# Release Notes

ForgeRock Access Management 5

ForgeRock AS
201 Mission St, Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

## Abstract

Notes covering new features, fixes and known issues in ForgeRock# Access Management. ForgeRock Access Management provides authentication, authorization, entitlement, and federation software.

# Table of Contents

# Preface

Read these release notes before you install ForgeRock Access Management or update your existing installation.

The information contained in these release notes cover prerequisites for installation, known issues and improvements to the software, changes and deprecated functionality, and other important information.

## About ForgeRock Identity Platform™ Software

ForgeRock Identity Platform™ is the only offering for access management, identity management, user-managed access, directory services, and an identity gateway, designed and built as a single, unified platform.

The platform includes the following components that extend what is available in open source projects to provide fully featured, enterprise-ready software:

- ForgeRock Access Management (AM)
- ForgeRock Identity Management (IDM)
- ForgeRock Directory Services (DS)
- ForgeRock Identity Gateway (IG)

Chapter 1
# What's New

This chapter covers the new features and improvements done in the current release of ForgeRock Access Management.

## 1.1. Major New Features in ForgeRock Access Management 5

ForgeRock Access Management 5 is a major release that introduces new features, functional enhancements, and fixes.

This release introduces the following product enhancements:

### 1.1.1. Cloud

- **Autonomous AM Servers**

  AM 5 servers are considered to be *autonomous*—they operate independently of one another. The concept of a home server—the server to which a user originally authenticated—is no longer applicable. User requests can be satisfied by any server in a cluster.

  Two architectural changes in AM 5 enable autonomous servers:

  - The authoritative source for sessions is now the Core Token Service (CTS) token store. Sessions are also cached in the memory heap of the server on which the user authenticated as a performance optimization. Previously, the authoritative source for sessions was in the memory heap of the user's home server.

    Prior to this release, the memory heap of the user's home server was the authoritative source for the session, and the CTS token store held a backup copy of the session that was used in the event of home server failure.

  - In versions prior to this release, cross-server session validation, or *session crosstalk*, described one OpenAM server making an HTTP request to another server in a clustered deployment.

    The removal of session crosstalk calls allows AM servers to manage sessions independently of one another, with less awareness of the context within which they run.

    All configuration settings related to session crosstalk have been removed.

- **Session High Availability Enabled by Default**

Session high availability, formerly referred to as session failover, is now enabled by default for all AM deployments. No configuration is required during installation to enable session high availability, and it cannot be disabled.

All configuration settings related to session high availability have been removed.

- **CTS Session Affinity Capability**

  AM can now connect to multiple master directory server instances, with each instance acting as the master for a subset of CTS tokens. In this architecture, CTS tokens are described as having an *affinity* for a given directory server instance.

  Versions prior to this release required the CTS token store to be deployed in an active/passive architecture, which limits AM's connection to the CTS token store to a single master instance with failover instances. In this release, the CTS token store can still be deployed in an active/passive architecture.

  For more information about CTS token affinity, see Section 3.1, "General Recommendations for CTS Configuration" in the *Installation Guide*.

### 1.1.2. DevOps

- **Amster Command-line Interface Tool**

  Amster is a command-line interface built upon the AM REST interface. Use Amster in DevOps processes, such as continuous integration, command-line installations, and scripted cloud deployments.

  For more information, see the Amster documentation.

- **Heartbeat Monitoring to External Configuration Store**

  AM now provides a heartbeat interval of ten seconds (default) to the configuration store. You can override the default settings by setting the JVM startup properties:

  - **org.forgerock.openam.ldap.sm.heartbeat.interval**. Sets the heartbeat interval. The default interval is ten seconds. If you set the JVM property to 0, it will disable the heartbeat.
  - **org.forgerock.openam.ldap.sm.heartbeat.unit**. Sets the time unit of the heartbeat interval. Default is `SECONDS`. Possible values also include: `DAYS`, `HOURS`, `MICROSECONDS`, `MILLISECONDS`, `MINUTES`, `NANOSECONDS`, and `SECONDS`.

  For more information, see Section 1.4.3, "Setting the Configuration Store Heartbeat" in the *Installation Guide*.

- **Bootstrap AM from Environment Variables**

AM can now be bootstrapped from environment variables or Java properties, overriding the `boot.json` file created during installation. See Section 2.4.1, "Overriding Startup Settings" in the *Installation Guide* for more information.

Previous releases could only be bootstrapped from the `bootstrap` file.

### 1.1.3. Stack Integration

- **Directory Services 5**

  AM now includes an embedded version of the latest Directory Services product (5), which you can use as the embedded data store, configuration store, token store, UMA resource set store, and UMA history store.

  You should be aware of the changes to the LDAP command-line tools for Directory Services 4.0. For information, see Important Changes to Existing Functionality.

- **New Splunk Audit Event Handler**

  AM can now log audit events to a Splunk platform. For more information, see Section 6.2.2.7, "Implementing Splunk Audit Event Handlers" in the *Setup and Maintenance Guide*.

### 1.1.4. Developer-Friendly

**API Explorer**

AM now provides an online AM REST API reference that can be accessed through the AM console. The API provides useful reference information for developers to create client applications to access AM's services.

You can access the API Explorer from the AM console by logging in as an administrator and pointing your browser to:

```
https://openam.example.com:8080/openam/XUI/#api/explorer/applications
```

You can also click the help icon in the top right corner, and then click API Explorer.

### 1.1.5. Security

- **New Stateless/OpenID Connect Encryption Modes**

  AM now provides additional encryption algorithms and encryption methods for stateless sessions and OpenID Connect ID tokens. This release also supports new compression features for stateless sessions.

  - **New Encryption Algorithms**

    The following encryption algorithms are supported:

- **RSA1_5**. RSA with PKCS#1 v1.5 padding
- **RSA-OAEP**. RSA with OAEP padding and SHA-1
- **RSA-OAEP-256**. RSA with OAEP padding and SHA-256
- **A128KW**. AES key wrap using 128-bit key
- **A192KW**. AES key wrap using 192-bit key
- **A256KW**. AES key wrap using 256-bit key
- **dir**. Direct encryption with a shared symmetric key

The following padding modes are supported: `RSA1_5`, `RSA-OAEP`, and `RSA-OAEP-256`. You can set the one of these values using the advanced setting: `org.forgerock.openam.session.stateless.rsa.padding`.

For more information, see Section 2.8, "Encrypting OpenID Connect ID Tokens" in the *OpenID Connect 1.0 Guide*.

- **New Encryption Modes**

  The following encryption methods are supported:

  - **A128CBC-HS256**. AES 128-bit in CBC mode using HMAC-SHA-256-128 hash (HS256 truncated to 128 bits)
  - **A192CBC-HS384**. AES 192-bit in CBC mode using HMAC-SHA-384-192 hash (HS384 truncated to 192 bits)
  - **A256CBC-HS512**. AES 256-bit in CBC mode using HMAC-SHA-512-256 hash (HS512 truncated to 256 bits)
  - **A128GCM**. AES 128-bit in GCM mode
  - **A192GCM**. AES 192-bit in GCM mode
  - **A256GCM**. AES 256-bit in GCM mode

  To set another encryption method from those listed above, you can set the method using the advanced property `org.forgerock.openam.session.stateless.encryption.method` in the AM console.

