and OATH authentication modules all support HOTP passwords, but the way that users obtain passwords differs. See "Comparing the ForgeRock Authenticator (OATH) to the HOTP Authentication Module" for more information.

ForgeRock Authenticator (Push) Authentication Module

The ForgeRock Authenticator (Push) module provides a way to send push notification messages to a device such as a mobile phone, enabling multi-factor authentication. For detailed information about multi-factor authentication with the ForgeRock Authenticator (Push) module in AM, see "About Multi-Factor Authentication".

For detailed information about this module's configuration properties, see "ForgeRock Authenticator (Push) Authentication Module Properties".

ForgeRock Authenticator (Push) Registration Authentication Module

The ForgeRock Authenticator (Push) Registration module provides a way to register a device such as a mobile phone for multi-factor authentication. For detailed information about multi-factor authentication with the ForgeRock Authenticator (Push) module in AM, see "Managing Devices for MFA".
For detailed information about this module's configuration properties, see "ForgeRock Authenticator (Push) Registration Authentication Module Properties".

**HOTP Authentication Module**

The HOTP authentication module works with an authentication chain with any module that stores the `username` attribute. The module uses the `username` from the `sharedState` set by the previous module in the chain and retrieves the user's email address or telephone number to send a one-time password to the user. The user then enters the password on a Login page and completes the authentication process if successful.

For example, to set up HOTP in an authentication chain, you can configure the Data Store module (or any module that stores the user's `username`) as the `requisite` first module, and the HOTP module as the second `requisite` module. When authentication succeeds against the Data Store module, the HOTP module retrieves the Email Address and Telephone Number attributes from the data store based on the `username` value. For the HOTP module to use either attribute, the Email Address must contain a valid email address, or the Telephone Number must contain a valid SMS telephone number.

You can set the HOTP module to automatically generate a password when users begin logging into the system. You can also set up mobile phone, mobile carrier, and email attributes for tighter controls over where the messages are generated and what provider the messages go through to reach the user.

For detailed information about this module's configuration properties, see "HOTP Authentication Module Properties".

**Note**

The ForgeRock Authenticator (OATH), HOTP, and OATH authentication modules all support HOTP passwords, but the way that users obtain passwords differs. See "Comparing the ForgeRock Authenticator (OATH) to the HOTP Authentication Module" for more information.

**HTTP Basic Authentication Module**

HTTP basic authentication takes a user name and password from HTTP authentication and tries authentication against the backend module in AM, depending on what you configure as the Backend Module Name.

For detailed information about this module's configuration properties, see "HTTP Basic Authentication Module Properties".

**JDBC Authentication Module**

The Java Database Connectivity (JDBC) module lets AM connect to a database, such as MySQL or Oracle DB to authenticate users.
LDAP Authentication Module


For detailed information about this module's configuration properties, see "LDAP Authentication Module Properties".

Legacy OAuth 2.0/OpenID Connect Authentication Module

**Note**

This authentication module is labelled as legacy. Use the replacements instead, as described in "Social Authentication Modules"

The Legacy OAuth 2.0/OpenID Connect authentication module lets AM authenticate clients of OAuth resource servers. References in this section are to RFC 6749, The OAuth 2.0 Authorization Framework.

If the module is configured to create an account if none exists, then you must provide valid SMTP settings. As part of account creation, the OAuth 2.0/OpenID Connect client authentication module sends the resource owner an email with an account activation code. To send email, AM uses the SMTP settings from the configuration for the OAuth 2.0/OpenID Connect authentication module.

For detailed information about this module's configuration properties, see "Legacy OAuth 2.0/OpenID Connect Authentication Module Properties".

MSISDN Authentication Module

The Mobile Station Integrated Services Digital Network (MSISDN) authentication module enables non-interactive authentication using a mobile subscriber ISDN associated with a terminal, such as a mobile phone. The module checks the subscriber ISDN against the value found on a user's entry in an LDAP directory service.

For detailed information about this module's configuration properties, see "MSISDN Authentication Module Properties".

OATH Authentication Module

The Open Authentication (OATH) module provides a more secure method for users to access their accounts with the help of a device, such as their mobile phone or Yubikey. Users can log into AM and
update their information more securely from a one-time password (OTP) displayed on their device. The OATH module includes the OATH standard protocols (RFC 4226 and RFC 6238). The OATH module has several enhancements to the HMAC One-Time Password (HOTP) Authentication Module, but does not replace the original module for those already using HOTP prior to the 10.1.0 release. The OATH module includes HOTP authentication and Time-Based One-Time Password (TOTP) authentication. Both types of authentication require an OATH compliant device that can provide the OTP.

