Release Notes

/ OpenAM 12

Latest update: 12.0.4

ForgeRock AS
33 New Montgomery St., Suite 1500
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Notes covering OpenAM prerequisites, fixes, known issues. OpenAM provides open source Authentication, Authorization, Entitlement and Federation software.

Table of Contents

Chapter 1

What's New in OpenAM 12

OpenAM 12 is a powerful centralized access management solution, enabling companies to manage access control, federated services, single sign-on, and many other services while protecting their resources. OpenAM is part of the ForgeRock Identity Platform.

Before you install OpenAM or update your existing OpenAM installation, read these release notes.

- If you have already installed OpenAM, see "*About Upgrading OpenAM*" in the *Upgrade Guide*.

  Do *not* perform an upgrade by deploying the new version and then importing an existing configuration by running the **ssoadm import-svc-config** command. Importing an outdated configuration can result in a corrupted installation.

- If you are installing OpenAM for the first time, see "Deciding How To Install OpenAM" in the *Installation Guide*.

1.1. What's New in OpenAM 12.0.4

In addition to fixes, OpenAM 12.0.4 includes the following product enhancements:

- **The REST authentication endpoint now supports MIME-encoded UTF-8**. You can now use UTF-8 user names and passwords in calls to the `/json/authenticate` endpoint.

  You should first Base64-encode the UTF-8 string, 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 `dëmø`:

  1. Encode the string in Base64 format: `yZfDq8mxw7g=`.
  2. Wrap the Base64-encoded string as per RFC 2047: `=?UTF-8?B?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: changeit" \
      --data "{}" \
      https://openam.example.com:8443/openam/json/authenticate
      {
       "tokenId": "AQIC5w...NTcy*",
       "successUrl": "/openam/console"
       }
```

- **The SAML v2.0 DigestMethod XML signature method is now configurable**. You can now use signature methods other than SHA1, for example SHA256, SHA384, or SHA512.

- **The default WS-Fed and SAML v2.0 IdP attribute mappers now support Base64-encoded binary values for NameID**. This change allows for a `binary` flag to be added to the `NameID` mapping to indicate that the attribute is binary. Use a semicolon (;) character as a delimiter for the flag. The mapping may resemble the following, for example:

  ```
  urn:oasis:names:tc:SAML:2.0:nameid-format:persistent=objectGUID;binary
  ```

  You should append the `;binary` flag to your NameID Value mapping if the chosen attribute is in binary format, or if the value needs to be transferred as Base64 encoded.

- **SAML IdP attribute mappers now allow profile attribute mapping when dynamic profile mode is used**. The SAML AttributeMapper now maps attributes associated with the newly created user account, allowing them to be used immediately at assertion generation time.

- **New `csrf` parameter required by the `/oauth2/authorize` endpoint**. The `/oauth2/authorize` endpoint requires a new `csrf` parameter. The value of the parameter duplicates the contents of the `iPlanetDirectoryPro` cookie, which contains the SSO token of the resource owner giving consent.

  For example:

  ```
  $ curl \
   --request POST \
   --header  "Content-Type: application/x-www-form-urlencoded" \
   --Cookie "iPlanetDirectoryPro=AQIC5w...*" \
   --data "redirect_uri=http://www.example.net" \
   --data "scope=profile" \
   --data "response_type=code" \
   --data "client_id=myClient" \
   --data "csrf=AQIC5w...*" \
   --data "decision=allow" \
   --data "save_consent=on" \
   "http://openam.example.com:8080/openam/oauth2/authorize?response_type=code&client_id=myClient"\
   "&realm=/&scope=profile&redirect_uri=http://www.example.net"
  ```

  Duplicating the cookie value helps prevent Cross-Site Request Forgery (CSRF) attacks.

1.2. What's New in OpenAM 12.0.3

In addition to fixes, OpenAM 12.0.3 includes the following product enhancements:

- **OATH Module Now Supports Resynchronization**. OpenAM's OATH authentication module now supports TOTP resynchronization as specified by RFC-6238. The resynchronization will occur automatically to allow for clock drift between the user's token and server when logging in. For information, see OPENAM-1462.

- **Support for XML Digital Signatures in SAML Query String Verification Process**. OpenAM now supports the following additional signature algorithms for query string signing:

  - RSA-SHA256
  - RSA-SHA384
  - RSA-SHA512
  - ECDSA-SHA1
  - ECDSA-SHA256
  - ECDSA-SHA384
  - ECDSA-SHA512

  For information, see OPENAM-1900.

- **Configurable Heartbeat Timeout**. Users can now set a heartbeat timeout for all OpenDJ SDK controlled connections via OpenAM's advanced setting `org.forgerock.openam.ldap.heartbeat.timeout` property (default: 3 seconds). The heartbeat timeout is the amount of time that OpenAM should wait for a heartbeat search operation to complete before considering the connection unavailable. For information, see OPENAM-3266.

- **Added sun-idrepo-ldapv3-config-memberurl to OpenDJ Data Store Configuration**. The attribute `sun-idrepo-ldapv3-config-memberurl` has been added to the `LDAPv3ForOpenDS` data store configuration schema. For information, see OPENAM-3762.

- **New Property to Allow Sending SAML AuthnRequests without RequestedAuthnContext**. OpenAM supports a new property `includeRequestedAuthnContext`, which is used in the hosted service provider extended metadata. The default value is `true`. When the property is set to false, this will cause the requested authentication context (`RequestedAuthnContext`) to be left out of the authentication request to the identity provider. For information, see OPENAM-4103.

- **New &auth_chain= URL Parameter Overrides Auth Chain Used by Password Grant Type**. The OAuth v2.0 `access_token` endpoint has been updated to allow clients to specify the authentication chain they want to use to authenticate. For information, see OPENAM-4177.

- **Administrators Can Reset A User's Password via REST**. Realm administrators can now reset a user's password using the `/json/users` REST endpoint. For information, see OPENAM-5695.

- **OAuth2 Displays Token and User Information in Access Logs**. OpenAM's OAuth v2.0 displays the token and user information in the `OAuth2Provider.access` log file for audit events. For information, see OPENAM-5759.

- **ssoadm Imports and Exports Agent Configurations with Hashed Passwords**. The **ssoadm** tool `show-agent` command exports the agent configuration with the hashed `userpassword`. To export the configuration with the password, use the new `--includepassword` parameter. For information, see OPENAM-5785.

- **Username Can Be Accessed using a PAP**. The username can now be accessed using a PAP with the following code snippet:

```
loginName = (String) requestParamsMap.get("javax.security.auth.login.name");
```

- **User Self-Registration Service Supports Forgotten Email URL as a Relative Path**. The Forgotten Email URL property can now be expressed as a relative path in a JSON request when using the User Self Service REST endpoints. For information, see OPENAM-6266.

- **Added OAuth2/OpenID Connect Token Lifetime Options**. The authorization code, access token, refresh token, and JWT token lifetimes can now be configured on a per OAuth v2.0/OpenID Connect 1.0 client basis. For information, see OPENAM-6236.

- **Configurable OAuth2/OIDC Login URL**. OpenAM now supports a configurable OAuth2/OIDC login URL when OpenAM acts as an OAuth2/OIDC Provider. For information, see OPENAM-6814.

- **New Shared Secret Provider Plugin for OATH Module**. The OATH authentication module now allows customization of the retrieval of the shared secret used by the OATH authentication module. Use this extension point if the OATH shared secret is stored in a custom format. For information, see OPENAM-6892.

- **User Self-Registration Service Supports Register Email URL as a Relative Path**. The Register Email URL property can now be expressed as a relative path in a JSON request when using the User Self Service endpoints. For information, see OPENAM-6996.

- **New Property to Adjust Max File Upload Size for `FileUpload.jsp`**. OpenAM now supports a new property, `org.forgerock.openam.console.max.file.upload.size` that sets the maximum file upload for `FileUpload.jsp`. The default size has also been increased from 50K to 750K. For information, see OPENAM-7109.

- **XUI Country-Specific Localization**. OpenAM's XUI now supports country-specific localization using the `XUI/locales/<locale>/translation.json` file. For information, see OPENAM-7123.

- **Policy Editor Now Supports Custom Resource Attributes**. The OpenAM console now supports policies with custom resource attributes. The custom resource attributes will be displayed in a read-only view. For information, see OPENAM-7298.

- **New OAuth v2.0 Endpoint for Token Deletion/Revocation**. OpenAM now supports a new OAuth v2.0 endpoint for token deletion and revocation.

  To revoke a token, create a POST request to the `/frrest/oauth2/token` endpoint, specifying the ID of the token, and setting the `_action` parameter to `revokeTokens`:

```
$ curl -X POST \
    -d  '{"client_id":"myOAuthClient"}' \
    -H "Content-Type: application/json" \
    -H "Accept-API-Version: protocol=1.0,resource=1.0" \
    http://openam.example.com:8080/openam/frrest/oauth2/token/{Token ID}?_action=revokeTokens
```

For information, see OPENAM-7820.

- **XML Signature Digest Method is Configurable via SAML v2.0**. OpenAM now supports a configurable XML signature digest method when using SAML v2.0.

  To configure the digest method, in the OpenAM console, navigate to Configuration > Global > Common Federation Configuration, and then set the XML digest algorithm property.

  For information, see OPENAM-7778.

- **OAuth Authorization Code Character Limit Increased**. The OAuth v2.0 authentication module's character limit has been increased from 512 to 2000 characters. For information, see OPENAM-7898.

- **Connections to TLS v1.2 Data Store**. OpenAM now is able to connect to a TLS v1.2-only data store. For information, see OPENAM-8091.

- **Default IdP Attribute Mapper Can Base64-encode Binary Attributes for WS-Federation**. OpenAM's default IdP attribute mapper can now base64-encode binary attributes before they are added to an assertion for WS-Federation. To map a binary attribute, use the `;binary` suffix for the attribute name when setting up the mapping. For information, see OPENAM-8194.

1.3. What's New in OpenAM 12.0.2

This release does not include any new product enhancements.

1.4. What's New in OpenAM 12.0.1

In addition to fixes, OpenAM 12.0.1 includes the following limited product enhancements:

- **New JVM Properties for ssoadm**. You can now specifically set the authentication module or chain for administrator logins using two JVM settings for the **ssoadm** command: `org.forgerock.openam.ssoadm.auth.indexType` and `org.forgerock.openam.ssoadm.auth.indexName`. These settings provide more control to select the exact authentication mechanisms to be used when **ssoadm** authenticates administrators in the top-level realm.

  To set the JVM properties, manually edit the **ssoadm** or **ssoadm.bat** script.

  The `indexType` property specifies the module or chain-based authentication mechanism used in the top-level realm. If the property is set, OpenAM uses only *that* authentication mechanism for administrators. Accepted values are:

- module_instance
- service
- user
- role
- level
- composite_advice
- resource

The `indexName` specifies the actual name of the authentication module/chain as controlled by the `indexType` property. For example, if `indexType` is set to `module_instance` and `indexName` is set to `LDAP`, then **ssoadm** authenticates using the LDAP authentication module. For more information, see OPENAM-816.

- **Add Option to Enable Debug Logging of Decrypted SAML Assertions**. OpenAM now provides a debug logging option to decrypt SAML assertions when OpenAM runs as a service provider and assertion encryption is enabled.

  To enable the feature, go to the `Debug.jsp` page and select the subpage where you want debugging to occur. Then, at the top of the page, click the button to turn decryption on or off. This feature operates independently of the other debug logging options on the page, so you can click Cancel or Back after pressing the button, and the setting will still be set. For more information, see OPENAM-1631.

- **Authentication Context Extensibility Support**. OpenAM supports the extensibility of authentication context classes as described in the SAMLv2 specification.

  Custom contexts are also now shown in the OpenAM console if included in the extended metadata. Note that this change does not include the ability to add new contexts via the console. Custom contexts still need to be loaded via `ssoadm/extended` metadata. For more information, see OPENAM-2238.

- **StartTLS Support for Directory Server-Based Data Stores**. You can now use StartTLS to initiate secure connections to directory server-based data stores. A new property, `sun-idrepo-ldapv3-config-connection-mode`, has been created with the possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature. For more information, see OPENAM-3714.

- **Specifying Trusted Realms Using the WindowsDesktopSSO Authentication Module**. The WindowsDesktopSSO authentication module now allows you to specify a list of trusted realms. When the setting is specified, Kerberos tokens issued by those realms will only be accepted. For more information, see OPENAM-4923.

- **StartTLS Support for AD/LDAP Authentication Modules**. You can now use StartTLS with the Active Directory and LDAP authentication modules to secure OpenAM's connection to the data stores. A new property, `openam-auth-ldap-connection-mode`, has been created with the possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature. For more information, see OPENAM-5097.

- **Default Time Limit Using Netscape SDK is Configurable**. The default timelimit for LDAP operations performed using the Netscape SDK is now configurable.

To set the property, open the OpenAM Console, and then click Configuration > Servers and Sites > Servers > *URL of the server* > Advanced to display the Advanced Properties table. Set `org.forgerock.openam.ldap.default.time=<time limit is milliseconds>`. For more information, see OPENAM-5311.

- **New Base URL Provider Service**. A new provider service has been created that allows the realm to have a configured option for obtaining the base URL (including protocol) for components that need to return a URL to the client. This service is used to provide the URL base that is used in the well-known OIDC endpoints.

  The provider service offers the following:

  - A radio button option for selecting a URL source from:

    Configured value
    RFC7239 Forwarded header
    X-Forwarded-Host + X-Forwarded-Proto headers
    Host and protocol from the incoming AM request
    an extension point that returns a base URL from a given `HttpServletRequest`.

  - A check box to include or exclude the container's context path.
  - A text field for specifying the configured fixed value if required.
  - A text field for specifying the extension class if required.

  For more information, see OPENAM-5534.

1.5. What's New in OpenAM 12.0.0

OpenAM 12.0.0 is a major release that introduces new features and enhancements to OpenAM.

New Features for Users

- **User Self-Service**

  OpenAM supports self-service user registration, device management and password reset - reducing costs and increasing customer satisfaction.

  Self-Service User Registration

  OpenAM now offers a user self-registration service through the XUI interface. Click the Register link on the Login page and enter an email address.

  OpenAM will email you to confirm your address, and include a link to a page where you can register your details, as shown below.

For more information, see the *Administration Guide* section *Configuring User Self-Registration* in the *Administration Guide*.

Trusted Device Management

OpenAM allows you to manage a list of trusted devices from your Dashboard page.

When you log in to the console, OpenAM determines if the device you are using differs from that in a stored profile. If there are differences, you will be asked to enter a one-time password.

After the one-time password is verified, you can provide a name for the device and add it to the list of trusted devices.

Trusted devices appear in the Dashboard when you log in, as shown below, and can be removed by clicking Delete Device.

For more information, see the *Administration Guide* sections *Hints for the Device ID (Match) Authentication Module* in the *Administration Guide* and *Hints for the Device ID (Save) Authentication Module* in the *Administration Guide*.

Authorized Application Management

You can now manage your authorized applications (those that use OAuth 2.0 tokens) from the Dashboard link on the user page of the OpenAM console. In the Authorized Apps section, view your OAuth 2.0 tokens or remove them by clicking the Revoke Access link.

- **Social Authentication**

Log in to an OpenAM protected resource by using your existing social website credentials. OpenAM supports Facebook, Google, Microsoft, or any other OpenID Connect 1.0 compliant identity provider.

The OpenAM administration console provides wizards for quickly configuring social authentication. For more information, see the *Administration Guide* section *Configuring Social Authentication* in the *Administration Guide*.

New Features for Administrators

- **New Policy Editor**

OpenAM policy configuration now supports applications. OpenAM applications act as templates for all the policies that govern access to the protected resources in your applications.

When you create or edit a policy in OpenAM console for a particular realm, you first choose the application that the policy belongs to, and then create the policy or choose the policy to edit.

The new policy editor user interface allows you to quickly create applications and complex authorization policies, using point-and-click and drag-and-drop operations.

For more information, see the *Administration Guide* chapter *Defining Authorization Policies* in the *Administration Guide*.

- **Policy Export and Import**

  You can import and export policies to and from XACML 3.0 format files. Use the files for version control, or migration between OpenAM test and production instances, for example.

  For more information, see the *Administration Guide* section *Importing and Exporting Policies* in the *Administration Guide*.

- **Extended Authorization Subjects**

  You can now choose between an SSO token and an OpenID Connect ID token as the subject to evaluate authorization policies against. OpenID Connect ID Tokens can be used when there is no current user session, for example when an offline batch processing routine acts on behalf of a user.

  For more information, see the *Administration Guide* section *Hints for the OpenID Connect id_token bearer Module* in the *Administration Guide*.

- **Scripted Authentication Modules**

  You can create custom authentication scripts to gather knowledge about a user to help determine their authentication path. A scripted authentication module runs a script to perform authentication, making it easier than ever before to develop custom authentication modules.

  For example your script could make a call to a third-party proofing service to determine risk, and require stronger authentication depending on the context of the login request.

  Scripted authentication modules have access to the same data as other modules in the chain, can access user profile data during authentication, can make HTTP calls to external services, and are sandboxed for more secure operation. The scripts are stored in OpenAM configuration data, and so transparently available across OpenAM Sites. Server-side scripts can be written in either Groovy or JavaScript.

  For details on writing authentication module scripts, see the *Developer Guide* chapter *Scripting Authentication* in the *Developer's Guide*.

  For details on configuring scripted authentication modules, see the *Administration Guide* section *Hints For Scripted Authentication Modules* in the *Administration Guide*.

- **Scripted Device Identification Modules**

  OpenAM 12.0 introduces new Device ID (Match) and Device ID (Save) authentication modules that support the ability to customize your device fingerprinting implementations.

  The Device ID (Match) Authentication Module uses the new JavaScript/Groovy scripting engine, and demonstrates how scripted modules can be used to add contextual intelligence to the login process.

For more information, see the *Administration Guide* section *Hints for the Device ID (Match) Authentication Module* in the *Administration Guide*.

New Features for Developers

- **REST STS for Token Transformation**

  Use the RESTful Security Token Service (REST STS) to convert tokens in the various formats that OpenAM supports, such as OpenID Connect, X.509, and SSO, into a SAML2 token. Given the variety of token types in use today, it can be helpful to have a configurable service that transform tokens.

  For more information, see the *Administration Guide* chapter *The RESTful Security Token Service* in the *Administration Guide*.

- **OAuth 2.0 and OpenID Connect 1.0 Improvements**

  Make use of improved support of the OAuth 2.0 and OpenID Connect 1.0 standards, widely used in mobile and web applications. OpenAM rigorously enforces these standards, improving interoperability, and shortening development lead times.

  For more information, see the *Developer's Guide* chapter *RESTful OAuth 2.0 and OpenID Connect 1.0 Services* in the *Developer's Guide*.

  OpenAM also supports the *JSON Web Token (JWT) Profile for OAuth 2.0 Client Authentication and Authorization Grants* (OPENAM-4394). This profile allows OAuth 2.0 clients to use JWTs for authentication and to request access tokens. For more information, see "Defining Applications" in the *Developer's Guide*.

- **Fine-Grained Policy APIs**

  Author sophisticated authorization policies by using OpenAM's RESTful interfaces. Manage realms, applications, and policies, list application, condition, and subject types, and request policy decisions using the API, simplifying your applications and deployment.

  For more information, see the *Developer's Guide* chapter *RESTful Authorization and Policy Management Services* in the *Developer's Guide*.

- **GSMA Mobile Connect Support**

  OpenAM now includes support for GSMA Mobile Connect, a profile of OpenID Connect 1.0.

  Mobile Connect lets you authenticate with a mobile phone, regardless of the service or the device on which it is consumed. This allows mobile network operators to serve as identity providers for their customers.

  For more information, see the *Administration Guide* section *Using OpenAM with Mobile Connect* in the *Administration Guide*.

- **REST API Versioning**

OpenAM now assigns REST API features version numbers, to help with backwards-compatibility. You can specify the required version to use when making a call.

Use the versioning to insulate your REST clients against breaking changes when upgrading an OpenAM instance.

For more information, see the *Developer's Guide* section *REST API Versioning* in the *Developer's Guide*.

- **Support for the Latest Platforms**

  OpenAM supports the latest platforms such as Java 8 and Apache Tomcat 8.

  For more information on OpenAM requirements and supported versions, see "*Before You Install OpenAM 12.0.x Software*".

Chapter 2

Security Advisories in OpenAM 12

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For more information on ForgeRock's security advisory policy, click the following link: http://www.forgerock.com/services/security-policy/

2.1. Security Advisories in OpenAM 12.0.4

- OpenAM Security Advisory #201608-01.
- OpenAM Security Advisory #201608-02.

2.2. Security Advisories in OpenAM 12.0.3

- OpenAM Security Advisory #201604-01.
- OpenAM Security Advisory #201604-02.
- OpenAM Security Advisory #201604-03.
- OpenAM Security Advisory #201604-04.
- OpenAM Security Advisory #201604-05.
- OpenAM Security Advisory #201604-06.
- OpenAM Security Advisory #201601-01.
- OpenAM Security Advisory #201601-02.
- OpenAM Security Advisory #201601-03.
- OpenAM Security Advisory #201601-04.
- OpenAM Security Advisory #201601-05.

- OpenAM Security Advisory #201601-06.
- OpenAM Security Advisory #201601-07.
- OpenAM Security Advisory #201601-08.
- OpenAM Security Advisory #201601-09.
- OpenAM Security Advisory #201601-10.
- OpenAM Security Advisory #201601-11.
- OpenAM Security Advisory #201601-12.
- OpenAM Security Advisory #201601-13.
- OpenAM Security Advisory #201601-14.
- OpenAM Security Advisory #201601-15.
- OpenAM Security Advisory #201507-01.
- OpenAM Security Advisory #201507-02.

2.3. Security Advisories in OpenAM 12.0.2

- OpenAM Security Advisory #201506-01
- OpenAM Security Advisory #201506-02

2.4. Security Advisories in OpenAM 12.0.1

- OpenAM Security Advisory #201503-01.
- OpenAM Security Advisory #201503-02.
- OpenAM Security Advisory #201503-03.
- OpenAM Security Advisory #201505-01.
- OpenAM Security Advisory #201505-02.
- OpenAM Security Advisory #201505-03.
- OpenAM Security Advisory #201505-04.
- OpenAM Security Advisory #201505-05.

Chapter 3

Before You Install OpenAM 12.0.x Software

This chapter covers software and hardware prerequisites for installing and running OpenAM server software.

ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.

3.1. OpenAM Operating System Requirements

ForgeRock supports customers using OpenAM server software on the following operating system versions.

- CentOS 6, 7
- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2
- Oracle Linux 6, 7
- Oracle Solaris x64 10, 11
- Oracle Solaris SPARC 10, 11
- Red Hat Enterprise Linux 6, 7
- SuSE Linux 11
- Ubuntu Linux 12.04 LTS, 14.04 LTS

3.2. Java Requirements

OpenAM server software runs in a Java EE Web container, and requires a Java Development Kit.

ForgeRock supports customers using the following Java versions. ForgeRock recommends the most recent Java update, with the latest security fixes.

- Oracle Java Development Kit 6, 7, or 8
- IBM Java Development Kit 6 or 7 (when deploying in WebSphere only)

3.3. OpenAM Web Application Container Requirements

ForgeRock supports customers using OpenAM server software in the following web application container versions.

- Apache Tomcat 6, 7, 8[1]
- IBM WebSphere Application Server 8, 8.5
- JBoss Enterprise Application Platform 6
- JBoss Application Server 7
- Oracle WebLogic Server 11g, 12c

The web application container must be able to write to its own home directory, where OpenAM stores configuration files.

[1] OpenAM supports Tomcat 8.0.x, but not 8.5.x. Tomcat 8.5.x is supported in Access Management 5.

3.4. Data Store Requirements

The following table summarizes OpenAM data store support.

Supported Data Stores

Data Store	Versions	Core Token Service (CTS) Data Store	Configuration Data Store	User Data Store
Embedded OpenDJ (included in OpenAM)	2.6.2	Supported	Supported	Supported
External OpenDJ	2.6, 2.6.2	Supported	Supported	Supported
IBM Tivoli Directory Server	6.3			Supported
Microsoft Active Directory	2008, 2008 R2, 2012, 2012 R2			Supported
Oracle Directory Server Enterprise Edition	11g	**NOT SUPPORTED**	Supported When using DSEE as a configuration store, you must set up an external OpenDJ directory service as a Core Token Service data store as well, and you must configure OpenAM to use the external OpenDJ directory service as the CTS data store.	Supported
Oracle Unified Directory	11g		Supported	Supported

3.5. Browser Requirements

The following table summarizes browser support.

Supported Platforms & Browsers

Client Platform	Chrome 16 or later	Internet Explorer 9 or later	Firefox 3.6 or later	Safari 5 or later
Apple iOS 7 or later	Supported			Supported
Apple Mac OS X 10.8 or later	Supported		Supported	Supported
Google Android 4.3 or later	Supported			
Microsoft Windows 7 or later	Supported	Supported	Supported	Supported
Ubuntu Linux 12.04 LTS or later	Supported		Supported	

3.6. Native Application Platform Requirements

ForgeRock supports customers' use of OpenAM REST and other client APIs in native applications on the following platforms.

- Apple iOS 7 or later
- Apple Mac OS X 10.8 or later
- Google Android 4.3 or later
- Microsoft Windows 7 or later
- Ubuntu Linux 12.04 LTS or later

Other combinations might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on one of these platforms.

3.7. Special Requests

If you have a special request regarding support for a combination not listed here, contact ForgeRock at info@forgerock.com.

Chapter 4

Installing or Upgrading

This chapter covers installing and upgrading OpenAM 12.0.4 software.

Before you install OpenAM or upgrade your existing OpenAM installation, read these release notes. Then, install or upgrade OpenAM.

- If you are installing OpenAM for the first time, see the Installation Guide.
- If you have already installed OpenAM, see the Upgrade Guide.

  Do *not* perform an upgrade by deploying the new version and then importing an existing configuration by running the **ssoadm import-svc-config** command. Importing an outdated configuration can result in a corrupted installation.

Chapter 5

OpenAM Changes & Deprecated Functionality

This chapter covers both major changes to existing functionality, and also deprecated and removed functionality.

5.1. Important Changes to Functionality in OpenAM 12

The following functionality has been changed in OpenAM 12:

5.1.1. Important Changes to Existing Functionality in OpenAM 12.0.4

The following changes are listed in OpenAM 12.0.4:

- **OAuth 2.0 tokeninfo endpoint changed**. The OAuth 2.0 `tokeninfo` endpoint now returns the `client_id` in the response.
- **SAML status codes proxied to Service Providers**. The OpenAM IdP proxy implementation now proxies SAML status codes that were received from the remote IdP over to the SPs.
- **SAML v2.0 Bearer Assertion Profile changes**. Fixes made to support SAML assertions that do not include a `KeyInfo` element mean the following additional checks are also performed:
  - The issuer of the assertion must be configured as a remote IdP.
  - The audience of the assertion must be configured as a hosted SP.
  - The hosted SP and the remote IdP must be in the same Circle Of Trust.
- **The OAuth 2.0 SAML grant assertion parameter must now be Base64 URL encoded.**. For more information, see Using SAML Assertions as Authorization Grants in *RFC 7522*.
- **New `csrf` parameter required by the `/oauth2/authorize` endpoint**. The `/oauth2/authorize` endpoint requires a new `csrf` parameter. The value of the parameter duplicates the contents of the `iPlanetDirectoryPro` cookie, which contains the SSO token of the resource owner giving consent.

  For example:

```
$ curl \
 --request POST \
 --header  "Content-Type: application/x-www-form-urlencoded" \
 --Cookie "iPlanetDirectoryPro=AQIC5w...*" \
 --data "redirect_uri=http://www.example.net" \
 --data "scope=profile" \
 --data "response_type=code" \
 --data "client_id=myClient" \
 --data "csrf=AQIC5w...*" \
 --data "decision=allow" \
 --data "save_consent=on" \
 "http://openam.example.com:8080/openam/oauth2/authorize?response_type=code&client_id=myClient"\
 "&realm=/&scope=profile&redirect_uri=http://www.example.net"
```

Duplicating the cookie value helps prevent Cross-Site Request Forgery (CSRF) attacks.

Important

If you are updating from version 12.0, 12.0.1, 12.0.2, or 12.0.3 to version 12.0.4 or 13.x, you will need to update your code to include the `csrf` parameter when sending REST requests to the `/oauth2/authorize` endpoint.

- **New property required by persistent cookie authentication modules**. For each persistent cookie authentication module instance in your configuration, you must set the newly introduced `openam-auth-persistent-cookie-hmac-key` property.

  The value can be generated with the following command:

  ```
  $ openssl rand -base64 32
  ```

  Existing **ssoadm** scripts to configure the persistent cookie authentication module will need to be updated due to this change.

  Use an **ssoadm** command similar to the following to update authentication module instances:

  ```
  $ openam/bin/ssoadm update-auth-instance --realm / --name pcookie --adminid amadmin --password-file
  .pass --attributevalues openam-auth-persistent-cookie-hmac-key=$(openssl rand -base64 32)
  ```

- **Updated Embedded OpenDJ**. The embedded OpenDJ server has been updated to version 2.6.4, replacing the previous 2.6.1.
- **.NET Fedlet Documentation Moved**: The .NET Fedlet documentation is now a KB article available to ForgeRock customers.

5.1.2. Important Changes to Existing Functionality in OpenAM 12.0.3

The following changes are listed in OpenAM 12.0.3:

- **Changes to SAML 2.0 NameID Persistence**. OpenAM's SAML 2.0 account management and NameID persistence logic has been updated to work better with non-persistent NameID formats.

The NameID persistence logic is summarized as follows:

```
Persistent NameID           -> NameID MUST be stored
Transient NameID            -> NameID MUST NOT be stored
Ignored user profile mode -> NameID CANNOT be stored (fails if used in
combination with persistent NameID-Format)
For any other case          -> NameID MAY be stored based on customizable logic
```

The following changes have been made on the identity provider side:

- **New Setting: idpDisableNameIDPersistence**. OpenAM now provides a new setting, `idpDisableNameIDPersistence`, which disables the storage of the NameID values for all NameIDs issued by that IdP instance, as long as the NameID-Format is anything but `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.

- **SP's spDoNotWriteFederationInfo Repurposed**. The SP's `spDoNotWriteFederationInfo` setting has been repurposed. It no longer is specific to unspecified NameID-Formats. Now, it affects all non-persistent NameID-Formats, similar to the `idpDisableNameIDPersistence` setting in the IdP configuration.

- **NameID Lookup Changes**. The NameID lookup mechanism has been modified, so that it only tries to look up existing NameID values for the user if the NameID is actually persisted for the corresponding NameID-Format.

- **New Method in the IDPAccountMapper Interface**. The `IDPAccountMapper` interface has been extended with the following new method:

```
/**
      * Tells whether the provided NameID-Format should be persisted in the user data
      *       store or not.
      *
      * @param realm The hosted IdP's realm.
      * @param hostEntityID The hosted IdP's entityID.
      * @param remoteEntityID The remote SP's entityID.
      * @param nameIDFormat The non-transient, non-persistent NameID-Format in question.
      * @return true if the provided NameID-Format should be persisted
      *       in the user data store, false otherwise.
      */
      public boolean shouldPersistNameIDFormat(String realm, String hostEntityID,
      String remoteEntityID,String nameIDFormat);
```

  The default implementation of `shouldPersistNameIDFormat` in `DefaultIDPAccountMapper` first checks whether `idpDisableNameIDPersistence` is enabled in the hosted IdP configuration. If `idpDisableNameIDPersistence` is disabled, the logic advances and accesses the remote SP's `spDoNotWriteFederationInfo` flag.

The following changes have been made on the service provider side:

- **Changes to SPAccountMapper**. The `SPAccountMapper` implementations now no longer need to perform reverse lookups using the received NameID value. The `SPACSUtils` now performs the reverse lookup if the NameID-Format should be persisted. This change was made to ensure that NameID values are only persisted in the data store if they have not been stored there previously.

- **SP's spDoNotWriteFederationInfo Repurposed**. The SP's `spDoNotWriteFederationInfo` setting has been repurposed. It no longer is specific to unspecified NameID-Formats. It affects all non-persistent NameID-Formats.

- **New Method in the SPAccountMapper Interface**. The `SPAccountMapper` interface has been extended with the following new method:

```
/**
      * Tells whether the provided NameID-Format should be persisted in the user data
      *       store or not.
      *
      * @param realm The hosted SP's realm.
      * @param hostEntityID The hosted SP's entityID.
      * @param remoteEntityID The remote IdP's entityID.
      * @param nameIDFormat The non-transient, non-persistent NameID-Format in question.
      * @return true if the provided NameID-Format should be persisted
      *       in the user data store, false otherwise.
      */
      public boolean shouldPersistNameIDFormat(String realm, String hostEntityID,
      String remoteEntityID, String nameIDFormat);
```

  The default implementation of `shouldPersistNameIDFormat` in `DefaultLibrarySPAccountMapper` checks whether `spDoNotWriteFederationInfo` is enabled in the hosted SP configuration.

  For more information, see OPENAM-6021.

- **OAuth v2.0 Token Administration Endpoint No Longer Lists All Tokens**. When querying the `/frrest/oauth2/token` REST endpoint as an admin user, the `_queryId` must contain `userName=`*`username`*. The OAuth v2.0 Token Administration endpoint no longer retrieves all tokens if the `SSOTokenID` for the OpenAM superuser is passed. This feature was found to be a potential problem if you had a very large number of tokens in the system. For information, see OPENAM-5847.

5.1.3. Important Changes to Existing Functionality in OpenAM 12.0.2

The following changes are listed in OpenAM 12.0.2:

- **OAuth2 Tokeninfo Endpoint is No Longer Realm-Specific**. Requests made to the `/oauth2/tokeninfo` endpoint no longer need to specify the realm the provided OAuth2 access token belongs to.

  For more information, see OPENAM-6534.

5.1.4. Important Changes to Existing Functionality in OpenAM 12.0.1

These changes are new in OpenAM 12.0.1:

- **Agent Group Membership Now Stored in Agent Profile**. Agent group membership information is now stored as part of the agent profile using the `agentgroup` attribute. You can assign an agent to a group by simply setting the `agentgroup` property upon creation. You can also use the **ssoadm show-agent** command to return the group membership detail in the `agentgroup` attribute. Note that the existing **ssoadm** commands (for example, `add-agent-to-grp` and `remove-agent-from-grp`) are still the preferred methods for managing group membership information.

  During upgrade, agent profiles will be automatically upgraded to use the new `agentgroup` attribute to store the group's name.

  For more information, see OPENAM-718.

- **Updated weblogic.xml for WebLogic**. When running OpenAM on WebLogic 11g, you must add a WebLogic-specific descriptor file, `WEB-INF/weblogic.xml` in the `.war` before deployment. The descriptor file maps resources defined for OpenAM in WebLogic deployments.

  An example `weblogic.xml` file is presented below:

```
<?xml version="1.0" encoding="UTF-8"?>
<weblogic-web-app xmlns="http://xmlns.oracle.com/weblogic/weblogic-web-app"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://xmlns.oracle.com/weblogic/weblogic-web-app
    http://xmlns.oracle.com/weblogic/weblogic-web-app/1.3/weblogic-web-app.xsd">

    <context-root>/openam</context-root>
    <container-descriptor>
       <prefer-application-packages>

          <!-- Use bundled Jersey library -->
          <package-name>com.sun.jersey.*</package-name>
          <package-name>com.sun.research.ws.wadl.*</package-name>
          <package-name>com.sun.ws.rs.ext.*</package-name>

          <!-- Rhino -->
          <package-name>org.mozilla.javascript.*</package-name>

          <package-name>org.apache.commons.lang.*</package-name>
       </prefer-application-packages>
    </container-descriptor>
</weblogic-web-app>
```

  For more information see, OPENAM-3333.

- **AD/LDAP/RADIUS Authentication Modules Allow More Than One Primary/Secondary Server**. The Active Directory, LDAP, and RADIUS authentication modules now allow one or more servers to be designated as primary or secondary servers.

When authenticating users from a directory server that is remote to OpenAM, 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, OpenAM determines priority within the primary and secondary remote servers, respectively, as follows:

- Every LDAP server that is mapped to the current OpenAM instance has highest priority.

  For example, if you are connected to `openam1.example.com` and `ldap1.example.com` is mapped to that OpenAM instance, then OpenAM uses `ldap1.example.com`.

- Every LDAP server that was not specifically mapped to a given OpenAM instance has the next highest priority.

  For example, if you have another LDAP server, `ldap2.example.com`, that is not connected to a specific OpenAM server and if `ldap1.example.com` is unavailable, OpenAM connects to the next highest priority LDAP server, `ldap2.example.com`.

- LDAP servers that are mapped to different OpenAM 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`.

For more information, see OPENAM-3575.

- **StartTLS Support for Directory Server-Based Data Stores**. You can now use StartTLS to initiate secure connections to directory server-based data stores. A new property, `sun-idrepo-ldapv3-config-connection-mode`, has been created and has possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature.

  The `sun-idrepo-ldapv3-config-connection-mode` property replaces `sun-idrepo-ldapv3-config-ssl-enabled`, which has been removed from the configuration schema (`sunIdentityRepositoryService`).

  OpenAM automatically updates the `sun-idrepo-ldapv3-config-ssl-enabled` property to the `sun-idrepo-ldapv3-config-connection-mode` property when you upgrade. To enable StartTLS, set the `sun-idrepo-ldapv3-config-connection-mode` property to `StartTLS`. You will also need to update existing **ssoadm** scripts to use the new `sun-idrepo-ldapv3-config-connection-mode` property.

  For more information, see OPENAM-3714.

- **Move of OAuth 2.0 Well-Known Endpoints**. The well-known endpoints have been moved from `/openam/.well-known` to `/openam/oauth2/.well-known`.

  For more information, see OPENAM-4333.

- **StartTLS Support for AD/LDAP Authentication Modules**. You can now use StartTLS with the Active Directory and LDAP authentication modules to secure OpenAM's connection to the data stores. A new property, `openam-auth-ldap-connection-mode`, has been created with the possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature.

  The `openam-auth-ldap-connection-mode` property replaces the `iplanet-am-auth-ldap-ssl-enabled` property, which has been removed from the configuration schema (`sunAMAuthADService` and `iPlanetAMAuthLDAPService`).

  OpenAM automatically updates the `iplanet-am-auth-ldap-ssl-enabled` property to the `openam-auth-ldap-connection-mode` property when you upgrade. You must manually set the value of the `openam-auth-ldap-connection-mode` to `StartTLS` to initiate a StartTLS connection to the data store. You will also need to update existing **ssoadm** scripts to use the new `openam-auth-ldap-connection-mode` property.

  For more information, see OPENAM-5097.

- **AD Authentication Module Now Provides iplanet-am-auth-ldap-ssl-trust-all**. The `iplanet-am-auth-ldap-ssl-trust-all` property in the Active Directory authentication module enables the `X509TrustManager` to trust all certificates when the Active Directory authentication module connects to AD servers protected by self-signed or invalid (for example, invalid hostnames) certificates.

  Caution: Use this property with care as it bypasses the normal certificate verification process.

  For more information, see OPENAM-5460.

- **Addional JVM Properties for WebSphere Installs**. OpenAM 12.0.1 requires an updated step when running OpenAM on WebSphere. The JVM settings require additional properties to be set.

```
-DamCryptoDescriptor.provider=IBMJCE
-DamKeyGenDescriptor.provider=IBMJCE
-Djavax.xml.parsers.DocumentBuilderFactory=org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
-Djavax.xml.parsers.SAXParserFactory=org.apache.xerces.jaxp.SAXParserFactoryImpl
```

  Run the following procedures to set up the JVM properties on WebSphere. Note that these steps were run on WebSphere 8.5 on a Windows platform:

  1. Log in to the WebSphere console.
  2. In the left pane, expand Servers.
  3. Expand Server Types.
  4. Click WebSphere application servers.
  5. In the right pane, click on the server name.
  6. In the Server infrastructure section, expand Java and Process Management.
  7. Click Process definition.

8. In the Advanced properties section, click Java Virtual Machine.
9. In the Generic JVM arguments text field, add the JVM properties.
10. Save the configuration.

For more information, see OPENAM-6109.

- **OAuth2 Scopes Behavior Affected By Upgrade**. After an upgrade, OAuth 2.0 scope behavior uses a deprecated implementation class, `org.forgerock.openam.oauth2.provider.impl.ScopeImpl`.

  The workaround is to manually update the OAuth 2.0 providers to use the `org.forgerock.openam.oauth2.OpenAMScopeValidator`.

  For background information, see OPENAM-6319.

5.1.5. Important Changes to Existing Functionality in OpenAM 12.0.0

- All OpenAM core server, tools, and agent installers now display a software license acceptance screen prior to configuration. You must agree to the license to continue the configuration.

  For users implementing scripted or silent installs, the installers and upgrader tools provide a `--acceptLicense` command-line option, indicating that you have read and accepted the terms of the license. If the option is not present on the command-line invocation, the installer or upgrader will interactively present a license agreement screen to the user.

- When you visit the Policies tab for a realm in OpenAM console, OpenAM now directs you to the new policy editor. For instructions on using the new policy editor, see the *Administration Guide* chapter, *Defining Authorization Policies* in the *Administration Guide*. Notice that policies now belong to applications as described in that chapter.

  OpenAM has changed its internal representation for policies to better fit the underlying implementation, which is based on a new engine designed for higher performance and finer grained policies. When you upgrade to this version, OpenAM migrates your policies to the new representation.

  Depending on your existing policies before upgrade, you can see the following differences:

  - Existing policies with multiple resource rules map to multiple new policies.

    When a single policy maps to multiple policies during migration, OpenAM appends a number to the existing name for each new policy. This allows you to recognize the set of policies when you must manage them together, for example to change them all in the same way.

    This behavior is to optimize policy evaluation performance. The newer policy engine matches resources to policies during evaluation with indexing that proves very efficient as long as each policy specifies one resource pattern. OpenAM processes the list of resources in policies in linear fashion, so long lists of resources can slow policy evaluation.

- Conditions in existing policies map to newer representations.

  New representations exist for all existing conditions provided in OpenAM out of the box. Custom conditions developed for your deployment do not map to any of the newer conditions provided. In that case you must implement your custom conditions by implementing the newer service provider interfaces, and then replace your existing policies to use them.

  To see how to implement a custom policy plugin, see the *Developer's Guide* chapter, *Customizing Policy Evaluation* in the *Developer's Guide*.

- When OpenAM encounters issues migrating policies during upgrade, it writes messages about the problems in the upgrade log. When you open a policy in the policy editor that caused problems during the upgrade process the policy editor shows the issues, but does not let you fix them directly. Instead you must create equivalent, corrected policies in order to use them in OpenAM.

- It is strongly recommended *not* to use the forward slash character in policy names. Users running OpenAM servers on Tomcat and JBoss web containers will not be able to manipulate policies with the forward slash character in their names without setting the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` argument in the `CATALINA_OPTS` environment variable before starting the OpenAM web container.

  It is also strongly recommended not to enable the `ALLOW_ENCODED_SLASH=true` setting while running OpenAM in production. Using this option introduces a security risk. See Apache Tomcat 6.x Vulnerabilities and the related CVE for more information.

  If you have policy names with forward slashes after migration to OpenAM 12, rename the policies so that they do not have forward slashes. Perform the following steps if you use Tomcat or JBoss as your OpenAM web container:

  1. Stop the OpenAM web container.
  2. Add the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting to the `CATALINA_OPTS` environment variable.
  3. Restart the OpenAM web container.
  4. Rename any policies with forward slashes in their names.
  5. Stop the OpenAM web container.
  6. Remove the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting from the `CATALINA_OPTS` environment variable.
  7. Restart the OpenAM web container.

OpenAM configuration has changed in several ways to accommodate the changes to the way policies are managed:

- The Policy Configuration Service is simplified. For details see the *Reference* section, *Policy Configuration* in the *Reference*.

- OpenAM now requires policy referrals only when an application is administered across multiple realms, as can be the case when one policy agent protects multiple applications. Otherwise, OpenAM can use new settings in policy agent profiles to direct policy agent requests to the appropriate realm and application.

  Note

  Referrals are not shown by default in the policy editor. To enable them, in the OpenAM console, select Configuration > Global > Policy Configuration, set Activate Referrals to Enabled, and then click Save.

  The web and Java EE policy agent profiles includes the new settings under OpenAM Services > Policy Client Service in OpenAM console. These new settings allow you to set the realm and application for a policy agent. The settings are compatible with existing policy agents, as they are not used by the policy agents themselves, but instead by OpenAM when handling policy agent requests.

The fix for OPENAM-3509 ensures that OpenAM considers a trailing slash as part of the resource name to match. This improves compatibility between self and subtree modes, and compatibility with older policy agents.

- The Device ID (Match), HMAC One-Time Password (HOTP), and Device ID (Save) modules, configured together in an authentication chain, provide the same functionality as the Device Print Authentication module that is present in OpenAM 11.x versions.

  The Device Print authentication module is only available for OpenAM 11.x versions and their upgrades. If you have upgraded from OpenAM 11.x to OpenAM 12.0 you can still use the Device Print module, customize it, and create new instances of the module or use the Device ID (Match) and Device ID (Save) modules.

  Important

  The Device ID (Match) profiles (that is, device fingerprints) are incompatible with profiles created from the Device Print authentication module. If the user has existing device print profiles, created from the Device Print authentication module, these old profiles will always fail to match the client's new device profiles using the scripted Device ID (Match) module even when using the same device.

  With the Device ID (Match) and Device ID (Save) modules, the user must re-save each device profile, which deletes the old 11.x profiles stored for the user.

- As part of a fix for OpenID Connect ID Token signing, the password storage format for OAuth 2.0 clients has changed. As a result you must reset OAuth 2.0 client passwords after upgrade. For details, see the *Upgrade Guide* procedure *To Complete Upgrade from OpenAM 11.0* in the *Upgrade Guide*

- Following a change to the SAML 2.0 pages in OpenAM, you no longer customize `saml2login.template` and `saml2loginwithrelay.template` to add a progress bar for single sign on. Instead, customize `saml2/jsp/autosubmitaccessrights.jsp` as described in the procedure, *To Indicate Progress During SSO* in the *Administration Guide*.

- Changing passwords by using a PUT REST API call is no longer supported.

  Use a POST request to `/json/subrealm/users/username?_action=changePassword` to change a password.

- The response returned when submitting incorrect credentials to `/json/authenticate` has changed as follows:

  - *OpenAM 11.0.1*

    ```
    {
          "errorMessage": "Authentication Failed!!",
          "failureUrl": "https://openam.example.com:8443"
    }
    ```

  - *OpenAM 12.0.0*

    ```
    {
          "code": 401,
          "reason": "Unauthorized",
          "message": "Authentication Failed!!",
          "detail": {
             "failureUrl": "https://openam.example.com:8443"
          }
    }
    ```

- When running OpenAM on WebLogic 11g, you must add a WebLogic-specific descriptor file, `WEB-INF/weblogic.xml` to the .war before deployment.

- In the OpenID Connect 1.0 module you can map local user profile attributes to OpenID Connect Token claims, allowing the module to retrieve the user profile based on the ID Token. The key is the ID Token field name and value is the local user profile attribute name. The default has been changed as follows: mail=email, uid=sub. (OPENAM-5263)

- The class hierarchy for the `ResourceName` interfaces has changed. Previous implementations should be source-compatible, but will not be binary-compatible, and will need recompiling.

- The OAuth2 provider uses RSA as its default encryption algorithm. The default OAuth2 client agent configuration has been changed to RS256 to match the OAuth2 provider algorithm. The client agent continues to support HMAC algorithms; only the default encryption algorithm has been changed to support out-of-the-box functionality. (OPENAM-5279)

- The distributed authentication service (DAS) and cross-domain single sign-on (CDSSO) do not support the `iPSPCookie/DProPCookie` query string parameter to set a `DProPCookie` in the user-agent as a mechanism for cookie persistence. Neither DAS nor CDSSO retains `iPSPCookie=yes`.

- Updates to OAuth 2.0 and OpenID Connect authentication modules mean that any custom implementations of `org.forgerock.openam.authentication.modules.oauth2.AccountMapper` or `org.forgerock.openam.authentication.modules.oauth2.AttributeMapper` no longer work, and needs to be reimplemented against `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` and/or `org.forgerock.openam.authentication.modules.common.mapping.AccountProvider` as appropriate.

- The XUI, now the default for end-user pages, handles DNS/realm alias differently from the classic UI, which was the default in previous OpenAM versions. With the classic UI, the realm alias is specified both in the host name and the URI path. With the XUI, the host name alone specifies the realm. The XUI evaluates a realm specified in the path of the URL as a subrealm of the realm specified by the host name alias.

  For example, with the classic UI, you could authenticate to a realm, `realm1` using the DNS alias `realm1.example.com:8080` and the realm query parameter, `realm=realm1`, as follows:

  ```
  http://realm1.example.com:8080/openam/UI/Login?realm=realm1
  ```

  With XUI, you do not include a realm in the URI if it has already been mapped as now any URI realm is additive and specifies a subrealm of the DNS alias realm. For example, using the following URL indicates that you are attempting to authenticate to `/realm1/realm1` (that is, the sub-realm, `realm1` under the realm, `realm1`).

  ```
  http://realm1.example.com:8080/openam/XUI/#Login/realm1
  ```

  As another example, if you have a sub-realm called `test` under `/realm1` and make a request to:

  ```
  http://realm1.example.com:8080/openam/XUI/#Login/test
  ```

  The request authenticates to `/realm1/test`. Note also that the use of URI realm is preferred over realm as a query parameter.

5.2. Deprecated Functionality in OpenAM 12

The following functionality has been deprecated in OpenAM 12 and will likely be removed in a future release:

5.2.1. Deprecated Functionality in OpenAM 12.0.4

- No functionality has been deprecated in this release.

5.2.2. Deprecated Functionality in OpenAM 12.0.3

- No functionality has been deprecated in this release.

5.2.3. Deprecated Functionality in OpenAM 12.0.2

- No functionality has been deprecated in this release.

5.2.4. Deprecated Functionality in OpenAM 12.0.1

- No functionality has been deprecated in this release.

5.2.5. Deprecated Functionality

The following functionality is deprecated in OpenAM 12.0.0, and is likely to be removed in a future release.

- Classic (JATO-based) UI is deprecated for end user pages. OpenAM offers the JavaScript-based XUI as a replacement. Classic UI for end user pages is likely to be removed in a future release.
- Older REST services relying on the following endpoints are deprecated.

  /identity/attributes
  /identity/authenticate
  /identity/authorize
  /identity/create
  /identity/delete
  /identity/isTokenValid
  /identity/logout
  /identity/read
  /identity/search
  /identity/update
  /ws/1/entitlement/decision
  /ws/1/entitlement/decisions
  /ws/1/entitlement/entitlement
  /ws/1/entitlement/entitlements

  The following table shows how legacy and newer endpoints correspond.

REST Endpoints

Deprecated in the *Administration Guide* URIs	**Newer Evolving in the *Administration Guide* URIs**
/identity/attributes	/json/users
/identity/authenticate	/json/authenticate
/identity/authorize	/json/policies?_action=evaluate, /json/policies?_evaluateTree
/identity/create, /identity/delete, /identity/read, /identity/search, /identity/update	/json/agents, /json/groups, /json/realms, /json/users
/identity/isTokenValid	/json/sessions/*tokenId*?_action=validate
/identity/logout	/json/sessions/?_action=logout

Deprecated in the *Administration Guide* URIs	Newer Evolving in the *Administration Guide* URIs
/ws/1/entitlement/decision, /ws/1/entitlement/decisions, /ws/1/entitlement/entitlement, /ws/1/entitlement/entitlements	/json/policies?_action=evaluate, /json/policies?_evaluateTree
N/A	/json/applications
N/A	/json/applicationtypes
N/A	/json/conditiontypes
N/A	/json/dashboard
N/A	/json/decisionscombiners
N/A	/json/policies
N/A	/json/referrals
N/A	/json/serverinfo
N/A	/json/subjectattributes
N/A	/json/subjecttypes
N/A	/xacml/policies

Find examples in the *Developer Guide* chapter *Using RESTful Web Services* in the *Developer's Guide*.

Support for the older REST services is likely to be removed in a future release in favor of the newer REST services. Older REST services will be removed only after replacement REST services are introduced.

- With the implementation of XACML 3.0 support when importing and exporting policies the following `ssoadm` commands have been replaced:

Policy Import and Export with ssoadm

Deprecated in the *Administration Guide* Command	Newer Evolving in the *Administration Guide* Command
`create-policies`	`create-xacml`
`delete-policies`	`delete-xacml`
`list-policies`	`list-xacml`
`update-policies`	`create-xacml`

For more information, see the *OpenAM Reference* section ssoadm — configure OpenAM core services in the *Reference*.

- With the implementation of OAuth 2.0 in this release, the following OAuth JSP endpoints are deprecated and targeted for future removal:

`deleteconsumer.jsp`

This endpoint is used to delete consumer systems, which get resources from service providers (SPs) based on OAuth 1.0 tokens.

`deletetoken.jsp`

This endpoint is used to delete an existing OAuth 1.0 token.

`index.jsp`

Specifies an endpoint used to register and delete service consumers, which get resources from SPs. Provides access to registerconsumer.jsp and deleteconsumer.jsp. Associated with OAuth 1.0.

`registerconsumer.jsp`

Defines an endpoint used to register a consumer of services from SPs. Associated with OAuth 1.0.

`userconsole.jsp`

Allows a user to authorize or revoke a request for an OAuth 1.0 token.

- The Netscape LDAP API is to be removed from OpenAM, with OpenAM using the OpenDJ LDAP SDK instead. This affects all classes in `com.sun.identity.shared.ldap.*` packages.
- OpenAM currently uses Sun Java System Application Framework (JATO). JATO is deprecated and is likely to be replaced in a future release.
- With the implementation of the Persistent Cookie authentication module, the Core Authentication module persistent cookie options are deprecated and are likely to be removed in a future release.
- The OAuth 2.0 plugin interface for custom scopes, `Scope` is deprecated and likely to be removed in a future release. Custom OAuth 2.0 scopes plugins now implement the `ScopeValidator` interface instead. For an example, see the *Developer's Guide* chapter, *Customizing OAuth 2.0 Scope Handling* in the *Developer's Guide*.
- The OAuth 2.0 plugin interface for custom response types, `ResponseType` is deprecated and likely to be removed in a future release. Custom OAuth 2.0 response type plugins now implement the `ResponseTypeHandler` interface instead.

5.3. Removed Functionality in OpenAM 12

The following functionality has been removed in OpenAM 12:

5.3.1. Removed Functionality in OpenAM 12.0.4

- No functionality has been removed in this release.

5.3.2. Removed Functionality in OpenAM 12.0.3

- No functionality has been removed in this release.

5.3.3. Removed Functionality in OpenAM 12.0.2

- **Removal of Unused Install-Time LDAP Users**. Default LDAP users that were set up during initial installation have been removed, because they were not referenced anywhere in the configuration. Any associated access control instructions to the removed entries have also been removed.

  When targeting Oracle DSEE as the user store, OpenAM no longer creates the following entries and ACIs:

  - dn: ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=dsameuser, ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=amldapuser,ou=DSAME Users, CHOSEN_SUFFIX
  - allow (all) userdn = "ldap:///cn=dsameuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - allow (read,search) userdn = "ldap:///cn=amldapuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - deny (write) userdn ="ldap:///self". The aci was updated to remove the `dsameuser` reference from the target filter.

  When targeting OpenDJ as the user store (internally or externally), OpenAM no longer creates the following entries and ACIs:

  - dn: ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX
  - allow (read,search) userdn = "ldap:///cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX";
  - allow (all) userdn = "ldap:///cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX";
  - deny (write) userdn ="ldap:///self". The aci was updated to remove the `openssouser` reference from the target filter.

New installations will not have these entries and ACIs. For upgraded deployments, you must manually remove the entries if they are not being used. For details, see the explanation in (OPENAM-1036 and in OpenAM Security Advisory #201505-05).

- The `sun-idrepo-ldapv3-config-connection-mode` property replaces `sun-idrepo-ldapv3-config-ssl-enabled`, which has been removed from the configuration schema (`sunIdentityRepositoryService`). For more information, see OPENAM-3714.

- The `openam-auth-ldap-connection-mode` property replaces `iplanet-am-auth-ldap-ssl-enabled`, which has been removed from the configuration schema (`sunAMAuthADService` and `iPlanetAMAuthLDAPService`). For more information, see OPENAM-5097.

5.3.4. Removed Functionality in OpenAM 12.0.1

- **Removal of Unused Install-Time LDAP Users**. Default LDAP users that were set up during initial installation have been removed, because they were not referenced anywhere in the configuration. Any associated access control instructions to the removed entries have also been removed.

  When targeting Oracle DSEE as the user store, OpenAM no longer creates the following entries and ACIs:

  - dn: ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=dsameuser, ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=amldapuser,ou=DSAME Users, CHOSEN_SUFFIX
  - allow (all) userdn = "ldap:///cn=dsameuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - allow (read,search) userdn = "ldap:///cn=amldapuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - deny (write) userdn ="ldap:///self". The aci was updated to remove the `dsameuser` reference from the target filter.

  When targeting OpenDJ as the user store (internally or externally), OpenAM no longer creates the following entries and ACIs:

  - dn: ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX
  - allow (read,search) userdn = "ldap:///cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX";
  - allow (all) userdn = "ldap:///cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX";

- deny (write) userdn ="ldap:///self". The aci was updated to remove the `openssouser` reference from the target filter.

New installations will not have these entries and ACIs. For upgraded deployments, you must manually remove the entries if they are not being used. For details, see the explanation in (OPENAM-1036 and in OpenAM Security Advisory #201505-05).

- The `sun-idrepo-ldapv3-config-connection-mode` property replaces `sun-idrepo-ldapv3-config-ssl-enabled`, which has been removed from the configuration schema (`sunIdentityRepositoryService`). For more information, see OPENAM-3714.
- The `openam-auth-ldap-connection-mode` property replaces `iplanet-am-auth-ldap-ssl-enabled`, which has been removed from the configuration schema (`sunAMAuthADService` and `iPlanetAMAuthLDAPService`). For more information, see OPENAM-5097.

5.3.5. Removed Functionality in OpenAM 12.0.0

- No functionality has been removed in this release.

Chapter 6

OpenAM Fixes, Limitations, & Known Issues

OpenAM issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM. This chapter covers the status of key issues and limitations at release for OpenAM 12.

6.1. Key Fixes

The following key fixes have been made for each OpenAM 12 release:

6.1.1. Key Fixes in OpenAM 12.0.4

- OPENAM-9611: InvalidStatusCodeSaml2Exception breaks the SAML2 SP Error handling in a non IDP-proxy environment.
- OPENAM-9526: Compiling the source code without git repo fails at openam-clientsdk module
- OPENAM-9407: Backport OPENAM-7556 to 12.0.x
- OPENAM-9400: NPE in LDAP module if "hasNext" throws an ErrorResultIOException
- OPENAM-9337: Attribute value in profile page is cached
- OPENAM-9290: OpenAM should send a response to the SP in case of empty NameIdPolicy value in SAML Authn Request
- OPENAM-9027: IdServiceImpl logs message level data on warning level
- OPENAM-8962: Unable to set Start and End IPCondition condition policy
- OPENAM-8944: PolicyRequestHandler does not take ignore profile into account when looking up profile attributes
- OPENAM-8919: DJLDAPv3Repo needs to escape special chars in search results.
- OPENAM-8910: NPE if a null siteID is passed to Session.validateSessionID
- OPENAM-8736: When upgrading OpenAM, upgrade can fail if sun-idrepo-ldapv3-config-ssl-enabled has not been removed.
- OPENAM-8708: Authentication can fail for users with non-ascii character in multi-server environment

- OPENAM-8689: javascript httpClient appends headers as querystring parameters
- OPENAM-8659: JSON REST authenticate endpoint doesn't check validity of sessionUpgradeSSOTokenId before returning authId
- OPENAM-8648: PostAuthentication not triggered for noSession=true authentication case
- OPENAM-8614: User status attribute mapping with Active Directory doesn't work when creating new users
- OPENAM-8578: The default WS-Fed and SAML2 IDP attribute mapper should provide a way to Base64 binary encoding of NameID
- OPENAM-8567: SAML v2.0 Bearer Assertion Profile fails if SAML assertion does not include KeyInfo Element
- OPENAM-8564: "Invalid Properties" warning when updating org.forgerock.openam.url.connectTimeout with ssoadm
- OPENAM-8543: Special characters are not always escaped correctly in universal identifier DNs
- OPENAM-8533: Case sensitivity in realm name for password reset REST calls
- OPENAM-8523: J2EE Agent does not pickup "DN Restriction Only Enabled" from OpenAM configuration
- OPENAM-8521: CacheBlockBase will deadlock when com.sun.identity.idm.cache.entry.expire.enabled=true
- OPENAM-8510: com.sun.identity.saml2.cacheCleanUpInterval should only accept values > 0
- OPENAM-8494: Certain services cannot be added/modified at realm level when psearch is disabled
- OPENAM-8483: OAUTH2.0 client MUST use the HTTP "POST" method when making access token requests
- OPENAM-8474: Active Directory (AD) DataStore doesn't show User Status in OpenAM GUI
- OPENAM-8463: Creating New SAMLv2 SOAP Binding Request Handler gives errors
- OPENAM-8433: JSON Authentication does not provide correct feedback for expired session
- OPENAM-8432: LocalSSOTokenSessionModule throws NPE when dependencies are not initialized