  For more information, see Section 6.1.3.2, "Configuring JWT Encryption" in the *Authentication and Single Sign-On Guide*.

- **DEFLATE Compression**

  AM now supports a compression option for stateless sessions. This feature does not apply to OpenID Connect ID tokens.

  **Warning**

  When set to `DEF` (deflate compression), this option leads to possible vulnerability with session state information leakage. Because the session token compression depends on the data in the session, an attacker can vary one part of the session (for example, the username or some other property) and then

deduce some secret parts of the session state by examining how the session compresses. Users should evaluate this threat depending on their use cases before enabling compression and encryption together.

For more information, see Section 6.1.3.2, "Configuring JWT Encryption" in the *Authentication and Single Sign-On Guide*.

- **Added OAuth 2.0 Proof-of-Possession Support**

  AM now supports use the proof-of-possession support when using OAuth 2.0 access tokens to ensure that the presenter of a bearer token was issued the access token originally.

  AM supports proof-of-possession keys for both stateful and stateless OAuth 2.0 tokens.

  For more information, see Section 3.1.1, "Using OAuth 2.0 JSON Web Token Proof-of-Possession" in the *OAuth 2.0 Guide*.

- **AES Wrap Encryption Support**

  AM now supports the Advanced Encryption Standard (AES) Key Wrap algorithm (RFC3394), implementing the Password-Based Key Derivation Function 2 (PBKDF2) (RFC2898). Administrators can choose the key size hash algorithms, such as SHA1, SHA256, SHA384, or SHA512.

  **Important**

  The AES Wrap Encryption algorithm is only enabled when installing OpenAM. There is no current upgrade path for existing installations.

  Several AM components, such as agents and the SOAP Security Token Service, require JCE encryption and decryption. Because a web container cannot be configured to support both JCE and AES Key Wrap encryption, you must make sure not to deploy any AM components that require JCE encryption on servers that run on web containers configured for AES Key Wrap encryption.

  For more information, see Section 1.2.6, "Preparing AES Wrap Encryption" in the *Installation Guide*.

- **OAuth 2.0 Token Endpoint Authentication Signing Algorithm Added**

  The new property Token Endpoint Authentication Signing Algorithm has been added to the OAuth 2.0 / OpenID Connect client to specify the JWS algorithm that must be used for signing JWTs used to authenticate the client at the Token Endpoint.

  For more information, see Section 5.4, "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OpenID Connect 1.0 Guide*.

- **OAuth 2.0 Mix-Up Mitigation Support**

  - The new Mix-Up Mitigation (`openam-auth-oauth-mix-up-mitigation-enabled`) property has been added to the OAuth 2.0 authentication module. This property protects the deployment for identity provider (IdP) Mix-Up attacks during an OAuth 2.0 authorization code flow, running additional verification steps when receiving the authorization code from the authorization server.

Due to this new setting, the field Name of OpenID Connect ID Token Issuer in the OAuth 2.0 / OpenID Connect authentication module has been renamed to Token Issuer. The authorization code response can contain an issuer value (`iss`) that is validated by the client. When the module is an OAuth2-only module (that is, OIDC is not used), the issuer value needs to be explicitly set in the Token Issuer property, so that the validation can succeed.

For more information, see Section 11.2.19, "OAuth 2.0/OpenID Connect Authentication Module Properties" in the *Authentication and Single Sign-On Guide* and Section 11.2.19.1, "OAuth 2.0 Mix-Up Mitigation" in the *Authentication and Single Sign-On Guide*.

- The new property OAuth 2.0 Mix-up Mitigation enabled has been added to the OAuth 2.0 / OpenID Connect client. Enable this property only if the client supports mix-up mitigation.

  For more information, see Section 5.4, "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OpenID Connect 1.0 Guide*.

- **Added Support for Signing and Encryption of Responses on the `UserInfo` OIDC Endpoint**

  AM 5 now supports signing and encrypting `UserInfo` responses as per the OIDC spec.

  Properties have been added to the OAuth 2.0 / OpenID Connect client for signing and encrypting the contents of the `UserInfo` response.

  For more information, see the OIDC spec.

  For more information, see Section 5.4, "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OpenID Connect 1.0 Guide*.

### 1.1.6. Documentation

- **Reorganization**

  AM now has reorganized documentation. Concise, topic-based guides replace the larger guides available for previous releases.

  Administrator tasks, developer tasks, and reference information now appear in a single guide per topic. For example, the OAuth 2.0 Guide contains information about working with OAuth 2.0 that was formerly spread across the *OpenAM Administration Guide*, the *OpenAM Developer's Guide*, and the *OpenAM Reference*.

## 1.2. Improvements in ForgeRock Access Management 5

The following improvements and additional features were added in this release:

- **OpenJDK Support**

OpenJDK 8 is now a supported JDK for OpenAM deployments.

- **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.

  For more information, see Section A.5, "Authentication and Logout" in the *Authentication and Single Sign-On Guide*.

- **The Default WS-Federation and SAML v2.0 IdP Attribute Mapper now Support Base64-encoded Binary Values for NameID**

  OpenAM now lets you add a `;binary` flag to a NameID Value Map attribute to indicate that it will be Base64-encoded before being added to the assertion. The mapping may resemble the following:

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

- **Realm DNS Alias Management Improved**

  Editing the list of DNS aliases for a realm in the AM console now also applies appropriate changes to the advanced default server property `com.sun.identity.server.fqdnMap`.

  For more information, see Procedure 2.2, "To Configure DNS Aliases for Accessing a Realm" in the *Setup and Maintenance Guide*.

- **New 503 Error Page When CTS Store is Disconnected**

  AM now displays a new 503 error status page when the store used for CTS data is not available. Previously the XUI remained available to users, even though functionality would not work as expected.

  Like other XUI pages, you can customize the 503 error page using the theme system. For more information, see the UI Customization Guide.

- **New OAuth 2.0 / OpenID Connect client JWKS URI Content Cache Timeouts**

  The JWKS content is cached to avoid loading URI content every time a token is encrypted or requires signature verification. AM 5 adds two new properties to the OAuth 2.0 / OpenID Connect client to define a timeout for the encryption and signature verification caches. See Section 5.4, "OAuth 2.0 and OpenID Connect 1.0 Client Settings" in the *OpenID Connect 1.0 Guide*.

## 1.3. Security Advisories

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/

Chapter 2

# Before You Install

This chapter covers software and hardware prerequisites for installing and running ForgeRock Access Management 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.*

## 2.1. Files to Download

Access Management software is available at https://backstage.forgerock.com. Table 2.1, "Access Management Software" describes the files available for download.