HOTP authentication generates the OTP every time the user requests a new OTP on their device. The device tracks the number of times the user requests a new OTP, called the counter. The OTP displays for a period of time you designate in the setup, so the user may be further in the counter on their device than on their account. AM will resynchronize the counter when the user finally logs in. To accommodate this, you set the number of passwords a user can generate before their device cannot be resynchronized. For example, if you set the number of HOTP Window Size to 50 and someone presses the button 30 on the user's device to generate a new OTP, the counter in AM will review the OTPs until it reaches the OTP entered by the user. If someone presses the button 51 times, you will need to reset the counter to match the number on the device's counter before the user can login to AM. HOTP authentication does not check earlier passwords, so if the user attempts to reset the counter on their device, they will not be able to login until you reset the counter in AM to match their device. See "Resetting Registered Devices by using REST" for more information.

TOTP authentication constantly generates a new OTP based on a time interval you specify. The device tracks the last two passwords generated and the current password. The Last Login Time monitors the time when a user logs in to make sure that user is not logged in several times within the present time period. Once a user logs into AM, they must wait for the time it takes TOTP to generate the next two passwords and display them. This prevents others from being able to access the users account using the OTP they entered. The user's account can be accessed again after the generation of the third new OTP is generated and displayed on their device. For this reason, the TOTP Time-Step Interval should not be so long as to lock users out, with a recommended time of 30 seconds.

An authentication chain can be created to generate an OTP from either HOTP or TOTP.

For detailed information about this module's configuration properties, see "OATH Authentication Module Properties".

**Note**

AM provides two authentication modules that support OATH:

- The ForgeRock Authenticator (OATH) authentication module, which is optimized for use with the ForgeRock Authenticator app and provides device profile encryption.

- The OATH authentication module, which is a raw OATH implementation requiring more configuration for users and the AM administrator.

We recommend using the ForgeRock Authenticator (OATH) authentication module when possible.
Also, the ForgeRock Authenticator (OATH), HOTP, and OATH authentication modules all support HOTP passwords, but the way that users obtain passwords differs. See "Comparing the ForgeRock Authenticator (OATH) to the HOTP Authentication Module" for more information.

OpenID Connect id_token bearer Module

The OpenID Connect id_token bearer module lets AM rely on an OpenID Connect 1.0 provider's ID Token to authenticate an end user.

**Note**

This module validates an OpenID Connect ID token and matches it with a user profile. You should not use this module if you want AM to act as a client in the full OpenID Connect authentication flow.

To provision AM as an OpenID Connect client, you should instead configure an OAuth 2.0 or OpenID Connect social auth module. For more information, see "Social Authentication".

The OpenID Connect id_token bearer module expects an OpenID Connect ID Token in an HTTP request header. It validates the ID Token, and if successful, looks up the AM user profile corresponding to the end user for whom the ID Token was issued. Assuming the ID Token is valid and the profile is found, the module authenticates the AM user.

You configure the OpenID Connect id_token bearer module to specify how AM gets the information needed to validate the ID Token, which request header contains the ID Token, the issuer identifier for the provider who issued the ID Token, and how to map the ID Token claims to an AM user profile.

*OpenID Connect id_token Bearer Example*

The OpenID Connect id_token bearer module configuration must match the claims returned in the id_token JWT used to authenticate.

Before configuring the module, use an OpenID Connect client to obtain an id_token. Decode the id_token value to see the claims in the middle portion of the JWT. The claims in the decoded id_token look something like the following example:
The \texttt{azp}, \texttt{aud}, and \texttt{iss} values are literally reused in the module configuration. The following figure shows an example configuration for this \texttt{id_token} format.
Sample OpenID Connect id_token Bearer Module Configuration

The following example command demonstrates a REST call that authenticates the user using the module:

```bash
```
Persistent Cookie Module

The Persistent Cookie module supports the configuration of cookie lifetimes based on requests and a maximum time. Note that by default, the persistent cookie is called session-jwt.

Important

If Secure Cookie is enabled (Deployment > Servers > Server Name > Security > Cookie), the Persistent Cookie module only works over HTTPS.