- OPENAM-8417: IdRepo attempts to access profile when session quotas are enabled, even if 'ignore' user profile is enabled
- OPENAM-8386: NPE in DelegationPolicyImpl due to non-thread safe initialization
- OPENAM-8335: OATH shows One time password callback view even if username is not defined

- OPENAM-8268: Null authnLevel can be set in DefaultIDPAuthnContextMapper.getIDPAuthnContextInfo() if no default set.
- OPENAM-8266: TLS issue with com.iplanet.am.util.AMSendMail
- OPENAM-8250: SAML + OAuth2 flow fails with ClassCastException
- OPENAM-8243: "Illegal universal identifier null." on UMUserPasswordResetOptions in multi-instance setup
- OPENAM-8201: setup.bat of SSOAdminTools always returning exit error code 1
- OPENAM-8199: Resource based authentication does not work with more than one environment condition
- OPENAM-8171: In-memory account lockout reset doesn't work when using LDAP module
- OPENAM-8151: SAML SSO for subrealm does not correctly login user as it ignores the org param when XUI enabled
- OPENAM-8146: XUI does not honor success URL set by PAP
- OPENAM-8073: Installation randomly fails with NPE when message level logging is enabled
- OPENAM-8040: Exception when loading schema for datastore
- OPENAM-8014: NullPointer when using "Default Failure Login URL" with IDP
- OPENAM-7860: Cannot setup 12.0.x with IBM JDK 7
- OPENAM-7778: XML Signature DigestMethod should be configurable when using SAML2
- OPENAM-7750: NPE when OpenAM shut downs
- OPENAM-7443: Password Encryption Key property is incorrect - in Advanced Server configuration
- OPENAM-7254: ClassNotFoundException for DenyOverride triggered from EntitlementUtils after OpenAM installation
- OPENAM-7233: NPE after viewing the OpenAM change organization page
- OPENAM-7071: container requirements are not stated for Distributed Authentication Server
- OPENAM-6974: SAML federation failover does not work to federate additional COT SPs
- OPENAM-6470: ThemeManager.js doesn't need to strip "/" anymore when loading theme for realm
- OPENAM-6390: Retrieving User in federation returns the amIdentity with id in lower case
- OPENAM-6344: Incorrect error when password length is not valid with Forgotten Password in XUI
- OPENAM-6315: Proxying SAML2 Second level status code

- OPENAM-6188: ssoadm list-xacml with –policynames throws a com.sun.identity.entitlement.EntitlementException: Incorrect search filter
- OPENAM-6160: auth_time is updated when refreshing token
- OPENAM-5938: Cert Auth module should not read cert from HTTP request when 'iplanet-am-auth-cert-gw-cert-auth-enabled' is set
- OPENAM-5923: JCE Certificate Validation won't work for Cert module consumed in 'portal' mode
- OPENAM-5640: SAML SP ignore Conditions in Assertion.
- OPENAM-5626: XUI not redirecting to console when no datastore in top realm
- OPENAM-5428: Missing log entry error when clicking IDP services tab
- OPENAM-5367: [and { characters in uid cause problems with Privilege evaluation
- OPENAM-5213: OAuth2 tokeninfo endpoint is not returning client_id info
- OPENAM-4499: XUI cannot cope with Ignored User Profile mode
- OPENAM-3891: SAML2 session upgrade fails if the request hits a different server where the old session was created
- OPENAM-3750: REST authentication failed if unicode/utf8 login/password
- OPENAM-3574: SMSGateway is missing JavaDoc
- OPENAM-2911: IdP initiated SSO with persistent identifier causes URLNotFoundException: Invalid service host name.

6.1.2. Key Fixes in OpenAM 12.0.3

- OPENAM-1068: In case of session upgrade the SAML IDPCache can lose the ssotoken sessionindex mapping
- OPENAM-1462: OATH Module TOTP does not implement Resyncronization part of RFC6238
- OPENAM-1900: Provide support for more XML signatures types in SAML query string verification process
- OPENAM-2028: java.lang.NullPointerException at com.sun.identity.saml2.common.SAML2Utils.getRemoteServiceURL
- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-3095: When a SP sends an unsigned Authn Request using SAML ECP OpenAM sees it as a wrong message

- OPENAM-3135: XUI does not support resource based authentication
- OPENAM-3253: XUI: sunIdentityUserPassword not set in com.sun.identity.authentication.spi.ReplayPasswd
- OPENAM-3266: Heartbeat timeouts can occur during operation
- OPENAM-3381: SAML login is not handled correctly on the SP if the user already has a local session on the SP
- OPENAM-3470: The SAML2 nameid should not be persisted if the nameid-format is not persistent
- OPENAM-3693: LDAP psearch uses DN to update the cache instead of valid Universal ID
- OPENAM-3698: Federation authentication module may be retrieved from the incorrect realm when running OpenAM as an SAML SP
- OPENAM-3762: sun-idrepo-ldapv3-config-memberurl doesn't exist for LDAPv3ForOpenDS
- OPENAM-3868: Regression: NPE in WDSSO module when authenticating via ClientSDK
- OPENAM-4103: Allow sending AuthnRequests without the RequestedAuthnContext element
- OPENAM-4135: Authentication triggers a search that retrieves all attributes - IDRepo
- OPENAM-4177: Update OAuth2 access_token endpoint to handle auth chain with non-name/password callback
- OPENAM-4754: NPE when SessionID doesn't contain StorageKey for SFO
- OPENAM-4765: AdminTokenAction - retrieving the admin token is not Synchronized
- OPENAM-4983: Commands for embedded DJ should use --noPropertiesFile switch
- OPENAM-5101: Policy Editor does not handle names which contain '/' character
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5264: Can't login to OpenAM with no cookies set in the platform service
- OPENAM-5364: 11.0 format policies with "?" in the rule name cannot be edited by the Policy Editor
- OPENAM-5400: Policy Editor: Unable to edit/delete policy whose name ends in a '/' character
- OPENAM-5416: XUI not handling correctly response from REST services during authentication
- OPENAM-5467: XUI/#logout/ route ignores "goto" parameter
- OPENAM-5505: Setting openam-session-timeout-handler-list= in ssoadm set-attr-defs ends up creating a list with one empty item

- OPENAM-5530: OpenAM does not set the destination in the last leg of IDP Proxy SLO
- OPENAM-5541: Resource based auth doesn't work in sub realm
- OPENAM-5554: run-xacml-client-sample.sh packaged with ExampleClientSDK-CLI-12.0.0.zip is missing libraries
- OPENAM-5567: User attribute mapping sometimes fail
- OPENAM-5614: Jackson can not instantiate AuthnRequestInfoCopy/IDPSessionCopy from JSON object
- OPENAM-5670: Create Policy UI can't get the subject attributes if you don't have a datastore configured.
- OPENAM-5695: Allow admin users to update user's password without the old password
- OPENAM-5712: Cross-realm session upgrade with ForceAuth does not trigger #confirmLogin
- OPENAM-5721: WindowsDesktopSSO trusted realm list doesn't work
- OPENAM-5733: validationService doesn't work if the datastore isn't configured
- OPENAM-5744: Authentication level login doesn't work if the module name doesn't match the module type
- OPENAM-5755: Prevent duplicate metaAliases in SAML2 entities
- OPENAM-5759: Update OAuth2 to display the token and user information in the OAuth2Provider.access log
- OPENAM-5785: Allow ssoadm to import and export agent configurations with hashed passwords
- OPENAM-5804: Forgot password in XUI with a sub-realm when using RFC3986 specs not redirecting correctly
- OPENAM-5826: Zero Page Login disallowed after OPENAM-sec-201503 CAS is applied
- OPENAM-5834: Changes since OPENAM-2274 to DefaultLibrarySPAccountMapper has meant that NameID can't be used in some cases using auto federation
- OPENAM-5835: Redirect loop between OpenAM and J2EE Agent in case of invalid admin token
- OPENAM-5841: Realm override query parameter on login not overriding realm
- OPENAM-5847: OAuth 2.0 Token Administration Endpoint should not allow to list all tokens as 'Super User'
- OPENAM-5883: SAML Time value should allow milliseconds values with less than 3 digits
- OPENAM-5894: Can't update WindowsDesktopSSO module with ssoadm

- OPENAM-5902: Persistent cookie fails on host cookies when domain deleted via console
- OPENAM-5917: IdP proxy in a subrealm is unable to send SLO response to the remote SP
- OPENAM-5920: Realm associated with OAuth2 tokens is not normalised
- OPENAM-5921: XUI Login page does not pass username to post auth plugin
- OPENAM-5922: Getting a user's resource sets from root realm doesn't work with realm override parameter
- OPENAM-5980: CTS async queue can cause threads to wait for a long time
- OPENAM-5987: Database audit logging 'failure buffer' does not write all records after DB recovery
- OPENAM-5998: Null Pointer Exception in Session.removeSID
- OPENAM-6000: Accessing XUI through a FQDN that is resolvable but not mapped throws an internal server error
- OPENAM-6039: Asynchronous queue for OAuth2 Tokens can result in token validation failures
- OPENAM-6056: LoginViewBean does not correctly handle empty ChoiceCallbacks
- OPENAM-6069: Make org.forgerock.openam.agents.config.policy.evaluation.* optional
- OPENAM-6156: orderedlist uitype in service config breaks when updated
- OPENAM-6192: For OAuth 2.0 don't expect the default Shared Consent Attribute to contain a value on first use
- OPENAM-6196: Exception With SAML 2.0 ECP IDP Profile (PAOS Binding)
- OPENAM-6235: NameID values that contain characters such as & cause parsing issues when used in XML documents.
- OPENAM-6236: Add token life time options per OAuth2 client
- OPENAM-6237: com.sun.xml.ws.api.pipe.TransportPipeFactory - ClassNotFoundException
- OPENAM-6244: In case of GeoIp2Exception in the adaptive module, only the score of the geolocation should be affected
- OPENAM-6266: Allow the confirmation email URL in the Forgotten password service to be a relative path
- OPENAM-6273: XUI self-service links are only available when data-store auth-module is used
- OPENAM-6293: XUI freezes at startup when serverinfo service call fails
- OPENAM-6318: IdP proxy should populate the AuthenticatingAuthority element in its Responses

- OPENAM-6323: Divide the message "JWT has expired or is not valid" into two messages
- OPENAM-6362: HOTP and OATH auth-modules do not set 'failureUserID' when throwing InvalidPasswordException, this breaks OpenAM account lockout
- OPENAM-6372: Browser back button and OpenAM internal authentication error
- OPENAM-6376: OAuth2 resource owner authentication code does not pass headers to auth module
- OPENAM-6377: CTSOperations is currently performing setLatestAccessTime on a local token, rather than the remote one.
- OPENAM-6423: Post Authentication Plugin can't set headers in the logout API on REST response
- OPENAM-6443: Unable to change a user password using admin token via REST
- OPENAM-6455: ConnectionCount logic does not produce a sensible ConnectionFactory max pool size for some scenarios
- OPENAM-6468: InvalidClassException with certauth after #201505-01 patch
- OPENAM-6472: NPE when choosing No on new_org.jsp
- OPENAM-6476: Initialization of a ServiceConfigImpl may block retrieval of already cached instances
- OPENAM-6499: Configuration store servers are not listed in Directory Configuration
- OPENAM-6501: RestSecurity is instantiated every time user makes serverinfo request
- OPENAM-6503: Unable to update policies in subrealm
- OPENAM-6506: Potential NPE in OpenAMScopeValidator.evaluateScope
- OPENAM-6514: OAuth2 authorization flow stores resource owner in universalID format if persistent mode is on
- OPENAM-6534: Update OAuth2 tokeninfo endpoint to be realm-independent
- OPENAM-6545: ServerInfoResource should attempt to cache ServiceConfigs per realm rather than creating one on each request
- OPENAM-6552: access_token request sent by OAuth2Saml2GrantSPAdapter is not realm aware
- OPENAM-6553: Fix Social Authentication in subrealms
- OPENAM-6558: jwt-bearer grant type handler doesn't call additionalDataToReturnFromTokenEndpoint of the Scope Validator Plugin
- OPENAM-6613: Updating Hosted IDP Authentication Context Mapper does not save values
- OPENAM-6620: jwks_uri generates a kid value different for each server in a site configuration

- OPENAM-6627: Self-registration fails in XUI when using realms
- OPENAM-6630: Policy Editor 'Export All Policies' does not specify realm
- OPENAM-6726: Issues creating Agent client using REST API
- OPENAM-6734: Shutdown race condition between embedded OpenDJ and OpenAM persistent search restart
- OPENAM-6741: STS configuration not showing in admin console
- OPENAM-6776: SAML authentication can fail with NumberFormatException
- OPENAM-6798: Remove ORIG_URL after OAUTH2 Authentication complete
- OPENAM-6825: Fails to issue OAuth2 access token if client type confidential is inherited from group
- OPENAM-6842: PAP onLogout() method is not triggered in a multi-server environment, if the logout is invoked from the OpeAM instance in which session is not created.
- OPENAM-6867: changePassword REST endpoint is not returning LDAP issues that are related to a user mistake.
- OPENAM-6872: Improved error message in OpenSSOConfigurator
- OPENAM-6878: OpenAM forgot password search hard coded for UID
- OPENAM-6883: SystemConfigurationUtil maintains a list of server URLs that assume lowercase deployment contexts
- OPENAM-6892: Create a Shared Secret Provider plugin for the standard OATH module
- OPENAM-7002: The email attribute property defined in the email service is not used when sending e-mail in forgotten password flow
- OPENAM-7055: Improved logic for POST binding Assertion/Response signature check
- OPENAM-7070: Datastore screen error when loading schema if host list has entries with pipe
- OPENAM-7075: endSession endpoint can't kill SSO Token for some OAuth2 grant type
- OPENAM-7095: ssoadm do-batch doesn't continue if the -c flag is applied for the SAML delete-entity command