*Table 2.1. Access Management Software*

| File | Description |
|---|---|
| `OpenAM-14.0.0.zip` | Cross-platform distribution including all software components.<br><br>For a list of the files in the .zip archive, see Section 1.3.1, "Obtaining Software" in the *Installation Guide*. |
| `OpenAM-14.0.0.war` | Deployable web application archive file.<br><br>This file is identical to the `OpenAM-14.0.0.war` file, found in `OpenAM-14.0.0.zip`. |
| `SSOAdminTools-14.0.0.zip` | The .zip file that contains tools to manage OpenAM from the command line.<br><br>This file is identical to the `SSOAdminTools-14.0.0.zip` file, found in `OpenAM-14.0.0.zip`. |
| `SSOConfiguratorTools-14.0.0.zip` | The .zip file that contains tools to configure OpenAM from the command line.<br><br>This file is identical to the `SSOConfiguratorTools-14.0.0.zip` file, found in `OpenAM-14.0.0.zip`. |

The platform version number that appears in the download file names may differ from the internal version number. The internal version number for this release is ${softwareVersion}.

## 2.2. Operating System Requirements

ForgeRock supports customers using ForgeRock Access Management server software on the following operating system versions:

*Table 2.2. Supported Operating Systems*

| Operating System | Version |
|---|---|
| Red Hat Enterprise Linux, Centos, Amazon Linux | 6, 7 |
| Amazon Linux | Amazon Linux 2016.09 |
| SuSE | 11 |
| Ubuntu | 14.04 LTS, 16.04 LTS |
| Solaris x64 | 10, 11 |
| Solaris Sparc | 10, 11 |
| Windows Server | 2012, 2012 R2, 2016 |

## 2.3. Java Requirements

*Table 2.3. JDK Requirements*

| Vendor | Version |
|---|---|
| Oracle JDK | 7, 8 |
| IBM SDK, Java Technology Edition (Websphere only) | 7 |
| OpenJDK | 8 |

**Important**

Support for Oracle JDK 7 and IBM SDK 7 will be removed in a future version.

## 2.4. Web Application Container Requirements

*Table 2.4. Web Containers*

| Web Container | Version |
|---|---|
| Apache Tomcat | 7, 8, 8.5 |
| Oracle WebLogic Server | 12c |
| JBoss Enterprise Application Platform | 7.0 |

| Web Container | Version |
|---|---|
| WildFly AS | 9, 10, 10.1 |
| IBM WebSphere | 8.5.5.8+ |

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

## 2.5. Data Store Requirements

*Table 2.5. Supported Data Stores*

| Data Store | Version | CTS Datastore | Config Datastore | User Datastore | UMA Datastore |
|---|---|---|---|---|---|
| Embedded OpenDJ | 4.0 | ✓ | ✓ | ✓ | ✓ |
| External OpenDJ | 2.6, 2.6.4 | | | ✓ | |
| | 3.0, 3.5, 4.0 | ✓ | ✓ | ✓ | ✓ |
| Oracle Unified Directory | 11g | | | ✓ | |
| Oracle Directory Server Enterprise Edition | 11g | | | ✓ | |
| Microsoft Active Directory | 2012, 2012 R2, 2016 | | | ✓ | |
| IBM Tivoli Directory Server | 6.3 | | | ✓ | |

# 2.6. Supported Clients

The following table summarizes supported clients and their minimum required versions:

*Table 2.6. Supported Clients*

| Client Platform | Native Apps[a] | Chrome 33+ | Internet Explorer 9+ [b] | Edge 0.1+ | Firefox 28+ | Safari 6.2+ | Mobile Safari |
|---|---|---|---|---|---|---|---|
| Windows 7 or later | ✓ | ✓ | ✓ | ✓ | ✓ | | |
| Mac OS X 10.8 or later | ✓ | ✓ | | | ✓ | ✓ | |
| Ubuntu 12.04 LTS or later | ✓ | ✓ | | | ✓ | | |
| iOS 7 or later | ✓ | ✓ | | | | | ✓ |
| Android 4.3 or later | ✓ | ✓ | | | | | |

[a] *Native Apps* is a placeholder to indicate OpenAM is not just a browser-based technology product. An example of a native app would be something written to use our REST APIs, such as the sample OAuth 2.0 Token Demo app.
[b] Internet Explorer 9 is the minimum required for end users. For the administration console, Internet Explorer 11 is required.

# 2.7. Supported Upgrade Paths

The following table contains information about the supported upgrade paths to AM 5:

*Table 2.7. Upgrade Paths*

| Version | Upgrade Supported? |
|---|---|
| OpenAM 9.0.x | No |
| OpenAM 9.5.x | No |
| OpenAM 10.0.x | No |
| OpenAM 11.0.x | No |
| OpenAM 12.0.x | Yes |
| OpenAM 13.x.x | Yes |
| Access Management 5 | Yes [a] |

[a]
[a] **Caution**
Access Management is incompatible with SSO session tokens from OpenAM.
Storage and processing of SSO tokens changed in AM 5, meaning both stateful and stateless SSO sessions created in earlier versions of OpenAM are not supported.

After upgrading from an earlier version, any existing SSO tokens created by that version will become invalid, and users will need to re-authenticate.
In mixed version deployments, earlier versions of OpenAM will not be able to read or process SSO session tokens created by AM 5 or later.
This incompatibility only affects SSO session tokens. OAuth 2.0 and OpenID Connect 1.0 tokens are interoperable between versions.
If your pre-AM 5 deployment relies on long-lived SSO session tokens, and re-authenticating your users will be problematic, raise a ForgeRock Support issue for more information and assistance regarding upgrading to AM 5 or later.

**Note**

Upgrading between Enterprise and OEM versions is not supported.

For more information, see Checking your product versions are supported in the *ForgeRock Knowledge Base*.

## 2.8. Special Requests

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

Chapter 3
# Installing or Upgrading

This chapter covers installing and upgrading AM 5 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 4

# Changes and Deprecated Functionality

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

## 4.1. Important Changes to Existing Functionality

This section lists changes done to existing functionality, services, endpoints, and others in the current release of OpenAM.

**Caution**

Access Management is incompatible with SSO session tokens from OpenAM.

Storage and processing of SSO tokens changed in AM 5, meaning both stateful and stateless SSO sessions created in earlier versions of OpenAM are not supported.

After upgrading from an earlier version, any existing SSO tokens created by that version will become invalid, and users will need to re-authenticate.

In mixed version deployments, earlier versions of OpenAM will not be able to read or process SSO session tokens created by AM 5 or later.

This incompatibility only affects SSO session tokens. OAuth 2.0 and OpenID Connect 1.0 tokens are interoperable between versions.

If your pre-AM 5 deployment relies on long-lived SSO session tokens, and re-authenticating your users will be problematic, raise a ForgeRock Support issue for more information and assistance regarding upgrading to AM 5 or later.