The module signs and encrypts the JSON Web Token (JWT) that is inserted as the value of the persistent cookie. The relevant secret IDs and the default public key and HMAC key aliases are shown in the table below:

<table>
<thead>
<tr>
<th>Secret ID</th>
<th>Default Alias</th>
<th>Algorithms</th>
</tr>
</thead>
<tbody>
<tr>
<td>am.default.authentication.modules.persistentcookie.encryption</td>
<td>test</td>
<td>RSA (at least 2048 bits)</td>
</tr>
<tr>
<td>am.default.authentication.modules.persistentcookie.signing</td>
<td>hmacsigningtest</td>
<td>HS256</td>
</tr>
</tbody>
</table>

For each instance of a persistent cookie module available in a realm, there is a dynamic secret ID associated with that module configuration instance.
For example, in a single realm you can have a Persistent Cookie module instance with the name *helloworld*, and a separate Persistent Cookie module instance with the name *hellomars*.

The following secret ID mappings could be used to encrypt and then sign persistent cookies:

<table>
<thead>
<tr>
<th>Secret ID</th>
<th>Default Alias</th>
</tr>
</thead>
<tbody>
<tr>
<td>am.authentication.modules.persistentcookie.helloworld.encryption</td>
<td>helloworld</td>
</tr>
<tr>
<td>am.authentication.modules.persistentcookie.helloworld.signing</td>
<td>hmacsigninghelloworld</td>
</tr>
<tr>
<td>am.authentication.modules.persistentcookie.hellomars.encryption</td>
<td>hellomars</td>
</tr>
<tr>
<td>am.authentication.modules.persistentcookie.hellomars.signing</td>
<td>hmacsigninghellomars</td>
</tr>
</tbody>
</table>

AM will attempt to look up the secrets with the Persistent Cookie module instance name. If unsuccessful, AM will look up the secrets using the default secret ID.

For information on mapping certificate aliases to secret IDs in secret stores, see "Mapping and Rotating Secrets" in the *Security Guide*.

When the Persistent Cookie module enforces the client IP address, and AM lies behind a load balancer or proxy layer, configure the load balancer or proxy to send the address by using the `X-Forwarded-For` header, and configure AM to consume and forward the header as necessary. For details, see "Handling HTTP Request Headers" in the *Setup Guide*.

The Persistent Cookie module belongs with a second module in an authentication chain. To see how this works, navigate to Realms > *Realm Name* > Authentication > Chains. Create a new chain and add modules as shown in the figure. The following example shows how a Persistent Cookie module is sufficient. If the persistent cookie does not yet exist, authentication relies on LDAP:
Select the Settings tab and locate settings for the post-authentication processing class. Set the Class Name to `org.forgerock.openam.authentication.modules.persistentcookie.PersistentCookieAuthModulePostAuthenticationPlugin`, as shown in the following figure:
You should now be able to authenticate automatically, as long as the cookie exists for the associated domain.

Tip

To configure the Persistent Cookie module globally in the AM console, navigate to Configure > Authentication, and then click Persistent Cookie.

For detailed information about this module's configuration properties, see "Persistent Cookie Authentication Module Properties".
RADIUS Authentication Module

The Remote Authentication Dial-In User Service (RADIUS) module lets AM authenticate users against RADIUS servers.

For detailed information about this module's configuration properties, see "RADIUS Authentication Module Properties".

SAE Authentication Module

The Secure Attribute Exchange (SAE) module lets AM authenticate a user who has already authenticated with an entity that can vouch for the user to AM, so that AM creates a session for the user. This module is useful in virtual federation, where an existing entity instructs the local AM instance to use federation protocols to transfer authentication and attribute information to a partner application.

For detailed information about this module's configuration properties, see "SAE Authentication Module Properties".

SAML2 Authentication Module

The SAML2 authentication module lets administrators integrate SAML v2.0 single sign-on and single logout into an AM authentication chain.

You use the SAML2 authentication module when deploying SAML v2.0 single sign-on in integrated mode. In addition to configuring SAML2 authentication module properties, integrated mode deployment requires that you make several changes to service provider configurations. Before attempting to configure a SAML2 authentication module instance, review "Implementing SSO in Integrated Mode (Chains)" in the SAML v2.0 Guide and make sure that you have made any required changes to your service provider configuration.

For detailed information about this module's configuration properties, see "SAML2 Authentication Module Properties".

Scripted Authentication Module

A scripted authentication module runs scripts to authenticate a user. The configuration for the module can hold two scripts, one to include in the web page run on the client user-agent, another to run in AM on the server side.

The client-side script is intended to retrieve data from the user-agent. This must be in a language the user-agent can run, such as JavaScript, even if the server-side script is written in Groovy.

The server-side script is intended to handle authentication.

Scripts are stored not as files, but instead as AM configuration data. This makes it easy to update a script on one AM server, and then to allow replication to copy it to other servers. You can manage the
scripts through the AM console, where you can write them in the text boxes provided or upload them from files.

You can also upload scripts and associate them with a scripted authentication module by using the `ssoadm` command.

The following example shows how to upload a server-side script from a file, create a scripted authentication module, and then associate the uploaded script with the new module.

```bash
# # Upload a server-side script from a script file, myscript.groovy. #

ssoadm create-sub-cfg
  --realm /
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org
  --password-file /tmp/pwd.txt
  --servicename ScriptingService
  --subconfigname scriptConfigurations/scriptConfiguration
  --subconfigid myScriptId
  --attributevalues
  "name=My Scripted Auth Module Script"
  "script-file=myscript.groovy"
  "context=AUTHENTICATION_SERVER_SIDE"
  "language=GROOVY"

# # Create a scripted authentication module, myScriptedAuthModule. #

ssoadm create-auth-instance
  --realm /
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org
  --password-file /tmp/pwd.txt
  --authtype Scripted
  --name myScriptedAuthModule

# # Associate the script with the auth module, and disable client-side scripts. #

ssoadm update-auth-instance
  --realm /
  --adminid uid=amAdmin,ou=People,dc=openam,dc=forgerock,dc=org
  --password-file /tmp/pwd.txt
  --name myScriptedAuthModule
  --attributevalues
  "iplanet-am-auth-scripted-server-script=myScriptId"
  "iplanet-am-auth-scripted-client-script-enabled=false"
```

If you have multiple separate sets of client-side and server-side scripts, then configure multiple modules, one for each set of scripts.

For details on writing authentication module scripts, see "Using Server-side Authentication Scripts in Authentication Modules".
For detailed information about this module's configuration properties, see "Scripted Authentication Module Properties".

Social Authentication Modules

The social authentication modules let AM authenticate clients of OAuth 2.0 or OpenID Connect 1.0 resource servers. References in this section are to RFC 6749, The OAuth 2.0 Authorization Framework.

AM provides pre-configured authentication modules for the following social identity providers:

- Instagram
- VKontakte
- WeChat

AM provides two authentication modules for the WeChat social identity provider. The Social Auth WeChat authentication module implements a login flow that requires the user to scan an on-screen QR code with the WeChat app. The Social Auth WeChat Mobile authentication module implements an alternative login flow for users authenticating on their mobile device, who would not be able to scan a QR code displayed on the mobile device's screen.

AM provides two generic authentication modules, one for OAuth 2.0, and another for OpenID Connect 1.0, for authenticating users of standards-compliant social identity providers, for example Facebook and Google.

If the social authentication module is configured to create an account when none exists, then you must provide valid SMTP settings in the Email tab. The social identity provider must also provide the user's email address. As part of account creation, the social authentication module sends the resource owner an email with an account activation code. To send email, AM uses the SMTP settings from the Email tab of the configuration of the social authentication module.

For detailed information about the social authentication module's configuration properties, see the following sections:

- "Social Authentication Module Properties - OAuth 2.0"
- "Social Authentication Module Properties - OpenID Connect 1.0"
- "Social Authentication Module Properties - Instagram"
- "Social Authentication Module Properties - VKontakte"
- "Social Authentication Module Properties - WeChat"
- "Social Authentication Module Properties - WeChat Mobile"
Windows Desktop SSO Authentication Module

The Windows Desktop SSO module uses Kerberos authentication. The user presents a Kerberos token to AM through the Simple and Protected GSS-API Negotiation Mechanism (SPNEGO) protocol. The Windows Desktop SSO authentication module enables desktop single sign on such that a user who has already authenticated with a Kerberos Key Distribution Center can authenticate to AM without having to provide the login information again. Users might need to set up Integrated Windows Authentication in Internet Explorer or Microsoft Edge to benefit from single sign on when logged on to a Windows desktop.

For detailed information about this module's configuration properties, see "Windows Desktop SSO Authentication Module Properties".

**Warning**

If you are using the Windows Desktop SSO module as part of an authentication chain and Windows Desktop SSO fails, you may no longer be able to POST data to non-NTLM-authenticated web sites. For information on a possible workaround, see Microsoft knowledge base article KB251404.

Scripted Module API Functionality

In addition to the functionality provided by the "Accessing HTTP Services" in the Getting Started with Scripting and "Debug Logging" in the Getting Started with Scripting, authentication modules that use server-side scripts can access the authorization state of a request, the information pertaining a session, and the login request itself.

Client-side scripts in modules gather data into a string, which is returned to AM in a self-submitting form.

**Tip**

When developing server-side scripts, it can be useful to increase the debug level of the org.apache.http.wire and org.apache.http.headers appenders to Message.

By default, these appenders are always set to the Warning level unless logging is disabled. For more information, see the org.forgerock.allow.http.client.debug advanced server property.

Authentication API functionality includes:

- "Accessing Authentication State"
- "Accessing Profile Data"
- "Accessing Client-Side Script Output Data"
- "Accessing Request Data"
- "Redirecting the User After Authentication Failure"
Accessing Authentication State

AM passes `authState` and `sharedState` objects to server-side scripts in order for the scripts to access authentication state.

Server-side scripts can access the current authentication state through the `authState` object.

The `authState` value is `SUCCESS` if the authentication is currently successful, or `FAILED` if authentication has failed. Server-side scripts must set a value for `authState` before completing.

If an earlier authentication module in the authentication chain has set the login name of the user, server-side scripts can access the login name through `username`.

The following authentication modules set the login name of the user:

- Anonymous
- Certificate
- Data Store
- Federation
- HTTP Basic
- JDBC
- LDAP
- Membership
- RADIUS
- Windows Desktop SSO

Accessing Profile Data

Server-side authentication scripts can access profile data through the methods of the `idRepository` object.

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>idRepository.getAttribute</td>
<td>User Name (type: String)</td>
<td>Set</td>
<td>Return the values of the named attribute for the named user.</td>
</tr>
<tr>
<td></td>
<td>Attribute Name (type: String)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>idRepository.setAttribute</td>
<td>User Name (type: String)</td>
<td>Void</td>
<td>Set the named attribute as specified by the attribute value for the named user.</td>
</tr>
</tbody>
</table>
### Accessing Client-Side Script Output Data

Client-side scripts add data they gather into a string object named `clientScriptOutputData`. Client-side scripts then cause the user-agent automatically to return the data to AM by HTTP POST of a self-submitting form.

### Accessing Request Data

Server-side scripts can get access to the login request by using the methods of the `requestData` object. The following table lists the methods of the `requestData` object. Note that this object differs from the client-side `requestData` object and contains information about the original authentication request made by the user.

<table>
<thead>
<tr>
<th>Method</th>
<th>Parameters</th>
<th>Return Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>requestData.getHeader</code></td>
<td><code>Header Name</code> (type: String)</td>
<td>String</td>
<td>Return the String value of the named request header, or null if parameter is not set.</td>
</tr>
<tr>
<td><code>requestData.getHeaders</code></td>
<td><code>Header Name</code> (type: String)</td>
<td>String[]</td>
<td>Return the array of String values of the named request header, or null if parameter is not set.</td>
</tr>
<tr>
<td><code>requestData.getParameter</code></td>
<td><code>Parameter Name</code> (type: String)</td>
<td>String</td>
<td>Return the String value of the named request parameter, or null if parameter is not set.</td>
</tr>
<tr>
<td><code>requestData.getParameters</code></td>
<td><code>Parameter Name</code> (type: String)</td>
<td>String[]</td>
<td>Return the array of String values of the named request parameter, or null if parameter is not set.</td>
</tr>
</tbody>
</table>

### Redirecting the User After Authentication Failure

Server-side scripts can redirect the user to a specific URL in case of authentication failure by adding a `gotoOnFailureUrl` property to the chain's shared state.
When the script reaches a **FAILED** authentication state (defined by the `authState` variable), it checks if the `gotoOnFailureUrl` property is stored in the shared state. If so, the script redirects the user to the specified URL.

You can redirect the user to a page relative to AM's URL, or to an absolute URL:

**Relative URL**

```java
sharedState.put("gotoOnFailureUrl","/am/XUI/?service=testChain#failedLogin");
authState = FAILED;
```

**Absolute URL**

```java
sharedState.put("gotoOnFailureUrl","http://www.example.com");
authState = FAILED;
```

Note that the failure URL relative to AM's domain includes the authentication service; this is so that when the user clicks on the link to log in again, AM constructs the login page with the appropriate service instead of with the default one for the realm.

When redirecting the user to an absolute URL different from AM's scheme, FQDN, and port, you must configure the URL in the Validation Service of the realm. Otherwise, AM will ignore the redirection. For more information, see "To Configure the Validation Service".
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access control</td>
<td>Control to grant or to deny access to a resource.</td>
</tr>
<tr>
<td>Account lockout</td>
<td>The act of making an account temporarily or permanently inactive after successive authentication failures.</td>
</tr>
<tr>
<td>Actions</td>
<td>Defined as part of policies, these verbs indicate what authorized identities can do to resources.</td>
</tr>
<tr>
<td>Advice</td>
<td>In the context of a policy decision denying access, a hint to the policy enforcement point about remedial action to take that could result in a decision allowing access.</td>
</tr>
<tr>
<td>Agent administrator</td>
<td>User having privileges only to read and write agent profile configuration information, typically created to delegate agent profile creation to the user installing a web or Java agent.</td>
</tr>
<tr>
<td>Agent authenticator</td>
<td>Entity with read-only access to multiple agent profiles defined in the same realm; allows an agent to read web service profiles.</td>
</tr>
<tr>
<td>Application</td>
<td>In general terms, a service exposing protected resources.</td>
</tr>
<tr>
<td></td>
<td>In the context of AM policies, the application is a template that constrains the policies that govern access to protected resources. An application can have zero or more policies.</td>
</tr>
<tr>
<td>Application type</td>
<td>Application types act as templates for creating policy applications.</td>
</tr>
<tr>
<td></td>
<td>Application types define a preset list of actions and functional logic, such as policy lookup and resource comparator logic.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Application types</td>
<td>Define internal normalization, indexing logic, and comparator logic for applications.</td>
</tr>
<tr>
<td>Attribute-based access control (ABAC)</td>
<td>Access control that is based on attributes of a user, such as how old a user is or whether the user is a paying customer.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The act of confirming the identity of a principal.</td>
</tr>
<tr>
<td>Authentication chaining</td>
<td>A series of authentication modules configured together which a principal must negotiate as configured in order to authenticate successfully.</td>
</tr>
<tr>
<td>Authentication level</td>
<td>Positive integer associated with an authentication module, usually used to require success with more stringent authentication measures when requesting resources requiring special protection.</td>
</tr>
<tr>
<td>Authentication module</td>
<td>AM authentication unit that handles one way of obtaining and verifying credentials.</td>
</tr>
<tr>
<td>Authorization</td>
<td>The act of determining whether to grant or to deny a principal access to a resource.</td>
</tr>
<tr>
<td>Authorization Server</td>
<td>In OAuth 2.0, issues access tokens to the client after authenticating a resource owner and confirming that the owner authorizes the client to access the protected resource. AM can play this role in the OAuth 2.0 authorization framework.</td>
</tr>
<tr>
<td>Auto-federation</td>
<td>Arrangement to federate a principal's identity automatically based on a common attribute value shared across the principal's profiles at different providers.</td>
</tr>
<tr>
<td>Bulk federation</td>
<td>Batch job permanently federating user profiles between a service provider and an identity provider based on a list of matched user identifiers that exist on both providers.</td>
</tr>
<tr>
<td>Circle of trust</td>
<td>Group of providers, including at least one identity provider, who have agreed to trust each other to participate in a SAML v2.0 provider federation.</td>
</tr>
<tr>
<td>Client</td>
<td>In OAuth 2.0, requests protected web resources on behalf of the resource owner given the owner's authorization. AM can play this role in the OAuth 2.0 authorization framework.</td>
</tr>
<tr>
<td>Client-based OAuth 2.0 tokens</td>
<td>After a successful OAuth 2.0 grant flow, AM returns a token to the client. This differs from CTS-based OAuth 2.0 tokens, where AM returns a reference to token to the client.</td>
</tr>
<tr>
<td>Client-based sessions</td>
<td>AM sessions for which AM returns session state to the client after each request, and require it to be passed in with the subsequent</td>
</tr>
</tbody>
</table>
request. For browser-based clients, AM sets a cookie in the browser that contains the session information.