- OPENAM-7109: Allow user to adjust the size of Metadata that can be uploaded by the Common Task "Create SAMLv2 Providers" buttons.
- OPENAM-7122: json/agents/?_action=create returns inconsistent error codes when an agent name already exists

- OPENAM-7123: Allow country-specific localization in XUI
- OPENAM-7260: OAuth2 authorization flow sets wrong resource owner if alias name + LDAP auth is used.
- OPENAM-7265: Post Authentication Plugin HttpServletRequest is null in onLogout() method
- OPENAM-7298: Custom response attributes are not visible in the policy editor UI and are erased when editing policies through the UI
- OPENAM-7320: Consider using JDK JAXP/XML instead of Xerces/Xalan to keep up with JDK fixes
- OPENAM-7467: Redirect loop with XUI and resource=true when user initially authenticated to different chain
- OPENAM-7547: OpenIdConnectAuthorizeRequestValidator doesn't take default scopes into account when checking.
- OPENAM-7549: Call to userinfo unexpectedly generates "WARNING: Couldn't find any helper support the HTTP_Bearer challenge scheme."
- OPENAM-7727: debugfiles.properties missing in ClientSDK jar
- OPENAM-7778: XML Signature DigestMethod should be configurable when using SAML2
- OPENAM-7820: Additional delete/revoke token endpoints for Oauth2
- OPENAM-7864: Failure to connect to syslog server can cause OpenAM to hang
- OPENAM-7898: Increase OAuth authorization code character limit to support Azure and others
- OPENAM-7966: hiddenValueBox not showed in DAS
- OPENAM-8074: Changing an user password with the same value returns 400 with ldap errorcode=20
- OPENAM-8091: OpenAM cannot connect to a DataStore which accepts only TLSv1.2
- OPENAM-8108: Radius auth module not usable in auth-chain with 'shared-state' enabled
- OPENAM-8174: OpenAM gives an Internal Server Error when the user tries to reset their password before the minimum password age
- OPENAM-8194: The default WS-Fed IDP attribute mapper should provide a way to Base64 encode binary attributes
- OPENAM-8204: XUI does not display proper error message when changing password
- OPENAM-8225: Reading binary attributes, for example objectGUID, from the IdRepo cache not always returning valid values

- OPENAM-8237: jaxrpc-impl-1.1.3_01-041406.jar and webservices-rt-2009-29-07.jar contain the same classes
- OPENAM-8282: Password Reset questions are not randomly chosen when resetting password
- OPENAM-8327: Unable to send e-mail via Google SMTP with SSL enabled

6.1.3. Key Fixes in OpenAM 12.0.2

- OPENAM-5804: Forgot password in XUI with a sub-realm when using RFC3986 specs not redirecting correctly
- OPENAM-5826: Zero Page Login disallowed after OPENAM-sec-201503-v1102-CAS is applied
- OPENAM-5841: Realm override query parameter on login not overriding realm
- OPENAM-6000: Accessing XUI through a FQDN that is resolvable but not mapped throws an internal server error
- OPENAM-6039: Asynchronous queue for OAuth2 Tokens can result in token validation failures
- OPENAM-6293: XUI freezes at startup when serverinfo service call fails
- OPENAM-6377: CTSOperations is currently performing setLatestAccessTime on a local token, rather than the remote one.
- OPENAM-6455: ConnectionCount logic does not produce a sensible ConnectionFactory max pool size for some scenarios
- OPENAM-6457: DirectoryContentUpgrader causes Entry Already Exists exception for CTS suffix when upgrading OpenAM
- OPENAM-6468: InvalidClassException with certauth after #201505-01 patch
- OPENAM-6499: Configuration store servers are not listed in Directory Configuration
- OPENAM-6501: RestSecurity is instantiated every time user makes serverinfo request
- OPENAM-6503: Unable to update policies in subrealm
- OPENAM-6534: OAuth2 tokeninfo endpoint should be realm-independent
- OPENAM-6545: ServerInfoResource should attempt to cache ServiceConfigs per realm rather than creating one on each request
- OPENAM-6613: Updating Hosted IDP Authentication Context Mapper does not save values
- OPENAM-6627: Self-registration fails in XUI when using realms

6.1.4. Key Fixes in OpenAM 12.0.1

- OPENAM-273: com.sun.identity.policy.PolicyManager, when used in client API, does not work across multiple SSO sessions in a single JVM instance
- OPENAM-718: Agent group membership lost after backup/restore
- OPENAM-816: ssoadm authentication depends on the sunEnableModuleBasedAuth=true
- OPENAM-1036: Review install-time created LDAP users
- OPENAM-1631: Add option to enable debug logging of decrypted SAML assertions
- OPENAM-2238: Support extensibility of auth context classes as described in the SAMLv2 spec
- OPENAM-2348: set-realm-svc-attrs: "Not a supported type: realm"
- OPENAM-3296: ssoadm uses LDAP auth module first to authenticate amadmin
- OPENAM-3575: LDAP auth module fails if more than one LDAP server is configured as primary/secondary LDAP server
- OPENAM-3714: The DJLDAPv3Repo doesn't support StartTLS
- OPENAM-3856: AMAuthenticationManager can get incorrectly initialized for subrealms
- OPENAM-3877: Changing password through new REST endpoint fails if default AuthN chain needs more than just the password to authenticate
- OPENAM-4164: AgentsRepo could cache stale ServiceConfigImpl
- OPENAM-4195: SAML2token saved in CTS with hex tokenId but read without converting to hex
- OPENAM-4333: OAuth2 endpoint doesn't honour realm DNS aliases - must specify realm via URL query string
- OPENAM-4344: OAuth2Saml2GrantSPAdapter does not pass the realm to the access_token endpoint
- OPENAM-4413: Agent sessions are affected by active session quotas when com.iplanet.am.session.agentSessionIdleTime is used
- OPENAM-4605: Unable to install OpenAM Configuration Data Store into an 'ou' through the console
- OPENAM-4614: MergeAll Option cause a desynchronisation of the log rotation
- OPENAM-4644: Log file rotation isn't respected
- OPENAM-4804: SAE fails with No_App_Attrs:https error

- OPENAM-4856: HOTP auth module can not be used in auth chain if the username in sharedstate map does not 'match' the search attribute of the data store
- OPENAM-4919: DNMapper.realmNameToAMSDKName logic adding extra = when checking against orgAttr
- OPENAM-4923: Windows Desktop SSO module should allow whitelisting Kerberos realms/KDCs
- OPENAM-5034: Legacy password pages unable to handle special characters in username
- OPENAM-5065: PLLClient should call getErrorStream() to get response body on IOException.
- OPENAM-5082: DJLDAPv3Repo setAttributes may add unnecessary objectclasses to modifyRequest.
- OPENAM-5097: LDAP and AD auth modules should support startTLS extended operation
- OPENAM-5120: SAML2 SP in a sub-realm not fully functional after OPENAM-474
- OPENAM-5148: URL links in email sent from REST forgotPassword or register is not URLEncoded
- OPENAM-5183: CTS port settings are reverted to default when doing upgrade from AM 11 to AM 12
- OPENAM-5208: SAML2 SLO error on IDP with Session Synchronization when SP does not support SOAP binding
- OPENAM-5237: OAuth2 authorization consent page uses absolute URL in FORM tag
- OPENAM-5241: DN cache is never enabled since OPENAM-3822
- OPENAM-5252: DJLDAPv3Repo returns different error code when DN cache is enabled
- OPENAM-5260: When using HTTP-POST binding allow to only sign the Response
- OPENAM-5311: Default timelimit in Netscape SDK should be configurable
- OPENAM-5312: Initialization of a ServiceSchemaManager may block retrieval of already cached instances
- OPENAM-5317: 1st. character from realm value is deleted from endpoint /json/authenticate?realm=myRealm"
- OPENAM-5326: When using .well-known/openid-configuration?realm=/shop the iss/issuers does not match
- OPENAM-5332: OAuth2 RefreshTokenServerResource should check the clientID case insensitively
- OPENAM-5381: Specifying an external user store when using configurator tool is not being processed correctly
- OPENAM-5383: CTS Reaper fails if simple paged control is not present in response

- OPENAM-5386: Policy editor doesn't always use realm-specific REST endpoints
- OPENAM-5388: Missing policy actions after upgrading to OpenAM 12
- OPENAM-5411: OpenAM is filling the ResponseLocation with a null instead of an empty string
- OPENAM-5417: Policy Conditions of same type can not be combined in OpenAM 12
- OPENAM-5419: TokenExpired exception message is not consistent
- OPENAM-5421: TokenResource ignores query string passed from client
- OPENAM-5451: Resource based authentication does not work as expected in 12 (with legacy UI)
- OPENAM-5472: NPE in #setAttributes when IdRepo fails to read directory schema
- OPENAM-5488: Upgrade fails from OpenAM 11 to OpenAM 12 with NPE from OAuth2 client profile
- OPENAM-5508: REST with Realm/DNS Aliases causes unexpected results
- OPENAM-5578: Although OpenDJ is selected as default for external user data store LDAPv3ForODSEE type is used
- OPENAM-5598: Adaptive Risk auth module can not be used in auth chain if the username in sharedstate map does not 'match' the search attribute of the data store
- OPENAM-5621: OIDC .well-known/webfinger endpoint is reporting wrong href URL
- OPENAM-5623: CTS uses inefficient search for coreTokenId=
- OPENAM-5660: NPE when the keyalias does not exist or does not contain a certificate
- OPENAM-5690: Get an Access Token From SAML 2.0 on 12.0.0 uses grant type saml2-bearer, but TokenEndpoint is not defined in OAuth2Application

6.1.5. Key Fixes in OpenAM 12.0.0

The following bugs were fixed in OpenAM 12.0.0:

- OPENAM-4340: Configurator is unable to handle special characters in passwords
- OPENAM-4264: IDPAccountMapper.getNameID() does not receive the SP Entity ID if there is no SPNameQualifier in the SAML request
- OPENAM-4262: IDP Proxy should set destination depending on the Binding
- OPENAM-4236: CookieUtils.addCookieToResponse only sends Max-Age attribute
- OPENAM-4229: Change Password as User does not work using AD-LDS (ADAM) User Store
- OPENAM-4227: Set Password as Administrator does not work using AD-LDS (ADAM) User Store

- OPENAM-4094: OAuth2 Authentication Module does not work, if com.iplanet.am.cookie.encode is true.
- OPENAM-3969: 403 on using /json/<realm>/policies?_action=evaluate
- OPENAM-3822: Datastore authentication fails after modify DN operation.
- OPENAM-3758: OAuth2 save consent when no scope is present is not working
- OPENAM-3731: Sun JDK 1.6.0_43: some requests cause never-ending loop in SAML2Utils.decodeFromRedirect
- OPENAM-3964: The class hierarchy for `ResourceName` interfaces has changed in this issue. Previous implementations should still be source-compatible but are not binary-compatible. You must recompile your custom code if you implemented the `ResourceName` interfaces.
- OPENAM-3640: StackOverFlowError in WebtopNaming
- OPENAM-3573: IDP Initiated federation with missing SPNameQualifier result in exception
- OPENAM-3513: wrong l10n key in code, ssoadm delete-auth-instance fails on error reporting
- OPENAM-3437: RelayState validation fails during SLO
- OPENAM-3428: DJLDAPv3Repo breaks Active Directory when using sAMAccountName as naming attribute with the DN being the CN
- OPENAM-3385: DJLDAPv3Repo Error Unexpected Results Returned when searching Active Directory users from the root
- OPENAM-3314: Hosted IDPs/SPs in COTs with Spaces
- OPENAM-3271: OpenAM Bootstrap file not found for upgrade from 10.0.1 to 11.0.0 if both .openamcfg and .openssocfg exist
- OPENAM-3225: SAML authentication throws NPE with IDP metadata showing certain characteristics
- OPENAM-2532: deleting ActiveDirectory DataStore from subrealm deleting parent's referrals too.
- OPENAM-2464: HOTP auth module sends 2 HOTP codes, if "Request new code" is clicked.
- OPENAM-2322: NULL pointer exception in windowsdesktopsso.java file when doing kerberos service ticket authentication with Openssoclientsdk.jar client program - backward compatibility broken
- OPENAM-1829: .NET Fedlet - "Signature Transform" and "Canonicalization Method" should be configurable
- OPENAM-1789: .NET Fedlet creates SAML2 IDs with incorrect format

- OPENAM-1773: DAS does not handle goto whitelisting
- OPENAM-1755: The .NET fedlet uses invalid constants "True" "False" for some boolean XML attributes
- OPENAM-1749: AttributeQueryUtil.getAttributeMapForFedlet eats non-Success StatusCode from IDP
- OPENAM-1655: AttributeQueryUtil ignores configured SPAttributeMapper
- OPENAM-1058: Enhance to use attribute names defined in the HOTP service config for the telephone, carrier and email address.
- OPENAM-957: Null pointer exceptions in IDPSSOFederate.getAuthnRequest()
- OPENAM-474: Dynamic User Creation not populating all available attributes onto newly created user
- OPENAM-371: Remove frequently occurring meaningless Error stack trace from debug log
- OPENAM-294: ssoadm: create and update
- OPENAM-110: Attribute name comparison in AttributeQueryUtil.isSameAttribute()
- OPENAM-61: SAML2 appliesTo not being HTML character-encoded

6.2. Limitations

The following limitations and workarounds exist for each OpenAM 12 release:

6.2.1. Limitations in OpenAM 12.0.4

The following limitations and workarounds are for OpenAM 12.0.4:

No new limitations are attributed to this release.

6.2.2. Limitations in OpenAM 12.0.3

The following limitations and workarounds are for OpenAM 12.0.3:

No new limitations are attributed to this release.

6.2.3. Limitations in OpenAM 12.0.2

The following limitations and workarounds are for OpenAM 12.0.2:

- **Manually Update Required for Some Fixes**. The changes related to OPENAM-6468 and OPENAM-6499 are not handled automatically by upgrade, thus when upgrading OpenAM from 12.0.1 or from a version where the #201505-01 security patch has been applied, the Object Deserialisation Class Whitelist server setting needs to be updated manually with the following new entries:

```
com.sun.identity.common.configuration.ServerConfigXML
com.sun.identity.common.configuration.ServerConfigXML$DirUserObject
com.sun.identity.common.configuration.ServerConfigXML$ServerGroup
com.sun.identity.common.configuration.ServerConfigXML$ServerObject
java.security.cert.Certificate
java.security.cert.Certificate$CertificateRep
```

6.2.4. Limitations in OpenAM 12.0.1

The following limitations and workarounds are for OpenAM 12.0.1:

- **Different OpenAM Version Within a Site**. Do not run different versions of OpenAM together in the same OpenAM site.
- **Deleting Referral Policy**. OpenAM allows you to delete a referral policy even if policies depending on the referral still exist in the target realm. Deleting a referral policy that other policies depend on can cause problems during policy evaluation. You must therefore make sure that no policies depend on any referrals that you delete.
- **Avoid Use of Special Characters in Policy or Application Creation**. Do not use special characters within policy, application or referral names (for example, "my+referral") using the Policy Editor or REST endpoints as OpenAM returns a 400 Bad Request error. The special characters are: double quotes ("), plus sign (+), command (,), less than (<), equals (=), greater than (>), backslash (\), and null (\u0000). (OPENAM-5262)
- **Avoid Using REST Endpoint Names for Realm Names**. Do not use the names of OpenAM REST endpoints as the name of a realm. The OpenAM REST endpoint names that should not be used includes: `users`, `groups`, `realms`, `policies`, and `applications`. (OPENAM-5314)
- **Deploying OpenAM on Windows in an IPv6 Network**. When deploying OpenAM components on Microsoft Windows in an IPv6 environment, you must use the Java 7 Development Kit on Windows (due to JDK-6230761, which is fixed only in Java 7).
- **Database Repository Type is Experimental**. The Database Repository type of data store is experimental and not supported for production use.
- **Enforcing Session Quotas With Session Failover**. By default, OpenAM does not enforce session quotas when running in Site mode without session failover. To work around this behavior, set the server configuration property `openam.session.useLocalSessionsInMultiServerMode=true`. You can set this property in OpenAM console under Configuration > Servers and Sites > Servers > Server Name > Advanced.

- **OpenAM with Embedded Directory Server in IPv6 Networks**. On hosts with pure IPv6 networks, OpenAM configuration has been seen to fail while starting the embedded OpenDJ directory server (OPENAM-3008).

- **JBoss 6.3 Support for Java 8**. As of this writing, JBoss 6.3/AS 7.4.0 does not support Java 8. Until JBoss 6.3 fully supports Java 8, you can use JDK 1.7.0_56 (OPENAM-4876).

- **Note about HttpServletResponse And HttpServletRequest**. The `HttpServletRequest` instance passed to `AMPostAuthProcessInterface#onLogout` will be null. The `HttpServletResponse` instance passed to `AMPostAuthProcessInterface#onLogout` is not the actual `HttpServletResponse` corresponding to the request but a faux instance whose only purpose is to transfer headers back to the actual `HttpServletResponse` (OPENAM-4045).

- **XACML Policy Import and Export**. OpenAM can only import XACML 3.0 files that were either created by an OpenAM instance, or that have had minor manual modifications, due to the reuse of some XACML 3.0 parameters for non-standard information.

6.2.5. Limitations in OpenAM 12.0.0

The following limitations and workarounds are for OpenAM 12.0.0:

- **Different OpenAM Version within a Site**. Do not run different versions of OpenAM together in the same OpenAM site.

- **Deleting Referral Policy**. OpenAM allows you to delete a referral policy even if policies depending on the referral still exist in the target realm. Deleting a referral policy that other policies depend on can cause problems during policy evaluation. You must therefore make sure that no policies depend on any referrals that you delete.

- **Avoid Use of Special Characters in Policy or Application creation**. Do not use special characters within policy, application or referral names (for example, "my+referral") using the Policy Editor or REST endpoints as OpenAM returns a 400 Bad Request error. The special characters are: double quotes ("), plus sign (+), comma (,), less than (<), equals (=), greater than (>), backslash (\), and null (\u0000). (OPENAM-5262)

- **Avoid Using REST Endpoint Names for Realm Names**. Do not use the names of OpenAM REST endpoints as the name of a realm. The OpenAM REST endpoint names that should not be used includes: "users", "groups", "realms", "policies" and "applications". (OPENAM-5314)

- **Deploying OpenAM on Windows in an IPv6 Network**. When deploying OpenAM components on Microsoft Windows in an IPv6 environment, you must use the Java 7 Development Kit on Windows (due to JDK-6230761, which is fixed only in Java 7).

- **Database Repository Type is Experimental**. The Database Repository type of data store is experimental and not supported for production use.

- **Enforcing Session Quotas with Session Failover**. By default OpenAM does not enforce session quotas when running in Site mode without session failover. To work around this behavior, set the

server configuration property `openam.session.useLocalSessionsInMultiServerMode=true`. You can set this property in OpenAM console under Configuration > Servers and Sites > Servers > Server Name > Advanced.

- **OpenAM with Embedded Directory Server in IPv6 Networks**. On hosts with pure IPv6 networks, OpenAM configuration has been seen to fail while starting the embedded OpenDJ directory server (OPENAM-3008).
- **JBoss 6.3 Support for Java 8**. As of this writing, JBoss 6.3/AS 7.4.0 does not support Java 8. Until JBoss 6.3 fully supports Java 8, you can use JDK 1.7.0_56 (OPENAM-4876).
- **Note about HttpServletResponse & HttpServletRequest**. The `HttpServletRequest` instance passed to `AMPostAuthProcessInterface#onLogout` will be null. The `HttpServletResponse` instance passed to `AMPostAuthProcessInterface#onLogout` is not the actual `HttpServletResponse` corresponding to the request but a faux instance whose only purpose is to transfer headers back to the actual `HttpServletResponse` (OPENAM-4045).
- **XACML Policy Import and Export**. OpenAM can only import XACML 3.0 files that were either created by an OpenAM instance, or that have had minor manual modifications, due to the reuse of some XACML 3.0 parameters for non-standard information.

6.3. Known Issues

The following known issues exist for each OpenAM 12 release:

6.3.1. Known Issues in OpenAM 12.0.4

- **Login page does not load or ssoadm fails if OpenAM is running on Apache Tomcat 8.5 or 9.**

  If you accidently upgraded Apache Tomcat to version 8.5 or later (see the supported Tomcat version at "OpenAM Web Application Container Requirements"), you may experience issues with the login page or **ssoadm** failing.

  For a workaround, see /knowledge/kb/article/a73027813.

- OPENAM-9757: ssoadm does not work properly on websphere without additional setup
- OPENAM-8975: Unable to install AM 12.0.3 on Websphere 8.5
- OPENAM-8796: Some of LDAP User Attributes are missing after upgrade
- OPENAM-8633: Message changed for the failed password when authenticating over REST
- OPENAM-7781: persistent cookie auth module does not allow to change cookie name by default
- OPENAM-7746: Authentication in sub-realm fails if DNS alias is used and persistence can not be guaranteed

- OPENAM-7282: Forgotten password submit button is disabled when using autocomplete
- OPENAM-7035: OAuth2ProviderSettings are not updated if configuration of baseUrlSource service is changed
- OPENAM-6426: Forgot password doesn't print an audit log
- OPENAM-6262: Admin console generates incorrect goto URLs when behind reverse proxy
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN

6.3.2. Known Issues in OpenAM 12.0.3

- **Login page does not load or ssoadm fails if OpenAM is running on Apache Tomcat 8.5 or 9.**

  If you accidently upgraded Apache Tomcat to version 8.5 or later (see the supported Tomcat version at "OpenAM Web Application Container Requirements"), you may experience issues with the login page or **ssoadm** failing.

  For a workaround, see /knowledge/kb/article/a73027813.

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-774: Invalid characters check not performed.
- OPENAM-1068: In case of session upgrade the SAML IDPCache can lose the ssotoken sessionindex mapping
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1521: Cookie Hijacking Prevention does not work properly under FireFox
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-2028: java.lang.NullPointerException at com.sun.identity.saml2.common.SAML2Utils.getRemoteServiceURL

- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2155: Non printable characters in some files. Looks like most should be copyright 0xA9
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-2911: IdP initiated SSO with persistent identifier causes URLNotFoundException: Invalid service host name.
- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-3095: When a SP sends an unsigned Authn Request using SAML ECP OpenAM sees it as a wrong message
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3253: XUI: sunIdentityUserPassword not set in com.sun.identity.authentication.spi.ReplayPasswd
- OPENAM-3266: Heartbeat timeouts can occur during operation
- OPENAM-3381: SAML login is not handled correctly on the SP if the user already has a local session on the SP
- OPENAM-3442: CTS TokenType is missing an index
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3470: The SAML2 nameid should not be persisted if the nameid-format is not persistent
- OPENAM-3693: LDAP psearch uses DN to update the cache instead of valid Universal ID
- OPENAM-3698: Federation authentication module may be retrieved from the incorrect realm when running OpenAM as an SAML SP
- OPENAM-3762: sun-idrepo-ldapv3-config-memberurl doesn't exist for LDAPv3ForOpenDS
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3868: Regression: NPE in WDSSO module when authenticating via ClientSDK
- OPENAM-3924: XUI is ignoring iplanet-am-admin-console-password-reset-enabled and requesting user password be entered anytime password is changed

- OPENAM-4135: Authentication triggers a search that retrieves all attributes - IDRepo
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-4517: GUI installer crashes and restarts in Safari
- OPENAM-4754: NPE when SessionID doesn't contain StorageKey for SFO
- OPENAM-4765: AdminTokenAction - retrieving the admin token is not Synchronized
- OPENAM-4983: Commands for embedded DJ should use --noPropertiesFile switch
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5243: REST HTTP codes are different for some actions in AM 11.0.2 and AM 12
- OPENAM-5264: Can't login to OpenAM with no cookies set in the platform service
- OPENAM-5321: Cross realm session upgrade not handled properly by XUI
- OPENAM-5364: 11.0 format policies with "?" in the rule name cannot be edited by the Policy Editor
- OPENAM-5400: Policy Editor: Unable to edit/delete policy whose name ends in a '/' character
- OPENAM-5416: XUI not handling correctly response from REST services during authentication
- OPENAM-5467: XUI/#logout/ route ignores "goto" parameter
- OPENAM-5505: Setting openam-session-timeout-handler-list= in ssoadm set-attr-defs ends up creating a list with one empty item
- OPENAM-5530: OpenAM does not set the destination in the last leg of IDP Proxy SLO
- OPENAM-5541: Resource based auth doesn't work in sub realm
- OPENAM-5554: run-xacml-client-sample.sh packaged with ExampleClientSDK-CLI-12.0.0.zip is missing libraries
- OPENAM-5567: User attribute mapping sometimes fail
- OPENAM-5614: Jackson can not instantiate AuthnRequestInfoCopy/IDPSessionCopy from JSON object
- OPENAM-5626: XUI not redirecting to console when no datastore in top realm
- OPENAM-5670: Create Policy UI can't get the subject attributes if you don't have a datastore configured.
- OPENAM-5712: Cross-realm session upgrade with ForceAuth does not trigger #confirmLogin
- OPENAM-5721: WindowsDesktopSSO trusted realm list doesn't work

- OPENAM-5733: validationService doesn't work if the datastore isn't configured
- OPENAM-5744: Authentication level login doesn't work if the module name doesn't match the module type
- OPENAM-5834: Changes since OPENAM-2274 to DefaultLibrarySPAccountMapper has meant that NameID can't be used in some cases using auto federation
- OPENAM-5847: OAuth 2.0 Token Administration Endpoint should not allow to list all tokens as 'Super User'
- OPENAM-5883: SAML Time value should allow milliseconds values with less than 3 digits
- OPENAM-5894: Can't update WindowsDesktopSSO module with ssoadm
- OPENAM-5902: Persistent cookie fails on host cookies when domain deleted via console
- OPENAM-5917: IdP proxy in a subrealm is unable to send SLO response to the remote SP
- OPENAM-5920: Realm associated with OAuth2 tokens is not normalised
- OPENAM-5921: XUI Login page does not pass username to post auth plugin
- OPENAM-5980: CTS async queue can cause threads to wait for a long time
- OPENAM-5987: Database audit logging 'failure buffer' does not write all records after DB recovery
- OPENAM-6056: LoginViewBean does not correctly handle empty ChoiceCallbacks
- OPENAM-6156: orderedlist uitype in service config breaks when updated
- OPENAM-6192: For OAuth 2.0 don't expect the default Shared Consent Attribute to contain a value on first use
- OPENAM-6196: Exception With SAML 2.0 ECP IDP Profile (PAOS Binding)
- OPENAM-6235: NameID values that contain characters such as & cause parsing issues when used in XML documents.
- OPENAM-6244: In case of GeoIp2Exception in the adaptive module, only the score of the geolocation should be affected
- OPENAM-6262: Admin console generates incorrect goto URLs when behind reverse proxy
- OPENAM-6273: XUI self-service links are only available when data-store auth-module is used
- OPENAM-6318: IdP proxy should populate the AuthenticatingAuthority element in its Responses
- OPENAM-6362: HOTP and OATH auth-modules do not set 'failureUserID' when throwing InvalidPasswordException, this breaks OpenAM account lockout
- OPENAM-6372: Browser back button and OpenAM internal authentication error

- OPENAM-6374: Registering UMA resource sometimes gives error
- OPENAM-6376: OAuth2 resource owner authentication code does not pass headers to auth module
- OPENAM-6384: XUI: Sharing resource twice (with another user) fails
- OPENAM-6385: Revoking access to individual resource using XUI fails
- OPENAM-6423: Post Authentication Plugin can't set headers in the logout API on REST response
- OPENAM-6426: Forgot password doesn't print an audit log
- OPENAM-6443: Unable to change a user password using admin token via REST
- OPENAM-6457: DirectoryContentUpgrader causes Entry Already Exists exception for CTS suffix when upgrading OpenAM
- OPENAM-6471: Cannot Initialize Authentication exception when upgrading OpenAM
- OPENAM-6472: NPE when choosing No on new_org.jsp
- OPENAM-6476: Initialization of a ServiceConfigImpl may block retrieval of already cached instances
- OPENAM-6506: Potential NPE in OpenAMScopeValidator.evaluateScope
- OPENAM-6514: OAuth2 authorization flow stores resource owner in universalID format if persistent mode is on
- OPENAM-6552: access_token request sent by OAuth2Saml2GrantSPAdapter is not realm aware
- OPENAM-6553: Fix Social Authentication in subrealms
- OPENAM-6558: jwt-bearer grant type handler doesn't call additionalDataToReturnFromTokenEndpoint of the Scope Validator Plugin
- OPENAM-6620: jwks_uri generates a kid value different for each server in a site configuration
- OPENAM-6630: Policy Editor 'Export All Policies' does not specify realm
- OPENAM-6666: Re-shared resource that is revoked by resource owner, re-shared user still has access
- OPENAM-6726: Issues creating Agent client using REST API
- OPENAM-6734: Shutdown race condition between embedded OpenDJ and OpenAM persistent search restart
- OPENAM-6739: Creating UMA policy as amadmin doesn't show in user's resources
- OPENAM-6741: STS configuration not showing in admin console

- OPENAM-6776: SAML authentication can fail with NumberFormatException