### 4.1.1. Important Changes in ForgeRock Access Management 5

- **Methods for Specifying Realms in REST and XUI URLs Changed**

  The methods for specifying the realm to target when using the REST API or making requests to the XUI have been altered.

  Realm paths must be absolute and include the top-level realm, and DNS aliases and realms specified in the query string are no longer concatenated if used together – the query string overrides the DNS alias.

For information on specifying realms in XUI URLs, see Section 8.1.1.1, "Specifying the Realm in the Login URL" in the *Authentication and Single Sign-On Guide*.

For information on specifying realms in REST API URLs, see Section A.4, "Specifying Realms in REST API Calls" in the *Authentication and Single Sign-On Guide*.

- **Upgraded Instances Will Use XUI User Interface**

  This version only supports the XUI user interface. Upgrading an instance will force use of the XUI, even if the upgraded instance had disabled it.

  The option to disable the XUI has also been removed in this release.

  For more information, see UI Customization Guide.

- **Stateless Post-Authentication Plugins**

  Releases prior to AM 5 implemented the Keep Authentication Module Objects for Logout Processing option in the Core Authentication module. When this option was enabled, OpenAM maintained state information in server memory throughout a session's duration for post authentication plugin module instances. When logout was triggered, OpenAM invoked the same post authentication plugin module instance with state information intact. Therefore, developers could access module state stored at login when users logged out.

  In AM 5, post authentication plugin modules can not hold state as module state is never maintained in an OpenAM server's memory. Post authentication plugins that relied on module state being maintained in OpenAM's memory between login and logout must be rewritten. You can store any information that you want to save between login and logout in a session property. OpenAM stores session properties in the CTS token store after login, and retrieves them from the token store as part of the logout process.

  The Keep Authentication Module Objects for Logout Processing option in the Core Authentication module has been removed from AM 5.

- **Two Default Post-Authentication Plugin Classes Renamed**

  The following default post authentication plugin classes have been renamed:

  - The default class for the Adaptive Risk post authentication plugin, `org.forgerock.openam.authentication.modules.adaptive.Adaptive`, has been renamed to `org.forgerock.openam.authentication.modules.adaptive.AdaptivePostAuthenticationPlugin`.
  - The default class for the Persistent Cookie post authentication plugin, `org.forgerock.openam.authentication.modules.persistentcookie.PersistentCookieAuthModule`, has been renamed to `org.forgerock.openam.authentication.modules.persistentcookie.PersistentCookieAuthModulePostAuthenticationPlugin`.

  Upgrading to AM 5 automatically converts these two post authentication plugin class names if they are defined in authentication chain properties and in Core Authentication module properties. If you

have specified the old class names anywhere else in OpenAM, you must update to the new class names manually.

- **Server Memory Configuration Changes**

  In previous releases of OpenAM, stateful sessions were always stored in OpenAM server memory. They were also optionally written to the CTS token store when OpenAM was configured for session failover.

  In AM 5, the CTS token store is now the authoritative source for stateful sessions. Sessions can also be cached in AM server memory for performance.

  The server property `com.iplanet.am.session.maxSessions`, which formerly specified the maximum number of sessions that could be held concurrently in AM server memory (including RADIUS client sessions), has been removed from AM 5. The maximum number of sessions that can be stored in the CTS token store is unconstrained.

  You can use either or both of the following two new properties if needed:

  `org.forgerock.openam.session.service.access.persistence.caching.maxsize`

  Specifies the maximum number of sessions to cache in the OpenAM server's internal session cache. The default is 5,000 sessions.

  `org.forgerock.openam.radius.server.context.cache.size`

  Specifies the number of RADIUS clients that can be cached concurrently on an OpenAM server. The default is 5,000 clients.

- **CTS Reaper Cache**

  When an AM server modifies a token in the CTS store, it also takes the responsibility to delete it when it expires. To reduce the number of relatively slow queries to the CTS store to determine which tokens have expired, each AM server maintains a local cache of which tokens to delete, and when.

  The new `org.forgerock.services.cts.reaper.cache.size` advanced property controls the size of the cache.

  For more information, see Section 3.5, "CTS Tuning Considerations" in the *Installation Guide*.

  As part of these CTS tuning changes, the following properties have been removed from OpenAM:

  - `com.sun.identity.session.repository.cleanupRunPeriod`
  - `com.sun.identity.session.repository.healthCheckRunPeriod`
  - `org.forgerock.services.datalayer.connection.timeout.cts.reaper`

- **Entity Tag Virtual Attribute**

To tune the CTS data store for a slight boost in throughput, you can disable the default virtual attributes, except for the Entity Tag virtual attribute, which is required.

- **Bootstrap File Change**

  The name and format of the file used to bootstrap OpenAM has been changed. The JSON file, `boot.json`, replaces the `bootstrap` file.

- **Federation Navigation Link Replaced**

  The Federation link in the AM console's top navigation bar has been removed.

  - Configure SAML 2.0 and SAML 1.0 federation components navigating to Realms > *`Realm Name`* > Applications > SAML.
  - Configure WS-Federation federation components navigating to Realms > *`Realm Name`* > Applications > WS-Fed.

- **Some CTS OIDs Now Use the Custom `Float2dp` Data Type**

  The following CTS OIDs now use the new, custom `Float2dp` data type:

  - enterprises.36733.1.2.3.3.1.2.*
  - enterprises.36733.1.2.3.3.1.6.*
  - enterprises.36733.1.2.3.4.1.2.*.*
  - enterprises.36733.1.2.3.6.0
  - enterprises.36733.1.2.3.7.1.2.0
  - enterprises.36733.1.2.3.7.2.2.0

  The `Float2dp` data type is a floating point number with the value `d-2` in the `DISPLAY-HINT` clause. SNMP clients that handle the `DISPLAY-HINT` clause will correctly display the value as a floating point number with two decimal places. Other types of clients that do not handle the `DISPLAY-HINT` clause will incorrectly display the value as an integer that is one hundred times larger than the correct value.

  All other CTS OIDs use the `Counter64` data type, a standard data type returned by SNMP OIDs.

  For more information, see Section 7.1, "Core Token Service (CTS) Object Identifiers" in the *Installation Guide*.

- **.NET Fedlet Documentation Moved**

  The .NET Fedlet documentation is now a ForgeRock Knowledge Base article available to ForgeRock customers.

- **Sessions Navigation Link Replaced**

  The Sessions link in the AM console's top navigation bar has been removed.

  A new XUI Sessions page is available in Realms > *`Realm Name`* > Sessions, and its functionality has changed as follows:

- The session management is now by realm instead of showing all users in all realms.
- Only one user can be managed at a time; wildcards are not available.

- **Change for OAuth 2.0 Mix-Up Mitigation**

  For the OAuth 2.0 authentication module, a new property `openam-auth-oauth-mix-up-mitigation-enabled` has been added, which lets the OAuth 2.0 for Mix-Up Mitigation feature to protect the deployment for identity provider (IdP) Mix-Up attacks during an OAuth 2.0 authorization code flow. This property will run additional verification steps when receiving the authorization code from the authorization server.

  On the AM console, the field Name of OpenID Connect ID Token Issuer has been changed to: Token Issuer. The authorization code response can contain an issuer value (`iss`) that is validated by the client. When the module is an OAuth2-only module (that is, OIDC is not used), the issuer value needs to be explicitly set in the Token Issuer property, so that the validation can succeed.

- **Push Authentication Level Attribute for Push Authentication Module Renamed**

  The authentication level attribute, `forgerock-am-auth-push-auth-level`, for the push authentication module has been renamed to `forgerock-am-auth-authenticatorpush-auth-level`.

- **Support for HttpOnly**

  HttpOnly support has been updated with the following features:

  - The `/json/authenticate` endpoint returns a `Set-Cookie` header upon successful authentication in addition to the original token in the payload.
  - Session upgrade automatically occurs upon the current SSO token when the `/json/authenticate` endpoint is called and the token was previously passed in.
  - Upon logout, the session cookie on the client is cleared by the `Set-Cookie` header in the response.
  - User self-service auto login feature (user registration now returns a `Set-Cookie` in the response.
  - When an invalid token is detected when calling the `/json/authenticate` is ignored and authentication continues. An additional `Set-Cookie` header is set to remove the invalid cookie from the client.
  - AM's XUI does not directly manipulate tokens, such as `iPlanetDirectoryPro`.

  For more information, see Section 7.1.1, "Configuring HttpOnly" in the *Authentication and Single Sign-On Guide*.

- **REST "sessionresource" Endpoint Changed**

  Starting with this release, the `sessionresource` endpoint no longer supports the `queryId=server` and `queryId=list` options.

The `queryId=all` option has also changed. The number of returned records is limited by the token store maximum page size. For example, a Directory Services 5 store has a a limit of 4000 records by default. Queries that would return more records than the limit will return no records, and an error.

You should use version 2 of the endpoint, which supports fine-grained querying to limit the number of session records returned from the token store.

- **The "Idtokeninfo endpoint requires client authentication" Option Now Applies to All Signing Algorithms**

  Starting with this release, if the "Idtokeninfo endpoint requires client authentication" option is enabled, all requests to the `/oauth2/idtokeninfo` endpoint must be authenticated, not just those that use HMAC-based signing.

  For more information, see Section 5.3, "OAuth2 Provider" in the *OpenID Connect 1.0 Guide*.

- **Support for External OpenDJ 2.6 Data Stores Reduced**

  OpenDJ 3.0 or later is now required for external configuration, UMA, and CTS data stores.

  For more information, see Section 2.5, "Data Store Requirements".

# 4.2. Deprecated Functionality

Functionality listed under this section has been deprecated in 5 or earlier and will be removed in a future release of OpenAM.

## 4.2.1. Deprecated in ForgeRock Access Management 5

- **Realm Aliases Deprecated**

  The use of realm aliases is deprecated in this release.

  DNS aliases remain unaffected.

  For information on aliases, see Chapter 2, "*Setting Up Realms*" in the *Setup and Maintenance Guide*.

- **Classic Logging Service Deprecated**

  The classic logging service is deprecated in this release.

  For information on the replacement audit logging service, see Section 6.1, "Introducing the Audit Logging Service" in the *Setup and Maintenance Guide*.

- **User-Managed Access v1.0 and v1.0.1 Deprecated**

Support for UMA 1.0 and UMA 1.0.1 will be removed in a future version of ForgeRock Access Management. Features and functionality will be upgraded to support upcoming UMA standards.

For more information on deprecation, see Appendix A, "*Release Levels and Interface Stability*".

- **The `ssoadm.jsp` Page Is Deprecated**
- **Deprecated REST APIs**

  The following table lists deprecated REST APIs and their newer equivalents:

*Table 4.1. Deprecated and New REST APIs*

| Deprecated APIs | Newer APIs |
|---|---|
| **Realm REST Endpoint** [a] | |
| /json/realms | /json/global-service/realms |
| **OAuth 2.0 Revoke Token Endpoint** [b] | |
| /frrest/oauth2/token | /oauth2/token |
| **Session Information APIs** [c] | |
| /json/sessions/?_action=getTimeLeft<br>/json/sessions/?_action=getMaxSessionTime<br>/json/sessions/?_action=getMaxIdle<br>/json/sessions/?_action=getIdle | /json/sessions/?_action=getSessionInfo |
| /json/sessions/?_action=isActive&refresh=true | /json/sessions/?_action=refresh |
| /json/sessions/?_action=getPropertyNames | /json/sessions/?_action=getSessionProperties |
| /json/sessions/?_action=setProperty | /json/sessions/?_action=updateSessionProperties |

[a] For more information about the new realm APIs, see Section 2.3.2, "Realm Management" in the *Setup and Maintenance Guide*.
[b] For more information about revoking OAuth 2.0 tokens, see Section 3.4, "OAuth 2.0 Token Administration Endpoint" in the *OAuth 2.0 Guide*.
[c] For more information about the new session information APIs, see Chapter 9, "*Using Sessions*" in the *Authentication and Single Sign-On Guide*.

- **HTTP Client Get() and Post() Scripting Methods Deprecated**

  The HTTP client methods `get()` and `post()` used when making HTTP calls from within scripts are deprecated. Use the `send()` method in their place.

  For more information, see Section 5.2.1, "Accessing HTTP Services" in the *Development Guide*.

- **JDK 7 Support Deprecated**

Support for Oracle JDK 7 and IBM SDK 7 will be removed in the next 5.5 release of ForgeRock Access Management.

When upgrading to the current release, also move to JDK 8 in order to be prepared for pending removal of support for JDK 7.

- **OAuth2Saml2GrantSPAdapter Adapter Class Deprecated**

  The `org.forgerock.openam.oauth2.saml2.core.OAuth2Saml2GrantSPAdapter` adapter class used in service provider configurations to POST assertions to OAuth 2.0 authorization services will be removed in a future version of ForgeRock Access Management.

- **The ssoadm, ampassword, configurator.jar and upgrade.jar Tools Are Deprecated**

  Amster is replacing the **ssoadm** command and the `configurator.jar`, `upgrade.jar`, and `ampassword` tools, which will be removed in a future release of ForgeRock Access Management.

  For more information about Amster, see the Amster documentation.

- **Client SDK Deprecated**

  The client SDK will be removed and replaced in a future version of ForgeRock Access Management.

### 4.2.2. Deprecated in OpenAM 13 or OpenAM 13.5

- **The Classic JATO-Based UI Is Deprecated**

  The classic JATO-based UI is deprecated for the end-user pages and replaced in OpenAM with the JavaScript-based XUI as a replacement. The classic UI for end user pages is likely to be removed in a future release.

- **Listing Tokens With the `/frrest/oauth2/token/?_queryId` Method is Deprecated**

  Improved `_queryFilter` support will be added to replace the `_queryId` method.

- **The Device Print Service Is Deprecated**

  For information on replacement device identification features, see Section 2.2.6, "Device ID (Match) Authentication Module" in the *Authentication and Single Sign-On Guide*.

- **OpenAM Logging and User Self Service Are Deprecated**

  The OpenAM Logging, User Self Service, and Password Reset Services are deprecated. The User Self Service has been renamed to Legacy User Self Service.

- **Deprecated REST APIs**

  The following table lists deprecated REST APIs and their newer equivalents:

*Table 4.2. Deprecated and New REST APIs*

| Deprecated APIs | Newer APIs |
|---|---|
| **Session Information APIs** [a] | |
| /json/sessions/?_action=getMaxTime | /json/sessions/?_action=getTimeLeft |
| **User Self-Service and Password Reset APIs** [b] | |
| /json/users/_action=register | /json/selfservice/userRegistration |
| /json/users/?_action=confirm | /json/selfservice/userRegistration |
| /json/users/?_action=anonymousCreate | /json/selfservice/userRegistration |
| /json/users/?_action=forgotPassword | /json/selfservice/forgottenPassword |
| /json/users/?_action=forgotPasswordReset | /json/selfservice/forgottenPassword |

[a] For more information about the new session information APIs, see Section 9.1, "Obtaining Information About Sessions" in the *Authentication and Single Sign-On Guide*.

[b] For more information about the new user self-service APIs, see Section 3.1, "RESTful User Self Service" in the *User Self Service Guide*.

# 4.3. Removed Functionality

Functionality listed under this section has been removed from the actual OpenAM release.

## 4.3.1. Removed Functionality in ForgeRock Access Management 5

- **Server Configuration Properties Removed**

  The following server configuration properties have been removed from OpenAM:

  - `com.iplanet.am.session.purgedelay`
  - `com.iplanet.am.session.maxSessions`
  - `com.sun.am.event.connection.idle.timeout`
  - `openam.session.useLocalSessionsInMultiServerMode`

- **Session Service Secondary Configuration Settings Removed**

  With the removal of crosstalk between OpenAM servers, the settings in Session Service secondary configuration are no longer needed. As a result, the ability to add a secondary configuration instance to the global Session Service has been removed from OpenAM.

- **Session Trimming Setting Removed**

With the removal of the session purge delay from OpenAM, there is no longer a need to trim sessions being held for purge delay. Therefore, the Session Service's session trimming property is also being removed from OpenAM.

- **Keep Authentication Module Objects For Logout Processing Option Removed**

  This option, formerly a property of the Core Authentication Service, is no longer available in OpenAM.

- **Specifying Session Listeners On All Removed**

  Schema attribute `iplanet-am-session-add-session-listener-on-all-sessions` has been removed. The `AddSessionListenerOnAllSessions` is a PLL call that allows you to specify a URL to be notified when changes occur, such as logout. It was found that this setting only applied to sessions that the current server was aware of and would not persist after a server restart.

  Existing user stores may still have the schema attribute. Leaving the attribute in the user stores does not cause any issues. If you want to update your directory schema, you can remove this schema attribute.

  For example, if you are using a Directory Services 5 data store, you can update the schema attribute as follows:

```
$ ldapsearch -p 1389 -b cn=schema -s base "(&)" \+ | \
 grep 2.16.840.1.113730.3.1.1070
 attributeTypes: ( 2.16.840.1.113730.3.1.1070 \
  NAME 'iplanet-am-session-add-session-listener-on-all-sessions' DESC 'an example' \
  SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications \
  X-SCHEMA-FILE '99-user.ldif' )

$ ldapmodify -p 1389 -D "cn=Directory Manager" -w password
 dn: cn=schema
 changetype: modify
 delete: attributeTypes
 attributeTypes: ( 2.16.840.1.113730.3.1.1070 NAME \
 'iplanet-am-session-add-session-listener-on-all-sessions' DESC 'An example' \
 SYNTAX 1.3.6.1.4.1.1466.115.121.1.15 USAGE userApplications \
 X-SCHEMA-FILE '99-user.ldif' )
 Processing MODIFY request for cn=schema
  MODIFY operation successful for DN cn=schema
```

  For more information, see AME-11448.

- **`ssoadm` Policy Commands Removed**

  The following policy commands have been removed from the **ssoadm** command:

*Table 4.3. Policy Import and Export with ssoadm*

| Removed Command | New Command |
|---|---|
| `create-policies` | `create-xacml` |

| Removed Command | New Command |
|---|---|
| `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*.

- **Safari for Windows No Longer Supported as Client Browser**

  For more information about supported clients, see Section 2.6, "Supported Clients".

- **Liberty ID-FF Global Configuration Removed**

  Support for Liberty Identity Framework was deprecated in a previous version of AM.

Chapter 5

# Fixes, Limitations, and Known Issues

This chapter covers the status of key issues and limitations at release 5.

## 5.1. Key Fixes

The following issues were fixed in the current release. For details, see the OpenAM issue tracker.

### 5.1.1. Key Fixes in ForgeRock Access Management 5

The following important issues were fixed in this release:

- OPENAM-2346: RFE: OAuth2 Resouce Owner Password Grant should support service and module auth parameters
- OPENAM-2632: RFE: The identity/authorize REST API should be able to consume an OAuth2 access token
- OPENAM-5114: User should be able to rename or clone an existing Application containing policies without first deleting the policies
- OPENAM-5802: Import of policies should import application and resource type information as well
- OPENAM-5969: Allowing RequesterID chain when using SAML2 Idp Proxy
- OPENAM-6360: Send notifications for sessions even when the authoritative server is down
- OPENAM-8078: Develop a REST endpoint that returns all sessions for a user
- OPENAM-8210: Enhance CTS to persist tokens across multiple OpenDJ instances rather than a single primary OpenDJ instance by some form of sharding
- OPENAM-8560: CTS should use replace rather than delete/add for single valued attributes
- OPENAM-8581: JSON REST authenticate should return 401 for session timed out error
- OPENAM-8627: Provide support for more XML signatures types in .NET fedlet
- OPENAM-8772: Soap STS application token should retry if an operation failed
- OPENAM-8790: Better error message when resource owner auth failed with grant_type=password

- OPENAM-8836: Realm alias in XUI Admin Console should be reflected in fqdnMap
- OPENAM-8983: introspect endpoint shouldn't be limited to the same client as token
- OPENAM-9234: Add health check for the SOAP STS
- OPENAM-9366: Install.log doesn't contain timestamps, which block performance issue investigation
- OPENAM-9454: Allow the .NET Fedlet to be serialized and stored in session state
- OPENAM-9460: Include SOAP STS WAR in OpenAM Distribution Zip
- OPENAM-9536: Reduce size of stateless sessions
- OPENAM-9555: Persistent Cookie should set username in shared state
- OPENAM-10144: Add introspection endpoint in .well_known discovery
- OPENAM-10207: Authorize sending both HTTP Basic Auth credentials and client_id if client secret is not defined
- OPENAM-10316: Remove error from Maven build on openam-ui-ria for Windows
- OPENAM-10388: Allow message from auth module to be returned when resource owner auth failed with grant_type=password
- OPENAM-10429: oauth2/authorize consent page (authorize.json) should take locale headers into account
- OPENAM-10444: FMSessionProvider should adhere to setCookieToAllDomains setting
- OPENAM-10570: Add support for the SAML2_CONFIG component in FedletConfigurationImpl

## 5.2. Limitations

The following limitations and workarounds apply to AM 5:

- **JCEKS Keystore Support for User Self-Services**

  In OpenAM 13.0.0, the user self-service feature is stateless, which means that the end-user is tracked and replayed by an encrypted and signed JWT token on each AM instance. It also generates key pairs and caches its keys locally on the server instance.

  In a multi-instance deployment behind a load balancer, one server instance with the user self-services enabled will not be able to decrypt the JWT token from the other instance due to the encryption keys being stored locally to its server.

  OpenAM 13.5.0 and newer solve this issue by providing a JCEKS keystore that supports asymmetric keys for encryption and symmetric keys for signing. Users who have installed OpenAM 13.0.0 and enabled the user self-service feature will need to run additional steps to configure a JCEKS keystore to get the user self-service feature operating after an upgrade.

For specific instructions to configure the JCEKS keystore, see Section 2.1, "Configuring the Signing and Encryption Key Aliases" in the *User Self Service Guide*.

**Note**

This procedure is not necessary for the following users:

- Users upgrading from versions prior to OpenAM 13.0.0 are not impacted.
- Users who upgrade from OpenAM 13.0.0 and do not enable the user self-services feature are not impacted.
- Users who do a clean install of OpenAM 13.5.0 or newer are not impacted.

- **Cached JavaScript Files from OpenAM 12.0.0 May Cause Redirect to undefined:8080**

  If you configure an OpenAM 12.0.0 instance with long-lived cache times for the `/XUI/index.html` file, you may experience unexpected redirects to `undefined:8080` after upgrading.

  To work around this issue, in your chosen web container, or proxy server, reconfigure the cache time for the `/XUI/index.html` file to be short-lived, for example, 5 minutes. Allow enough time that cached files with the long-lived cache time will have expired before upgrading.

  **Note**

  This issue does not affect upgrades from OpenAM 12.0.1 or later. OpenAM 12.0.1 and later set a short-lived `cache-control` header on UI files to work around the problem of having stale files cached locally.

- **RADIUS Service Only Supports Commons Audit Logging**. The new RADIUS service only supports the new Commons Audit Logging, available in this release. The RADIUS service cannot use the older Logging Service, available in releases prior to OpenAM 13.0.0.

- **Administration Console Access Requires the `RealmAdmin` privilege**

  In this version of AM, administrators can use the AM console as follows:

  - Delegated administrators with the `RealmAdmin` privilege can access full AM console functionality within the realms they can administer. In addition, delegated administrators in the Top Level Realm who have this privilege can access OpenAM's global configuration.
  - Administrators with lesser privileges, such as the `PolicyAdmin` privilege, can not access the AM administration console.
  - The top-level administrator, such as `amadmin`, has access to full AM console functionality in all realms and can access OpenAM's global configuration.

- **Do Not End Policy Names with a "/" Character**

Do not use a "/" character at the end of a policy name as it will cause OpenAM to not read, edit, or delete the policy.

After upgrade, users who have policies with a trailing slash "/" character at the end of a policy name should remove the slash (OPENAM-5400). ways:

To remove slashes in the policy names, remove them as recommended in: OPENAM-5187.

- **OAuth2 Scopes Behavior Affected by Upgrade**

  After an upgrade from OpenAM 12.0.x, OAuth v2.0 scope behavior uses a deprecated implementation class, `org.forgerock.openam.oauth2.provider.impl.ScopeImpl`.

  The workaround is to manually update the OAuth v2.0 providers to use the `org.forgerock.openam.oauth2.OpenAMScopeValidator`.

  For background information, see OPENAM-6319.

- **Different OpenAM Version Within a Site**

  Do not run different versions of OpenAM together in the same OpenAM site.

- **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)

- **Supported ID Token Algorithms and Methods not Updated After Upgrade**

  AM 14 adds additional algorithms and methods for encrypting ID tokens. Performing an upgrade from OpenAM 13.5 does not add these new values to the affected properties.

  After upgrade, navigate to *`Realm Name`* > Services > OAuth2 Provider > OpenID Connect, and manually update the ID Token Encryption Algorithms supported and ID Token Encryption Methods supported properties.

  For more information on the available algorithms and methods, see Section 2.8, "Encrypting OpenID Connect ID Tokens" in the *OpenID Connect 1.0 Guide*.

- **Database Repository Type is Experimental**

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

- **XACML Policy Import and Export**

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

- **Custom Profile Attributes Are Not Visible in the User Profile Only With the XUI**

  Custom profile attributes do not appear in the user profile when users log in to OpenAM using the XUI.

## 5.3. Known Issues

The following important known issues remained open at the time release 5 became available. For details and information on other issues, see the OpenAM issue tracker.

### 5.3.1. Known Issues in ForgeRock Access Management 5

The following important issues remained open when ForgeRock Access Management 5 became available:

- OPENAM-820: AMSetupServlet only checks for product bootstrap validity on initial load
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-4040: SSO failure between SPs in separate CoTs with same hosted IDP
- OPENAM-5984: The XUI is unhappy when the CORS filter is enabled
- OPENAM-7836: User Self Service forgottenPassword endpoint throws HTTP 500
- OPENAM-8336: XUI+REST authentication with chains must have sticky load balancing
- OPENAM-8396: Extend depth of the heartbeat used between OpenAM<>LDAP to check a baseDN beyond the root DSE
- OPENAM-8831: Accessing policy editor through a subrealm DNS alias displays the policies for that subrealm independently of the realm selected
- OPENAM-8862: ServiceProvider (SP) meta data import succeeds with incorrect encryption key size
- OPENAM-8886: "OpenID Connect default acr claim" is not implemented
- OPENAM-8977: Force the user to set the security questions
- OPENAM-9112: Audit logging outputs errors in debug log under high load
- OPENAM-9447: OAuth2 client has different default values for clean installation and upgraded AM from 13.0.0 to 13.5
- OPENAM-9756: RFE: Allow pagination on Identity endpoints
- OPENAM-9798: CTS Query element order should be optimised

- OPENAM-9808: Forgot Username self-service can return "username" that might not be the same as login "username"
- OPENAM-9938: REST API to delete all tokens of a user
- OPENAM-9980: add package com.iplanet.security to public API
- OPENAM-10088: Make the set of characters used to create code in OAuth2 Device flow configurable
- OPENAM-10394: RFE: Include goto URL in verification email sent during User Registration / Forgot Password flow
- OPENAM-10446: Need more Audit logging for OAuth2/OIDC/UMA request/response fields
- OPENAM-10467: RFC7662: oauth2/introspect OpenAM returns token_type not as Bearer
- OPENAM-10478: kids used by AM for signing are not accessible to developers implementing a remote JWKs URI for AM
- OPENAM-10481: Default JWKS_URI of an OpenID provider doesn't allow signing key rotation
- OPENAM-10562: Audit log 'Configuration' entries are not written when using external configuration store
- OPENAM-10578: Stateless access token doesn't contain the grant type
- OPENAM-10585: The "claims" Request Parameter from the openid standard isn't functional
- OPENAM-10613: Provide support for using multiple attributes from the assertion when looking up the user in the auto federation case
- OPENAM-10624: Support validation of arbitrary scheme goto URLs
- OPENAM-10717: Encryption algorithms and encryptions methods don't all work out of the box
- OPENAM-10735: Amster script does not work on Solaris SPARC 10
- OPENAM-10816: Amster - SAML2 Entity fails to import
- OPENAM-10869: SAML2 Authentication module return "Unable to link local user to remote user" ambiguous.
- OPENAM-10921: Provide ability to retrieve OAuth2 consent dates

# Chapter 6
# Documentation Updates

The following table tracks changes to the documentation set following the release of AM 5:

*Table 6.1. Documentation Change Log*

| Date | Description |
|---|---|
| 2016-01-15 | OpenAM's documentation set has been reorganized based on topic to better aid the reader. |
| 2017-04-03 | Initial release of ForgeRock# Access Management 5. |
| 2017-04-13 | Refreshed release notes. |
| 2017-04-19 | Restored missing Javadoc. |
| 2017-06-19 | Documentation refresh, containing the following documentation updates:<br>• Added the following release notes:<br>  • Added Support for Signing and Encryption of Responses on the UserInfo OIDC Endpoint<br>  • New OAuth 2.0 / OpenID Connect client JWKS URI Content Cache Timeouts<br>  • OAuth 2.0 Token Endpoint Authentication Signing Algorithm Added<br>• Updated the release note OAuth 2.0 Mix-Up Mitigation Support to add that there are new properties in the OAuth 2.0 / OpenID Connect client<br>• Added caution to the release notes and upgrade guide about upgrades from OpenAM invalidating SSO session tokens. |

# Appendix A. Release Levels and Interface Stability

This appendix includes ForgeRock definitions for product release levels and interface stability.

## A.1. ForgeRock Product Release Levels

ForgeRock defines Major, Minor, and Maintenance product release levels. The release level is reflected in the version number. The release level tells you what sort of compatibility changes to expect.

*Table A.1. Release Level Definitions*

| Release Label | Version Numbers | Characteristics |
|---|---|---|
| Major | Version: x[.0.0] (trailing 0s are optional) | • Bring major new features, minor features, and bug fixes<br>• Can include changes even to Stable interfaces<br>• Can remove previously Deprecated functionality, and in rare cases remove Evolving functionality that has not been explicitly Deprecated<br>• Include changes present in previous Minor and Maintenance releases |
| Minor | Version: x.y[.0] (trailing 0s are optional) | • Bring minor features, and bug fixes |

| Release Label | Version Numbers | Characteristics |
|---|---|---|
| | | • Can include backwards-compatible changes to Stable interfaces in the same Major release, and incompatible changes to Evolving interfaces<br>• Can remove previously Deprecated functionality<br>• Include changes present in previous Minor and Maintenance releases |
| Maintenance | Version: x.y.z | • Bring bug fixes<br>• Are intended to be fully compatible with previous versions from the same Minor release |

# A.2. ForgeRock Product Interface Stability

ForgeRock products support many protocols, APIs, GUIs, and command-line interfaces. Some of these interfaces are standard and very stable. Others offer new functionality that is continuing to evolve.

ForgeRock acknowledges that you invest in these interfaces, and therefore must know when and how ForgeRock expects them to change. For that reason, ForgeRock defines interface stability labels and uses these definitions in ForgeRock products.

*Table A.2. Interface Stability Definitions*

| Stability Label | Definition |
|---|---|
| Stable | This documented interface is expected to undergo backwards-compatible changes only for major releases. Changes may be announced at least one minor release before they take effect. |
| Evolving | This documented interface is continuing to evolve and so is expected to change, potentially in backwards-incompatible ways even in a minor release. Changes are documented at the time of product release.<br><br>While new protocols and APIs are still in the process of standardization, they are Evolving. This applies for example to recent Internet-Draft implementations, and also to newly developed functionality. |
| Deprecated | This interface is deprecated and likely to be removed in a future release. For previously stable interfaces, the change was likely announced in a previous release. Deprecated interfaces will be removed from ForgeRock products. |
| Removed | This interface was deprecated in a previous release and has now been removed from the product. |
| Internal/Undocumented | Internal and undocumented interfaces can change without notice. If you depend on one of these interfaces, contact ForgeRock support or email info@forgerock.com to discuss your needs. |

# Appendix B. Getting Support

For more information or resources about OpenAM and ForgeRock Support, see the following sections:

## B.1. Accessing Documentation Online

ForgeRock publishes comprehensive documentation online:

- The ForgeRock Knowledge Base offers a large and increasing number of up-to-date, practical articles that help you deploy and manage ForgeRock software.
- ForgeRock core documentation, such as this document, aims to be technically accurate and complete with respect to the software documented. It is visible to everyone and covers all product features and examples of how to use them.

Core documentation therefore follows a three-phase review process designed to eliminate errors:

- Product managers and software architects review project documentation design with respect to the readers' software lifecycle needs.
- Subject matter experts review proposed documentation changes for technical accuracy and completeness with respect to the corresponding software.
- Quality experts validate implemented documentation changes for technical accuracy, completeness in scope, and usability for the readership.

The review process helps to ensure that documentation published for a ForgeRock release is technically accurate and complete.

Fully reviewed, published core documentation is available at http://backstage.forgerock.com/. Use this documentation when working with a ForgeRock Identity Platform release.

## B.2. Joining the ForgeRock Community

Visit the Community resource center where you can find information about each project, download trial builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and find the source code for open source software.

## B.3. Getting Support and Contacting ForgeRock

ForgeRock provides support services, professional services, classes through ForgeRock University, and partner services to assist you in setting up and maintaining your deployments. For a general overview of these services, see https://www.forgerock.com.

ForgeRock has staff members around the globe who support our international customers and partners. For details, visit https://www.forgerock.com, or send an email to ForgeRock at info@forgerock.com.