For browser-based clients, AM sets a cookie in the browser that contains the session state. When the browser transmits the cookie back to AM, AM decodes the session state from the cookie.

<table>
<thead>
<tr>
<th>Conditions</th>
<th>Defined as part of policies, these determine the circumstances under which a policy applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Environmental conditions reflect circumstances like the client IP address, time of day, how the subject authenticated, or the authentication level achieved.</td>
</tr>
<tr>
<td></td>
<td>Subject conditions reflect characteristics of the subject like whether the subject authenticated, the identity of the subject, or claims in the subject's JWT.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Configuration datastore</th>
<th>LDAP directory service holding AM configuration data.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cross-domain single sign-on (CDSSO)</td>
<td>AM capability allowing single sign-on across different DNS domains.</td>
</tr>
<tr>
<td>CTS-based OAuth 2.0 tokens</td>
<td>After a successful OAuth 2.0 grant flow, AM returns a reference to the token to the client, rather than the token itself. This differs from client-based OAuth 2.0 tokens, where AM returns the entire token to the client.</td>
</tr>
<tr>
<td>CTS-based sessions</td>
<td>AM sessions that reside in the Core Token Service's token store. CTS-based sessions might also be cached in memory on one or more AM servers. AM tracks these sessions in order to handle events like logout and timeout, to permit session constraints, and to notify applications involved in SSO when a session ends.</td>
</tr>
</tbody>
</table>

| Delegation | Granting users administrative privileges with AM. |
| Entitlement | Decision that defines which resource names can and cannot be accessed for a given identity in the context of a particular application, which actions are allowed and which are denied, and any related advice and attributes. |

| Extended metadata | Federation configuration information specific to AM. |
| Extensible Access Control Markup Language (XACML) | Standard, XML-based access control policy language, including a processing model for making authorization decisions based on policies. |
| Federation | Standardized means for aggregating identities, sharing authentication and authorization data information between trusted providers, and |
allowing principals to access services across different providers without authenticating repeatedly.

<table>
<thead>
<tr>
<th>Term</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fedlet</td>
<td>Service provider application capable of participating in a circle of trust and allowing federation without installing all of AM on the service provider side; AM lets you create Java Fedlets.</td>
</tr>
<tr>
<td>Hot swappable</td>
<td>Refers to configuration properties for which changes can take effect without restarting the container where AM runs.</td>
</tr>
<tr>
<td>Identity</td>
<td>Set of data that uniquely describes a person or a thing such as a device or an application.</td>
</tr>
<tr>
<td>Identity federation</td>
<td>Linking of a principal's identity across multiple providers.</td>
</tr>
<tr>
<td>Identity provider (IDP)</td>
<td>Entity that produces assertions about a principal (such as how and when a principal authenticated, or that the principal's profile has a specified attribute value).</td>
</tr>
<tr>
<td>Identity repository</td>
<td>Data store holding user profiles and group information; different identity repositories can be defined for different realms.</td>
</tr>
<tr>
<td>Java agent</td>
<td>Java web application installed in a web container that acts as a policy enforcement point, filtering requests to other applications in the container with policies based on application resource URLs.</td>
</tr>
<tr>
<td>Metadata</td>
<td>Federation configuration information for a provider.</td>
</tr>
<tr>
<td>Policy</td>
<td>Set of rules that define who is granted access to a protected resource when, how, and under what conditions.</td>
</tr>
<tr>
<td>Policy agent</td>
<td>Java, web, or custom agent that intercepts requests for resources, directs principals to AM for authentication, and enforces policy decisions from AM.</td>
</tr>
<tr>
<td>Policy Administration Point (PAP)</td>
<td>Entity that manages and stores policy definitions.</td>
</tr>
<tr>
<td>Policy Decision Point (PDP)</td>
<td>Entity that evaluates access rights and then issues authorization decisions.</td>
</tr>
<tr>
<td>Policy Enforcement Point (PEP)</td>
<td>Entity that intercepts a request for a resource and then enforces policy decisions from a PDP.</td>
</tr>
<tr>
<td>Policy Information Point (PIP)</td>
<td>Entity that provides extra information, such as user profile attributes that a PDP needs in order to make a decision.</td>
</tr>
<tr>
<td>Principal</td>
<td>Represents an entity that has been authenticated (such as a user, a device, or an application), and thus is distinguished from other entities.</td>
</tr>
</tbody>
</table>
When a **Subject** successfully authenticates, AM associates the Subject with the Principal.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privilege</td>
<td>In the context of delegated administration, a set of administrative tasks that can be performed by specified identities in a given realm.</td>
</tr>
<tr>
<td>Provider federation</td>
<td>Agreement among providers to participate in a circle of trust.</td>
</tr>
<tr>
<td>Realm</td>
<td>AM unit for organizing configuration and identity information.</td>
</tr>
<tr>
<td>Realms</td>
<td>Realms can be used for example when different parts of an organization have different applications and identity stores, and when different organizations use the same AM deployment.</td>
</tr>
<tr>
<td>Administrators</td>
<td>Administrators can delegate realm administration. The administrator assigns administrative privileges to users, allowing them to perform administrative tasks within the realm.</td>
</tr>
<tr>
<td>Resource</td>
<td>Something a user can access over the network such as a web page.</td>
</tr>
<tr>
<td>Resource owner</td>
<td>In OAuth 2.0, entity who can authorize access to protected web resources, such as an end user.</td>
</tr>
<tr>
<td>Resource server</td>
<td>In OAuth 2.0, server hosting protected web resources, capable of handling access tokens to respond to requests for such resources.</td>
</tr>
<tr>
<td>Response attributes</td>
<td>Defined as part of policies, these allow AM to return additional information in the form of &quot;attributes&quot; with the response to a policy decision.</td>
</tr>
<tr>
<td>Role based access control (RBAC)</td>
<td>Access control that is based on whether a user has been granted a set of permissions (a role).</td>
</tr>
<tr>
<td>Security Assertion Markup Language (SAML)</td>
<td>Standard, XML-based language for exchanging authentication and authorization data between identity providers and service providers.</td>
</tr>
<tr>
<td>Service provider (SP)</td>
<td>Entity that consumes assertions about a principal (and provides a service that the principal is trying to access).</td>
</tr>
<tr>
<td>Authentication Session</td>
<td>The interval while the user or entity is authenticating to AM.</td>
</tr>
<tr>
<td>Session</td>
<td>The interval that starts after the user has authenticated and ends when the user logs out, or when their session is terminated. For browser-based clients, AM manages user sessions across one or more applications by setting a session cookie. See also CTS-based sessions and Client-based sessions.</td>
</tr>
<tr>
<td><strong>Session high availability</strong></td>
<td>Capability that lets any AM server in a clustered deployment access shared, persistent information about users' sessions from the CTS token store. The user does not need to log in again unless the entire deployment goes down.</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>Session token</strong></td>
<td>Unique identifier issued by AM after successful authentication. For a CTS-based sessions, the session token is used to track a principal's session.</td>
</tr>
<tr>
<td><strong>Single log out (SLO)</strong></td>
<td>Capability allowing a principal to end a session once, thereby ending her session across multiple applications.</td>
</tr>
<tr>
<td><strong>Single sign-on (SSO)</strong></td>
<td>Capability allowing a principal to authenticate once and gain access to multiple applications without authenticating again.</td>
</tr>
<tr>
<td><strong>Site</strong></td>
<td>Group of AM servers configured the same way, accessed through a load balancer layer. The load balancer handles failover to provide service-level availability. The load balancer can also be used to protect AM services.</td>
</tr>
<tr>
<td><strong>Standard metadata</strong></td>
<td>Standard federation configuration information that you can share with other access management software.</td>
</tr>
<tr>
<td><strong>Stateless Service</strong></td>
<td>Stateless services do not store any data locally to the service. When the service requires data to perform any action, it requests it from a data store. For example, a stateless authentication service stores session state for logged-in users in a database. This way, any server in the deployment can recover the session from the database and service requests for any user. All AM services are stateless unless otherwise specified. See also Client-based sessions and CTS-based sessions.</td>
</tr>
<tr>
<td><strong>Subject</strong></td>
<td>Entity that requests access to a resource</td>
</tr>
<tr>
<td><strong>Identity store</strong></td>
<td>Data storage service holding principals' profiles; underlying storage can be an LDAP directory service or a custom IdRepo implementation.</td>
</tr>
<tr>
<td><strong>Web Agent</strong></td>
<td>Native library installed in a web server that acts as a policy enforcement point with policies based on web page URLs.</td>
</tr>
</tbody>
</table>