- OPENAM-6798: Remove ORIG_URL after OAUTH2 Authentication complete
- OPENAM-6825: Fails to issue OAuth2 access token if client type confidential is inherited from group
- OPENAM-6842: PAP onLogout() method is not triggered in a multi-server environment, if the logout is invoked from the OpeAM instance in which session is not created.
- OPENAM-6867: changePassword REST endpoint is not returning LDAP issues that are related to a user mistake.
- OPENAM-6878: OpenAM forgot password search hard coded for UID
- OPENAM-6883: SystemConfigurationUtil maintains a list of server URLs that assume lowercase deployment contexts
- OPENAM-6976: OAuth2 Error Page on oauth2/authorize with valid params and cookie
- OPENAM-6977: Validate OIDC script returns "No privilege mapping for requested action validate"
- OPENAM-7002: The email attribute property defined in the email service is not used when sending e-mail in forgotten password flow
- OPENAM-7021: XUI login script queries "/openam/json/users?realm=/?_action=idFromSession"
- OPENAM-7035: OAuth2ProviderSettings are not updated if configuration of baseUrlSource service is changed
- OPENAM-7054: RADIUS Server Does not Start After Initial Install Without a Web Container Restart
- OPENAM-7070: Datastore screen error when loading schema if host list has entries with pipe
- OPENAM-7075: endSession endpoint can't kill SSO Token for some OAuth2 grant type
- OPENAM-7095: ssoadm do-batch doesn't continue if the -c flag is applied for the SAML delete-entity command
- OPENAM-7122: json/agents/?_action=create returns inconsistent error codes when an agent name already exists
- OPENAM-7255: XUI "Delete Label" is inactive for orphan labels
- OPENAM-7260: OAuth2 authorization flow sets wrong resource owner if alias name + LDAP auth is used.
- OPENAM-7265: Post Authentication Plugin HttpServletRequest is null in onLogout() method
- OPENAM-7282: Forgotten password submit button is disabled when using autocomplete

- OPENAM-7298: Custom response attributes are not visible in the policy editor UI and are erased when editing policies through the UI
- OPENAM-7321: Update scripting whitelist to allow use of CHF client in scripts
- OPENAM-7334: Client Authentication method not compliant with OpenID standard
- OPENAM-7382: HTTP GET to uma/auditHistory with param "sortKeys=-eventTime" returned 500 server error
- OPENAM-7467: Redirect loop with XUI and resource=true when user initially authenticated to different chain
- OPENAM-7547: OpenIdConnectAuthorizeRequestValidator doesn't take default scopes into account when checking.
- OPENAM-7549: Call to userinfo unexpectedly generates "WARNING: Couldn't find any helper support the HTTP_Bearer challenge scheme."
- OPENAM-7727: debugfiles.properties missing in ClientSDK jar
- OPENAM-7746: Authentication in sub-realm fails if DNS alias is used and persistence can not be guaranteed
- OPENAM-7781: persistent cookie auth module does not allow to change cookie name by default
- OPENAM-7785: 404 on <server:port>/openam
- OPENAM-7864: Failure to connect to syslog server can cause OpenAM to hang
- OPENAM-7939: Audit file retention "Minimum Free Space Required" field doesn't stop growing the occupied disk space
- OPENAM-7966: hiddenValueBox not showed in DAS
- OPENAM-8058: ForgeRock Authenticator settings cannot be changed when in production
- OPENAM-8074: Changing an user password with the same value returns 400 with ldap errorcode=20
- OPENAM-8077: XUI does not overwrite stateless session on session upgrade
- OPENAM-8091: OpenAM cannot connect to a DataStore which accepts only TLSv1.2
- OPENAM-8108: Radius auth module not usable in auth-chain with 'shared-state' enabled
- OPENAM-8111: User Self Service is active if configured however not turned on in the realm
- OPENAM-8125: IE 9/10: can't create policy resource
- OPENAM-8148: Adding new subject with Tivoli as datastore missing kbaInfoContainer schema

- OPENAM-8174: OpenAM gives an Internal Server Error when the user tries to reset their password before the minimum password age
- OPENAM-8180: Custom auth breaks after upgrade due to lack of "resourceName"
- OPENAM-8204: XUI does not display proper error message when changing password
- OPENAM-8225: Reading binary attributes, for example objectGUID, from the IdRepo cache not always returning valid values
- OPENAM-8237: jaxrpc-impl-1.1.3_01-041406.jar and webservices-rt-2009-29-07.jar contain the same classes
- OPENAM-8282: Password Reset questions are not randomly chosen when resetting password
- OPENAM-8327: Unable to send e-mail via Google SMTP with SSL enabled
- OPENAM-8633: Message changed for the failed password when authenticating over REST
- OPENAM-8796: Some of LDAP User Attributes are missing after upgrade

6.3.3. Known Issues in OpenAM 12.0.2

- **Login page does not load or ssoadm fails if OpenAM is running on Apache Tomcat 8.5 or 9.**

  If you accidently upgraded Apache Tomcat to version 8.5 or later (see the supported Tomcat version at "OpenAM Web Application Container Requirements"), you may experience issues with the login page or **ssoadm** failing.

  For a workaround, see /knowledge/kb/article/a73027813.
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-480: Adding a server to a site requires restart of OpenAM
- OPENAM-774: Invalid characters check not performed.
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled
- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents

- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-2085: Unreliable policy evaluation results with com.sun.identity.agents.config.fetch.from.root.resource enabled
- OPENAM-2155: Non printable characters in some files. Looks like most should be copyright 0xA9
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- OPENAM-2469: IdP initiated SSO endpoints should honor RelayState even when they're POSTed
- OPENAM-2537: SAML AuthContext mapper auth level setting inconsistencies
- OPENAM-2564: resource-based authentication with DistAuth not working
- OPENAM-2608: Restricted Token validation does not work in legacy REST API
- OPENAM-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-3056: Retrieving roles may fail when using more than one data store
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3442: CTS TokenType is missing an index

- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3924: XUI is ignoring iplanet-am-admin-console-password-reset-enabled and requesting user password be entered anytime password is changed
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-4517: GUI installer crashes and restarts in Safari
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5243: REST HTTP codes are different for some actions in AM 11.0.2 and AM 12
- OPENAM-5321: Cross realm session upgrade not handled properly by XUI
- OPENAM-6056: LoginViewBean does not correctly handle empty ChoiceCallbacks
- OPENAM-6319: OAuth2 scopes behaviour affected by the upgrade
- OPENAM-6340: XUI needs to support DNS/Alias behaviour for subrealms as per OPENAM-5508
- OPENAM-6565: .well-known/openid-configuration is published with both DNS Realm alias AND realm in the path, resulting in failed authentication

6.3.4. Known Issues in OpenAM 12.0.1

- **Login page does not load or ssoadm fails if OpenAM is running on Apache Tomcat 8.5 or 9.**

  If you accidently upgraded Apache Tomcat to version 8.5 or later (see the supported Tomcat version at "OpenAM Web Application Container Requirements"), you may experience issues with the login page or **ssoadm** failing.

  For a workaround, see /knowledge/kb/article/a73027813.

The following important known issues remained open at the time release OpenAM 12.0.1 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-774: Invalid characters check not performed.
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled

- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-2085: Unreliable policy evaluation results with com.sun.identity.agents.config.fetch.from.root.resource enabled
- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2155: Non printable characters in some files. Looks like most should be copyright 0xA9
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- OPENAM-2469: IdP initiated SSO endpoints should honor RelayState even when they're POSTed
- OPENAM-2537: SAML AuthContext mapper auth level setting inconsistencies
- OPENAM-2564: resource-based authentication with DistAuth not working
- OPENAM-2608: Restricted Token validation does not work in legacy REST API
- OPENAM-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI

- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-3056: Retrieving roles may fail when using more than one data store
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3442: CTS TokenType is missing an index
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3924: XUI is ignoring iplanet-am-admin-console-password-reset-enabled and requesting user password be entered anytime password is changed
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-4517: GUI installer crashes and restarts in Safari
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5243: REST HTTP codes are different for some actions in AM 11.0.2 and AM 12
- OPENAM-5321: Cross realm session upgrade not handled properly by XUI
- OPENAM-6056: LoginViewBean does not correctly handle empty ChoiceCallbacks
- OPENAM-6302: Upgrade incorrectly sets default value for the REST APIs service
- OPENAM-6319: OAuth2 scopes behaviour affected by the upgrade

6.3.5. Known Issues in OpenAM 12.0.0

- **Login page does not load or ssoadm fails if OpenAM is running on Apache Tomcat 8.5 or 9.**

  If you accidently upgraded Apache Tomcat to version 8.5 or later (see the supported Tomcat version at "OpenAM Web Application Container Requirements"), you may experience issues with the login page or **ssoadm** failing.

  For a workaround, see /knowledge/kb/article/a73027813.

The following important known issues remained open at the time release OpenAM 12.0.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-5321: Cross realm session upgrade not handled properly by XUI
- OPENAM-5243: REST HTTP codes are different for some actions in AM 11.0.2 and AM 12
- OPENAM-5237: OAuth2 authorization consent page uses absolute URL in FORM tag
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5183: CTS port settings are reverted to default when doing upgrade from AM 11 to AM 12
- OPENAM-4517: GUI installer crashes and restarts in Safari
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-3924: XUI is ignoring iplanet-am-admin-console-password-reset-enabled and requesting user password be entered anytime password is changed
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3442: CTS TokenType is missing an index
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3056: Retrieving roles may fail when using more than one data store
- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-2705: People container name/value configs are not always correctly used - backport
- OPENAM-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- OPENAM-2608: Restricted Token validation does not work in legacy REST API
- OPENAM-2564: resource-based authentication with DistAuth not working
- OPENAM-2537: SAML AuthContext mapper auth level setting inconsistencies
- OPENAM-2469: IdP initiated SSO endpoints should honor RelayState even when they're POSTed
- OPENAM-2453: HTTP GET /ws/1/entitlement/privilege? HTTP 400 with message "Unable to search privileges."
- OPENAM-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0

- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2085: Unreliable policy evaluation results with com.sun.identity.agents.config.fetch.from.root.resource enabled
- OPENAM-2023: Federation Connectivity Test fails with Account termination is not working
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1852: Oauth2 auth-module can not be used with DistAuth
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1811: DAS response serialization is not working as expected when using PAP
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1456: Change of the agent group in the J2EE policy agent profile causes profile corruption
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents
- OPENAM-1269: Entitlements are incorrectly converted to policies
- OPENAM-1237: Property 'noSubjectKeyIdentifier' is missing in fmWSSecurity.properties
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled
- OPENAM-1105: Init properties sometimes don't honor final settings

- OPENAM-774: Invalid characters check not performed.
- OPENAM-291: SelfWrite permissions are denied to sub realms
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings

Chapter 7
Documentation Updates

The following table tracks changes to the documentation set following the release of OpenAM 12:

Documentation Change Log

Date	Description
2018-06-08	Added a warning about enabling the `org.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH`. For more information, see "Preparing Apache Tomcat" in the *Installation Guide*.
2017-12-11	• Revised and clarified deprecated JSP endpoints in the Release Notes for OpenAM 12.0.0. See "Deprecated Functionality".
2016-12-05	• Revised and clarified "Administering the amadmin Account" in the *Administration Guide*. • Removed the .NET Fedlet section from the documentation. For more information, see "Important Changes to Existing Functionality in OpenAM 12.0.4".
2016-11-16	• Revised and clarified "To Set up Administration Tools" in the *Installation Guide*. • Corrected the description of the Mobile Carrier Attribute Name in "Hints for the HOTP Authentication Module" in the *Administration Guide*. • Removed the incorrect statement that the REST Security Token Service is compatible with the WS-Trust 1.4 specification.
2016-09-26	• Maintenance release of OpenAM 12.0.4.
2016-08-25	• Clarified which web containers are supported for deploying the Distributed Authentcation `.war` file in "*Installing OpenAM Distributed Authentication*" in the *Installation Guide*.
2016-07-15	• Corrected the description of the Auto Federation Attribute property in "Hints for Assertion Processing" in the *Administration Guide*. • Added a warning not to allow `Content-Type` headers to CORS filters to "Enabling CORS Support" in the *Installation Guide*. • Added the new `org.forgerock.openam.redirecturlvalidator.maxUrlLength` property to "Servers and Sites Configuration" in the *Reference*. • The procedure to turn off user data caching has a new step to disable persistent search. See "To Turn Off Global User Data Caching" in the *Administration Guide*.

Date	Description
2016-04-20	• The descriptions of the Relay State URL List property in "Configuring Identity Providers" in the *Administration Guide* and "Configuring Service Providers" in the *Administration Guide* have been corrected. • "To Customize Files You Copied" in the *Installation Guide* has been corrected to reflect the changes that occur to the French login page after customization.
2016-04-05	"Hints for the Active Directory Authentication Module" in the *Administration Guide* and "Hints for the LDAP Authentication Module" in the *Administration Guide* has been updated with the property `openam-auth-ldap-operation-timeout`.
2016-03-10	Reorganization of 12.0.x docs, combining 12.0.0, 12.0.1, 12.0.2 release notes
2015-10-15	Maintenance release of OpenAM 12.0.2, which includes a new security advisories section.
2015-07-15	Maintenance release of OpenAM 12.0.1, which include security advisories.
2013-12-15	Initial release of OpenAM 12.0.0.

Chapter 8
Support

You can purchase OpenAM support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see http://forgerock.com/partners/find-a-partner/.

Chapter 9

How to Report Problems & Provide Feedback

If you have questions regarding OpenAM which are not answered by the documentation, there is a mailing list which can be found at https://lists.forgerock.org/mailman/listinfo/openam where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenAM 12, report them in https://bugster.forgerock.org.

When requesting help with a problem, include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:
  - Machine type
  - Operating system and version
  - Web server or container and version
  - Java version
  - OpenAM version
  - Any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps