Release Notes

/ OpenAM 13.5

Latest update: 13.5.2

ForgeRock AS
201 Mission St, Suite 2900
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

1. What's New 1
    1.1. New Features 1
    1.2. Major Improvements 6
    1.3. Security Advisories 11
2. Before You Install OpenAM Software 12
    2.1. OpenAM Operating System Requirements 12
    2.2. Java Requirements 12
    2.3. OpenAM Web Application Container Requirements 13
    2.4. Data Store Requirements 13
    2.5. Supported Clients 14
    2.6. Supported Upgrade Paths 14
    2.7. Special Requests 15
3. Installing or Upgrading 16
4. Changes and Deprecated Functionality 18
    4.1. Important Changes to Existing Functionality 18
    4.2. Deprecated Functionality 28
    4.3. Removed Functionality 29
5. Fixes, Limitations, and Known Issues 31
    5.1. Key Fixes 31
    5.2. Limitations 41
    5.3. Known Issues 42
6. How to Report Problems or Provide Feedback 44
7. Documentation Updates 45
8. Support 50

Chapter 1
What's New

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

1.1. New Features

OpenAM 13.5.2

- OpenAM 13.5.2 is a maintenance release that introduces functional improvements, changes, and fixes to OpenAM.

OpenAM 13.5.1

- OpenAM 13.5.1 is a maintenance release that introduces functional improvements, changes, and fixes to OpenAM.

> **Note**
>
> Licensing changes to the Berkeley DB Java Edition (JE) mean that there is now a single distribution for OEM and Enterprise customers, which is based on Berkeley DB JE. There is no longer a separate OEM version of the product.

OpenAM 13.5

- OpenAM 13.5 introduces the following product features and enhancements:
  - Smarter Security Features
  - OAuth v2.0/OpenID Connect 1.0 Enhancements
  - Performance Enhancements
  - User Experience Enhancements
  - Dev Ops Features

Smarter Security Features

- **Push Authentication for Passwordless Login and Easy Multi-Factor**

  OpenAM 13.5 introduces a new authentication option that uses push notifications alongside an updated ForgeRock Authenticator app.

  The ForgeRock Authenticator app can now respond to push notifications for multi-factor authentication, including a passwordless login mechanism.

  For more information, see "About Push Authentication" in the *Administration Guide*.

- **New Elliptic Curve Digital Signature Algorithms**. OpenAM 13.5 introduces Elliptic Curve Digital Signature Algorithm (ECDSA) support for signing OpenID Connect `id_tokens` and stateless session tokens.

  The following ECDSA algorithms are now supported:

  - ES256 - ECDSA using SHA-256 hashes and the NIST standard P-256 elliptic curve.
  - ES384 - ECDSA using SHA-384 hashes and NIST standard P-384 curve.
  - ES512 - ECDSA using SHA-512 hashes and NIST standard P-521 curve.

  You can generate public and private keys for these algorithms using **keytool**.

  For more information, see "Configuring Elliptic Curve Digital Signature Algorithms" in the *Administration Guide*.

- **Default JCEKS Keystore**. OpenAM now uses a JCEKS keystore as its default keystore. User self service requires two key aliases: one for signing and one for encryption. OpenAM's JCEKS keystore comes with two default test aliases that can be used for out-of-the-box configuration that should be used for demo purposes only.

  For upgrades to OpenAM 13.5, the keystore remains the same as previously configured. For example, if you had a JKS keystore configured, the keystore configuration remains as JKS after upgrade to OpenAM 13.5. You will need to reconfigure the keystore to JCEKS on OpenAM 13.5.

  For more information, see "Configuring the Signing and Encryption Key Aliases" in the *Administration Guide*.

- **New Trust Transaction Header System Property**. OpenAM supports the propagation of the transaction ID across the ForgeRock platform, such as from OpenDJ or OpenIDM to OpenAM, using the HTTP header `X-ForgeRock-TransactionId`.

  You can set a new property `org.forgerock.http.TrustTransactionHeader` to `true`, which will trust any incoming `X-ForgeRock-TransactionId` headers. By default, the `org.forgerock.http.TrustTransactionHeader`

is set to `false`, so that a malicious actor cannot flood the system with requests using the same transaction ID header to hide their tracks.

For more information, see "Configuring the Trust Transaction Header System Property" in the *Administration Guide*.

OAuth v2.0/OpenID Connect 1.0 Enhancements

OpenAM 13.5 introduces a number of enhancements for its OAuth 2.0 and OpenID Connect 1.0 components:

- **New Stateless `idtokeninfo` Endpoint for OIDC Token Validation**

  OpenAM 13.5 now supports a new `/oauth2/idtokeninfo` endpoint for OpenID Connect 1.0 (OIDC) `id_token` validation. The feature allows clients to offload validation of an OIDC token to the endpoint and to retrieve the claims contained within the `id_token` directly without accessing the datastore.

  For more information, see "Endpoint for Validating OpenID Connect 1.0 ID Tokens" in the *Developer's Guide*.

- **OAuth v2.0 Stateless Token Blacklisting**

  OpenAM 13.5 now supports stateless OAuth v2.0 token blacklisting.

  For more information, see "Configuring Stateless OAuth 2.0 Token Blacklisting" in the *Administration Guide*.

- **Stateless OAuth 2.0 Access and Refresh Tokens**

  OpenAM 13.5 now supports stateless OAuth 2.0 access and refresh tokens that can be quickly validated

  For more information, see "Stateless OpenID Connect 1.0 Access and Refresh Tokens" in the *Administration Guide*.

- **New Field in OAuth2/OIDC Agent Settings: `com.forgerock.openam.oauth2provider.jwks`.**

  OpenAM 13.5 has been updated with a new field in the OAuth v2.0/OIDC agent setting to specify a static JWKSet value: `com.forgerock.openam.oauth2provider.jwks`.

  This setting will allow the Public Key Selector to accept `JWKS` rather than `JWKs_URL`.

  For more information, see "Configuring OAuth 2.0 and OpenID Connect 1.0 Clients" in the *Administration Guide*.

- **OpenID Connect ID Token Encryption**

OpenAM 13.5 now supports the ability to encrypt OIDC ID tokens. Administrators can now enable encryption in the OpenAM console.

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

- **Expose OAuth v2.0 Access/Refresh Token Signing Public Key via HTTP**

  OpenAM 13.5 supports the ability for an application to obtain the public key used to digitally sign the access and refresh tokens from OpenAM via HTTP.

  Applications can use the `/oauth2/connect/jwk_uri` endpoint to obtain the public key to sign the access and refresh tokens from OpenAM. The application can then validate an OAuth v2.0 stateless token without contacting OpenAM.

  For more information, see "To Obtain the OAuth 2.0/OpenID Connect 1.0 Public Signing Key" in the *Administration Guide*.

- **OAuth 2.0 User Consent Page Can Be Optional**

  OpenAM 13.5 can now make the OAuth 2.0 user consent page optional. You can set this up by configuring two new settings:

  - On the OAuth2 Provider settings, enable the `Allow clients to skip consent` option.
  - On the OAuth 2.0 Client (agent) settings, enable `Implied consent`.

  When both settings are configured, OpenAM treats the requests as if the client has already saved consent and will suppress any user consent pages to the client.

  For more information, see "Allowing Clients To Skip Consent" in the *Administration Guide*.

- **New `csrf` Parameter Requied 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" \
       "https://openam.example.com:443/openam/oauth2/authorize?response_type=code&client_id=myClient"\
       "&realm=/&scope=profile&redirect_uri=http://www.example.net"
```

Performance Enhancements

OpenAM 13.5 has made a number of fixes that improves OpenAM's performance. Some of the fixes are as follows:

- **Option to Generate or Disable Sign Out Tokens**

  OpenAM 13.5 now provides a `Store Ops Token` option to generate and store a sign out token in the CTS store for an OIDC provider.

  When the property is disabled, OAuth 2.0 performance may be improved by not storing the sign out tokens in the CTS store.

  For more information, see "OAuth2 Provider" in the *Reference*.

- **Same Calls to /oauth2/authorize and /oauth2/access_token Endpoints Optimized**

  OpenAM 13.5 has optimized the sequence to generate an /oauth2/OIDC token (for example, SSO login, oauth2/authorize, access_token with authz code).

- **CTS Uses Replace Instead Of Delete/Add for Single Valued Attributes**

  OpenAM 13.5 now uses LDIF `replace` instead of a `delete/add` combination for single valued attributes in OpenDJ. This feature improves performance, requiring less processing in OpenDJ.

User Experience Enhancements

- **Continued Migration of JATO Objects to XUI**

  In OpenAM 13.5, the Services and Global configuration screens in the OpenAM console have migrated to the new XUI interface.

Dev Ops Features

- **New Policy Export/Import ssoadm Command**

  OpenAM 13.5 has enhanced its **ssoadm** command to support policy export and import to JSON.

  For more information, see "To Export Policies in JSON Format (Command Line)" in the *Administration Guide*.

Platform Enhancements

- **New Elasticsearch and JMS Audit Event Handlers**

  Enhancements to the ForgeRock Common Audit Framework allow OpenAM 13.5 to log user and administrative activity to Elasticsearch and JMS.

For more information about the Elasticsearch audit event handler, see "Implementing Elasticsearch Audit Event Handlers" in the *Administration Guide*.

For more information about the JMS audit event handler, see "Configuring JMS Audit Event Handlers" in the *Administration Guide*.

1.2. Major Improvements

OpenAM 13.5.2

- **New OAuth 2.0 Stateless Access Token Claim**

  OpenAM adds a new OAuth 2.0 stateless access token claim, `"grant_type"`.

  - **"grant_type"**. The `"grant_type"` claim indicates the type of authorization flow that the user has completed. This information is useful for the resource server to make decisions based on both the scopes and the grant type of the user.

- **Allow Custom Audiences in SAML Assertions**

  OpenAM now allows you to add a custom Audience URI to the SAML assertion `<AudienceRestrictions>` element. You can do so by manually adding the new `audienceUri` parameter to the Extended SP Metadata and

- **Configurable Failure Retry Attempts for OTP Authentication Modules**

  OpenAM now provides a configuration option to set the number of failed retry attempts for HMAC-based One-Time Password (HOTP), ForgeRock Authenticator, and Oath modules. The default is 3 failure attempts. The minimum number is 1 and the maximum number of retries is 10.

- **Introspection Endpoint Allows Different Clients to Inspect a Token**

  OpenAM now allows clients other than the one issued the token to use the token introspection endpoint (`/introspect` endpoint. You can add a new scope, `am-introspect-all-tokens` to grant access to clients to introspect all tokens using the OAuth 2.0 introspection endpoint.

- **Updated WS-Federation Attribute Mapping Configuration**

  The WS-Federation attribute mapper now checks the attribute mapping configuration from the remote service provider (SP) first, and if it was present, uses that instead of a identity provider attribute mapping configuration.

  This WS-Federation configuration change allows it to function in a similar manner as the SAML2 attribute mapping solution.

- **Fix to Session Debug File When Invalid Sessions are Checked**

Previously, OpenAM would log a stack trace in the Session debug file when making a call to the `/json/sessions` endpoint with the validate action and passing in a token whose related session is invalid.

The message level has been changed from ERROR to MESSAGE, which no longer results in a stack trace in the logs.

- **Use org.forgerock.http.util.Uris for Query Parameter Encoding/Decoding**

  Previously, OpenAM used application/x-www-form-urlencoded-based encoding from `com.sun.identity.shared.encode.URLEncDec` for HTTP request query parameters. This often led to issues when using proxies, such as OpenIG that apply strict RFC decoding and encoding routines.

  OpenAM now uses `org.forgerock.http.util.Uris` from the Commons library, which provides encoding and decoding methods for both application/x-www-form.urlencoded and query parameters.

- **Reduced Metadata for Stateless OAuth 2.0 Tokens**

  OpenAM now stores less metadata in the CTS when the server uses Stateless OAuth 2.0 tokens. This improvement does not render any existing OAuth 2.0 tokens invalid.

  When you upgrade an OpenAM server, the upgrade process enables Stateless Grant Token upgrade compatibility mode. This mode allows the CTS to store both former and current formats of Stateless OAuth 2.0 token metadata. The mode enables you to benefit from the improvement when performing a rolling, zero-downtime upgrade of an OpenAM cluster.

  After successfully upgrading all servers in the cluster, disable this mode on each OpenAM server in one of the following ways:

  - In OpenAM console, under Configure > Global Services > OAuth2 Provider, disable Stateless Grant Token upgrade compatibility mode, and save the change.
  - Set the global OAuth2 Provider service property, `statelessGrantTokenUpgradeCompatibilityMode`, to `false`.

OpenAM 13.5.1

- **CTS Session Affinity Capability**

  OpenAM 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 of OpenAM that do not support session affinity require the CTS token store to be deployed in an active/passive architecture, which limits OpenAM'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 "General Recommendations for CTS Configuration" in the *Installation 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. OpenAM 13.5.1 adds two new properties to the OAuth 2.0 / OpenID Connect client to define a timeout for the encryption and signature verification caches:

  - JWKs URI content cache timeout in ms, `com.forgerock.openam.oauth2provider.jwksCacheTimeout`
  - JWKs URI content cache miss cache time, `com.forgerock.openam.oauth2provider.jwkStoreCacheMissCacheTime`

  For more information, see OAuth 2.0 and OpenID Connect 1.0 Client Configuration Fields in the *Administration Guide*.

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

  OpenAM 13.5.1 now supports signing and encrypting `UserInfo` responses as per the OIDC spec.

  The following properties have been added to the OAuth 2.0 / OpenID Connect client:

  - User Info signed response algorithm, `com.forgerock.openam.oauth2provider.userinfo.signedResponseAlg`
  - User Info encrypted response algorithm, `com.forgerock.openam.oauth2provider.userinfo.encryptedResponseAlg`
  - User info encrypted response encryption algorithm, `com.forgerock.openam.oauth2provider.userinfo.encryptedResponseEnc`
  - User info response format, `com.forgerock.openam.oauth2provider.userinfo.responseFormat`

  For more information, see OAuth 2.0 and OpenID Connect 1.0 Client Configuration Fields in the *Administration 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 "OAuth 2.0 Mix-Up Mitigation" in the *Administration Guide* and "Hints for the OAuth 2.0/OpenID Connect Authentication Module" in the *Administration Guide*.

- **OAuth 2.0 Authentication Module Can Return Specific Failure Messages**

  OpenAM 13.5.1 adds a new property, Enable auth module messages for Password Credentials Grant, to allow the OAuth 2.0 Authentication Module to return specific failure messages. For example:

  ```
  {"error_description":"Your account has been locked.","error":"invalid_grant"}
  ```

  For more information, see "OAuth2 Provider" in the *Reference*.

- **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 "Configuring OAuth 2.0 and OpenID Connect 1.0 Clients" in the *Administration Guide*.

- **User Self-Registration Flow Improved**

  The user self-registration flow has been improved so the email validation occurs after the user has provided their details. For more information, see "To Register a User with the REST APIs (13.5.1 or later)" in the *Developer's Guide*.

- **OpenAM 13.5.1 also features the following improvements:**

  - OPENAM-3574: SMSGateway is missing JavaDoc
  - OPENAM-5969: Allowing RequesterID chain when using SAML2 Idp Proxy
  - OPENAM-8210: Enhance CTS to persist tokens across multiple OpenDJ instances rather than a single primary OpenDJ instance by some form of sharding
  - OPENAM-9009: When using REST endpoint "json/users/?_action=create" with password policy violation, AM returns HTTP 400 "bad request", reason "Bad Request" , Message "Bad Request" rather than a more meaningful error message
  - OPENAM-9234: Add health check for the SOAP STS
  - OPENAM-9366: Install.log doesn't contain timestamps, which block performance issue investigation
  - OPENAM-9460: Include SOAP STS WAR in OpenAM Distribution Zip
  - 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 13.5

- **The following improvements and additional features were added in OpenAM 13.5:**
  - OPENAM-5093: OAuth2 user consent confirmation can be optional
  - OPENAM-5131: FederationConfig.properties in unconfigured Fedlet should have com.sun.identity.common.serverMode=false by default
  - OPENAM-5213: OAuth2 tokeninfo endpoint is not returning client_id info
  - OPENAM-5938: Cert Auth module should not read cert from HTTP request when 'iplanet-am-auth-cert-gw-cert-auth-enabled' is set
  - OPENAM-6315: Proxying SAML2 Second level status code
  - OPENAM-7146: Revoke access tokens while revoking refresh tokens
  - OPENAM-7294: Support for WS-Federation active requestor profile
  - OPENAM-7320: Consider using JDK JAXP/XML instead of Xerces/Xalan to keep up with JDK fixes
  - OPENAM-7702: Give the ability to disable creation of sign out tokens
  - OPENAM-7778: XML Signature DigestMethod should be configurable when using SAML2
  - OPENAM-7820: Additional delete/revoke token endpoints for Oauth2
  - OPENAM-7914: Make the attribute com.sun.identity.server.fqdnMap hot-swappable
  - OPENAM-7996: Self-registration destination after registration
  - OPENAM-8194: The default WS-Fed IDP attribute mapper should provide a way to Base64 encode binary attributes

- OPENAM-8387: OpenAM should provide more detailed log messages when KeyUtil.getDecryptionKey does not find the requested key
- OPENAM-8423: Introduce "audience URL" attribute in OAuth2 client for Saml2GrantTypeHandler
- OPENAM-8578: The default WS-Fed and SAML2 IDP attribute mapper should provide a way to Base64 binary encoding of NameID
- OPENAM-8580: OpenAM should allow to use objectGUID value from AD when working with persistent NameID
- OPENAM-8932: WS-Federation should support attribute mapping with custom namespaces
- OPENAM-9124: FaceBook authentication module & documentation should be updated to reflect changes to FaceBook API
- OPENAM-9279: User registration should return authn success addition properties inline with the authn endpoint

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 details of all the security advisories across ForgeRock products, see Security Advisories in the *Knowledge Base library*.

Chapter 2

Before You Install OpenAM 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.

2.1. OpenAM Operating System Requirements

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

Supported Operating Systems

Operating System	Version
Red Hat Enterprise Linux, Centos	6, 7
SuSE	11
Ubuntu	12.04 LTS, 14.04 LTS
Solaris x64	10, 11
Solaris Sparc	10, 11
Windows Server	2008, 2008 R2, 2012, 2012 R2

2.2. Java Requirements

JDK Requirements

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

2.3. OpenAM Web Application Container Requirements

Web Containers

Web Container	Version
Apache Tomcat	7, 8[a]
Oracle WebLogic Server	12c
JBoss Enterprise Application Platform	6.1+
JBoss Application Server	7.2+
WildFly AS	9
IBM WebSphere	8.0, 8.5.5.8+

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

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

2.4. Data Store Requirements

Supported Data Stores

Data Store	Version	CTS Datastore	Config Datastore	User Datastore	UMA Datastore
Embedded OpenDJ	3.5	✓	✓	✓	✓
External OpenDJ	2.6, 2.6.4, 3.0, 3.5	✓	✓	✓	✓
Oracle Unified Directory	11g			✓	
Oracle Directory Server Enterprise Edition	11g			✓	
Microsoft Active Directory	2008, 2008 R2, 2012, 2012 R2			✓	
IBM Tivoli Directory Server	6.3			✓	

2.5. Supported Clients

The following table summarizes supported clients:

Supported Clients

Client Platform	Native Apps[a]	Chrome 16+[b]	IE 9+, Microsoft Edge	Firefox 3.6+	Safari 5+
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] Chrome, Firefox, and Safari are configured to update automatically, so customers will typically running the latest versions. The versions listed in the table are the minimum required versions.

2.6. Supported Upgrade Paths

The following table contains information about the supported upgrade paths to OpenAM 13.5.2-15:

Upgrade Paths

Version	Upgrade Supported?
OpenAM 9.0.x	No
OpenAM 9.5.x	No
OpenAM 10.0.x	No
OpenAM 11.0.x	Yes
OpenAM 12.0.x	Yes
OpenAM 13.x.x	Yes

Note

Upgrading between OpenAM Enterprise and OpenAM OEM versions is not supported.

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

2.7. 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 OpenAM 13.5.2-15 software.

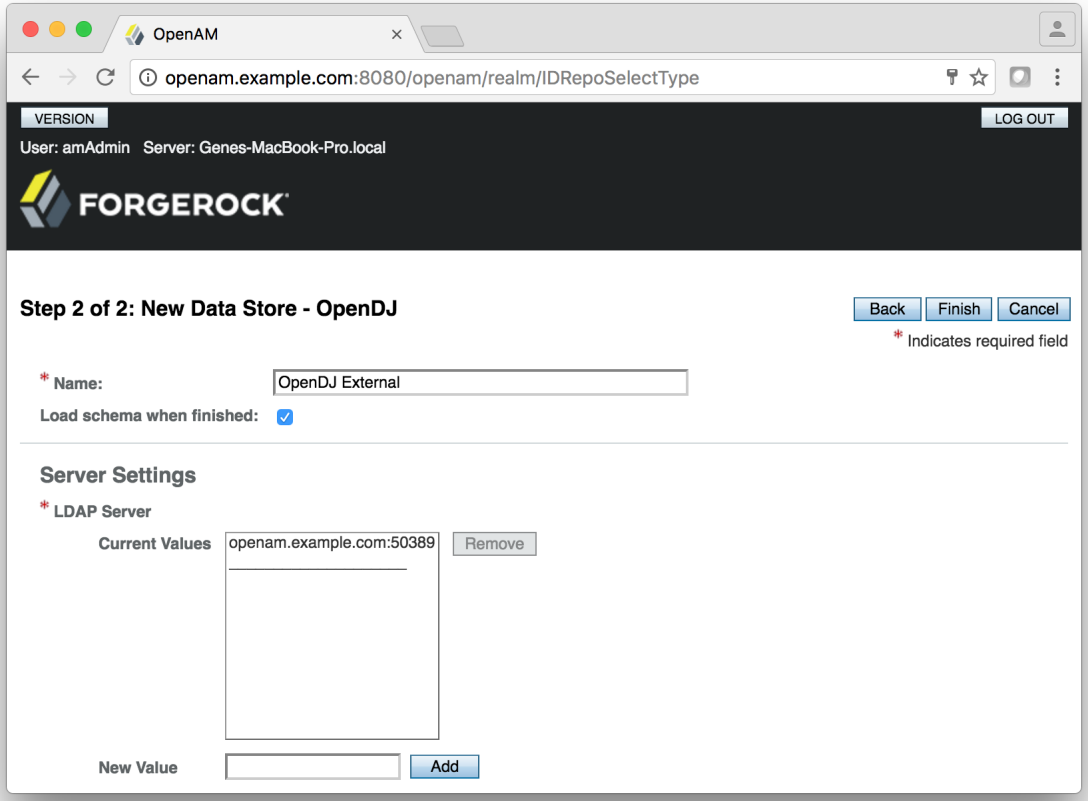
Note

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.

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 are upgrading from OpenAM 13.0 to OpenAM 13.5 and want to configure Push Authentication with your external data store, you must manually apply the schema update to the data store by enabling the `load schema when finished` in the OpenAM console. You can set the property on the OpenAM console by navigating to Top Level Realm > Data Stores > New > data store type.

Load Schema When Finished



- In a clean OpenAM 13.5 installation, you must manually update the schema using the `opendj_pushdevices.ldif` if you want to use Push Notifications. The `opendj_pushdevices.ldif` is located in `/path/to/tomcat/webapps/openam/WEB-INF/template/ldif/opendj` [1] folder. To manually update the schema, see Updating Directory Schema in the *OpenDJ Administration Guide* for instructions.

For additional information about upgrading OpenAM, see the Upgrade Guide.

[1] There are analogous `pushdevices.ldif` files for Active Directory in the `/path/to/tomcat/webapps/openam/WEB-INF/template/ldif/ad` folder; Oracle DSEE in the `/path/to/tomcat/webapps/openam/WEB-INF/template/ldif/odsee` folder; Tivoli in the `/path/to/tomcat/webapps/openam/WEB-INF/template/ldif/tivoli` folder. For instructions to update the schema, see the respective directory server documentation.

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

OpenAM 13.5.2

- **Updated WS-Federation Attribute Mapping Configuration**

  The WS-Federation attribute mapper now checks the attribute mapping configuration from the remote service provider (SP) first, and if it was present, uses that instead of a hosted identity provider (IDP) attribute mapping configuration.

  This WS-Federation configuration change allows it to function in a similar manner as the SAML2 attribute mapping solution.

- **New Property: org.forgerock.policy.subject.evaluation.cache.size**

  The property controls the size of the `SubjectEvaluationCache`. The default value is 10000.

OpenAM 13.5.1

- **Some CTS OIDs 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 "*Core Token Service (CTS) Object Identifiers*" in the *Reference*.

- **Client ID can now be sent alongside HTTP Basic Auth Credentials**

  Previously, sending both HTTP Basic Auth credentials and the `client_id` property, without including the `client_secret`, returned: ERROR: Client (client) using multiple authentication methods. This is in accordance to RFC 6749, section 2.3.1, which states that a client MUST only send a single form of authentication. However, passing `client_id` in the message body, but not `client_secret`, does not constitute credentials and therefore is now permitted.

- **User Self-Service Now Respects the Locale Parameter in HTTP Requests.**

  User self-service emails are now returned displaying the requested locale attributes configured within user self-service.

- **Improved Audit Logs for Not Found Failures.**

  The failure reason is now printed in audit log for "User Not Found" cases.

- **Added Cross-store Inactivity Checks.**

  The logic for checking whether a user is active or not should now fail if the user is inactive in any of the configured user stores.

OpenAM 13.5

- 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 13.5, 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.

- **Cookie Domain Defaults to FQDN**. When adding another server to an existing OpenAM 13.5.0 deployment using the GUI configurator, the cookie domain in the OpenAM setup wizard sets the cookie domain to be the full URL that was used to access the configurator, such as `example.com`.

  For more information, see OPENAM-9369.

- **SAML 2.0 NameID Persistence Extended**. OpenAM's SAML 2.0 account management and NameID persistence logic was updated to work better with non-persistent NameID formats in OpenAM 13.0.0. It has now been extended to have persistence completely controlled by the hosted IdP flag (`idpDisableNameIDPersistence`) and the hosted/remote SP flag (`spDoNotWriteFederationInfo`). These flags now also control whether the persistent NameID details should be stored in the datastore.

  This change allows deployments that have a read-only user store shared by the SP and IdP to not store persistent federation information.

  The NameID persistence logic can now summarized as follows:

  ```
  Persistent NameID         -> NameID RECOMMENDED 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 were made on the identity provider side:

  - **Setting: idpDisableNameIDPersistence**. OpenAM provides a setting, `idpDisableNameIDPersistence`, which disables the storage of the NameID values for all NameIDs issued by that IdP instance.
  - **SP's spDoNotWriteFederationInfo Repurposed**. The SP's `spDoNotWriteFederationInfo` setting has been repurposed. It no longer applies to unspecified NameID-Formats and now allows persistence to be set to NOT store federation info.
  - **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.
  - **Method in the IDPAccountMapper Interface**. The `IDPAccountMapper` interface has been extended with a new `shouldPersistNameIDFormat` method.

    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.

For more information, see shouldPersistNameIDFormat in the *OpenAM API Javadoc*.

- **The default WS-Fed 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
```

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.
- **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);
```

This implementation first checks whether NameID persistence has been completely disabled at the IdP level (idpDisableNameIDPersistence setting), and if not, it will look at the SP configuration as well (spDoNotWriteFederationInfo setting).

For more information, see OPENAM-8580.

- **.NET Fedlet Documentation Moved**: The .NET Fedlet documentation is now a KB article available to ForgeRock customers.
- **New Attribute Required in Authentication Service Definition**. OpenAM 13 requires that schemas in the definition of an authentication service contain `resourceName` attributes.

The attributes are not added to custom authentication service definitions when upgrading from a previous version, so must be added manually.

The specific changes required in the service definition schema are:

- The `Schema` element in the service definition must contain a `resourceName` attribute. This value is used to refer to the service when managing the service using REST.

  For example:

```
<Schema
 serviceHierarchy="/DSAMEConfig/authentication/iPlanetAMAuthSampleAuthService"
 i18nFileName="amAuthSampleAuth"
 revisionNumber="10"
 i18nKey="sampleauth-service-description"
 resourceName="mySampleAuthService">
```

- Any `SubSchema` elements in the service definition must contain a `resourceName` attribute, with a value of `USE-PARENT`.

  For example:

```
<SubSchema
 name="serverconfig"
 inheritance="multiple"
 resourceName="USE-PARENT">
```

An example of a service definition compatible with OpenAM 13 can be found in "The Sample Auth Service Configuration" in the *Developer's Guide*.

To Add Required Attributes to Custom Service Definition Schemas

You can add the required attributes either before or after upgrading to OpenAM 13. The steps in this procedure cover adding the attributes before upgrading.

1. If you have not already done so, install and configure a tool for altering the contents of the OpenDJ configuration store, for example the OpenDJ Control Panel or Apache Directory Studio.

2. Connect to the embedded configuration store using the same bind DN credentials as configured in OpenAM. The default is `cn=Directory Manager`.

3. In the directory tree of the configuration store, locate the `sunServiceSchema` attribute for your custom service definition under `ou=services`.

   For example, on a default install the definition for the data store service is located here: `ou=1.0,ou=sunAMAuthDataStoreService,ou=services,dc=openam,dc=forgerock,dc=org`

4. Edit the XML stored within the `sunServiceSchema` attribute, adding the required `resourceName` attribute to `Schema` and `SubSchema` elements.

5. Commit the changes to the configuration store, and proceed to upgrade OpenAM.

Failure to add the required attributes will result in the OpenAM 13 user interface being unable to view or edit custom services, or create or edit authentication modules based on them after upgrade. You may also see a `Not found error` message displayed in the administration console when creating or editing authentication modules.

- **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.

- **Legacy User Self Service Endpoints Disabled by Default**.

  The REST endpoints used by the legacy user self service features, such as registering for an account or resetting a forgotten password, are now disabled by default.

  Legacy deployments should migrate to the new user self-service features in OpenAM 13.5.2-15, see "*Configuring User Self-Service Features*" in the *Administration Guide*.

To restore the legacy endpoints, enable the Configure > Global Services > Legacy User Self Service > Legacy Self-Service REST Endpoint option.

Warning

Restoring the legacy self service endpoints allows REST requests crafted such that the body of the self-service email contains a malicious URL that end users may visit, hiding the correct OpenAM URL that is appended to the end of the email body.

- **REST Endpoint Changes**

Version 3.0 of the `/users` endpoint is provided in this release of OpenAM. The response differs from version 2.0 of the endpoint, which remains available for backwards compatibility.

The new version of the endpoint returns details about all users. The previous version only returned a list of usernames.

Version 3.0 of the `/users` endpoint does not support the following `_action` values:

```
https://openam.example.com:8443/openam/json/users/?_action=register
https://openam.example.com:8443/openam/json/users/?_action=confirm
https://openam.example.com:8443/openam/json/users/?_action=anonymousCreate
https://openam.example.com:8443/openam/json/users/?_action=forgotPassword
https://openam.example.com:8443/openam/json/users/?_action=forgotPasswordReset
```

Responses to Different Versions of the /users Endpoint

In this section, long URLs are wrapped to fit the printed page, and some of the output is formatted or truncated for easier reading.

Version 3.0 of the `/users` endpoint:

```
$ curl \
--header "iPlanetDirectoryPro: AQIC5w...2NzEz*"
 \
--header Accept-API-Version: protocol=1.0,resource=3.0 \
"https://openam.example.com:8443/openam/json/users?_queryId=*"
{
  "result": [
    {
      "username": "amAdmin",
      "realm": "dc=openam,dc=forgerock,dc=org",
      "sn": [
        "amAdmin"
      ],
      "givenName": [
        "amAdmin"
      ],
      "universalid": [
        "id=amAdmin,ou=user,dc=openam,dc=forgerock,dc=org"
      ],
```

```
      "cn": [
        "amAdmin"
      ],
      "roles": [
        "ui-global-admin",
        "ui-realm-admin"
      ],
      "inetuserstatus": [
        "Active"
      ],
      "dn": [
        "uid=amAdmin,ou=people,dc=openam,dc=forgerock,dc=org"
      ]
    },
    {
      "username": "demo",
      "realm": "dc=openam,dc=forgerock,dc=org",
      "uid": [
        "demo"
      ],
      "createTimestamp": [
        "20160108155628Z"
      ],
      "inetUserStatus": [
        "Active"
      ],
      "mail": [
        "demo.user@example.com"
      ],
      "sn": [
        "demo"
      ],
      "cn": [
        "demo"
      ],
      "objectClass": [
        "devicePrintProfilesContainer",
        "person",
        "iplanet-am-auth-configuration-service",
        "sunFMSAML2NameIdentifier",
        "organizationalperson",
        "inetuser",
        "kbaInfoContainer",
        "forgerock-am-dashboard-service",
        "iplanet-am-managed-person",
        "iplanet-am-user-service",
        "sunAMAuthAccountLockout",
        "top"
      ],
      "kbaInfo": [
        {
          "questionId": "2",
          "answer": {
            "$crypto": {
              "value": {
                "algorithm": "SHA-256",
                "data": "VXGtsnjJMC...MQJ/goU5hkfF"
              },
              "type": "salted-hash"
```

```
            }
          }
        }
      ],
      "dn": [
        "uid=demo,ou=people,dc=openam,dc=forgerock,dc=org"
      ],
      "universalid": [
        "id=demo,ou=user,dc=openam,dc=forgerock,dc=org"
      ],
      "modifyTimestamp": [
        "20160113010610Z"
      ]
    }
  ],
  "resultCount": 2,
  "pagedResultsCookie": null,
  "totalPagedResultsPolicy": "NONE",
  "totalPagedResults": -1,
  "remainingPagedResults": -1
}
```

Version 2.0 of the `/users` endpoint:

```
$ curl \
--header "iPlanetDirectoryPro: AQIC5w...2NzEz*"
 \
--header Accept-API-Version: protocol=1.0,resource=2.0 \
"https://openam.example.com:8443/openam/json/users?_queryId=*"
{
    "result": [
        "amAdmin",
        "demo"
    ],
    "resultCount": 2,
    "pagedResultsCookie": null,
    "totalPagedResultsPolicy": "NONE",
    "totalPagedResults": -1,
    "remainingPagedResults": -1
}
```

- **Workaround for java.lang.VerifyError in WebSphere**.

  When loading classes from OpenAM within WebSphere Application Server using the IBM Technology for JVM and Apache Axis2 framework, a `java.lang.VerifyError JVMVRFY013 class loading constraint violated` error may occur. For more information on the `java.lang.VerifyError` error, see "java.lang.VerifyError: JVMVRFY013 class loading constraint violated" Error.

  Fixing a WebSphere java.lang.VerifyError Error

  1. Remove the following JARs from the `WEB-INF/lib` directory in the `openam.war` file:
     - `jaxp-api-1.4.2.jar`
     - `xercesImpl-2.11.0.jar`

- `xml-apis-2.11.0.jar`
- `xml-resolver-2.11.0.jar`
- `xml-serializer-2.11.0.jar`

For instructions on how to expand the `openam.war` file, make changes to `bootstrap.properties` file, and then rebuild the `openam.war` file, see "To Prepare OpenAM for JBoss and WildFly" in the *Installation Guide*.

2. Set the following custom JVM properties on the WebSphere server:

```
-
Djavax.xml.soap.MessageFactory=com.sun.xml.internal.messaging.saaj.soap.ver1_1.SOAPMessageFactory1_1Impl
-Djavax.xml.soap.SOAPFactory=com.sun.xml.internal.messaging.saaj.soap.ver1_1.SOAPFactory1_1Impl
-
Djavax.xml.soap.SOAPConnectionFactory=com.sun.xml.internal.messaging.saaj.client.p2p.HttpSOAPConnectionFactor
-Djavax.xml.soap.MetaFactory=com.sun.xml.internal.messaging.saaj.soap.SAAJMetaFactoryImpl
-Dcom.ibm.websphere.webservices.DisableIBMJAXWSEngine=true
```

3. Restart the WebSphere server.

- **Different return type for GetUserInfo method of ScopeValidator interface**.

  The return type for the `getUserInfo` method of the `org.forgerock.oauth2.core.ScopeValidator` interface, formerly `Map<String, Object>`, is now `org.forgerock.oauth2.core.UserInfoClaims`. The new return type lets callers of the `getUserInfo` method see values of users' claims.

  This change affects OAuth v2.0 scope validator plugins. For more information, see "Customizing OAuth 2.0 Scope Handling" in the *Developer's Guide*.

- **Oracle Directory Server Enterprise Edition no longer supported for the OpenAM configuration store**.

  In previous versions, it was possible to deploy the OpenAM configuration store in an external Oracle Directory Server Enterprise Edition instance.

  In OpenAM 13.5.2-15, this is no longer possible. You must deploy the OpenAM configuration store in an OpenDJ server instance: either the embedded OpenDJ directory server instance that is installed together with OpenAM, or in an external server instance.

- **The steps to install and configure a Java Fedlet have changed**.

  In previous versions, the Create Fedlet wizard included the federation configuration in the `fedlet.war` file, and added the `fedlet.war` file to the `Fedlet.zip` file. This is no longer the case, and as a result, the steps you perform to install and configure a Java Fedlet have changed.

  For updated steps to install and configure a Java Fedlet, see "Creating and Installing a Java Fedlet" in the *Developer's Guide*.

- **Persistent cookies are now encrypted and signed**.

In previous versions, persistent cookies were encrypted with OpenAM's public RSA key. OpenAM 13.5.2-15 now signs the persistent cookie with a user-specified HMAC signing key in addition to encrypting it.

For information about the new HMAC Signing Key property in the Persistent Cookie authentication module, see "Hints for the Persistent Cookie Module" in the *Administration Guide*.

4.2. Deprecated Functionality

OpenAM 13.5.2

- No features have been deprecated in OpenAM 13.5.2.

OpenAM 13.5.1

- No features have been deprecated in OpenAM 13.5.1.

OpenAM 13.5.0

- The following REST endpoints have been deprecated from OpenAM and will be removed in a future release:
  - `/identity/attributes`
  - `/identity/authenticate`
  - `/identity/authorize`
  - `/identity/create`
  - `/identity/delete`
  - `/identity/isTokenValid`
  - `/identity/logout`
  - `/identity/read`
  - `/identity/search`
  - `/identity/update`

  For more information on deprecated and removed endpoints, see How Do I know which endpoint to use for REST calls in new versions of OpenAM/AM? in the *ForgeRock Knowledge Base*.

4.3. Removed Functionality

OpenAM 13.5.2

- No functionality has been removed from OpenAM 13.5.2.

OpenAM 13.5.1

- **LDAPS Server Protocol Version Removed**

  The LDAPS Server Protocol Version and its accompanying property, `openam-idrepo-ldapv3-config-secure-protocol-version` has been removed from OpenAM 13.5.1.

  If your external configuration store uses TLSv1.2 connections only, set the TLS version using a JVM property:

  ```
  -Dorg.forgerock.openam.ldap.secure.protocol.version=TLSv1.2
  ```

- `ssoadm` **Policy Commands Removed**

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

  Policy Import and Export With the `ssoadm` Command

Removed in the *Administration Guide* Command	**New 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*.

- **Relational Database Identity Repository (Early Access) Removed**

  The early access feature of storing identity data in a relation databasehas been removed from OpenAM. This feature was only supported for test and development environments.

- **Support for the OAuth2 JWT Bearer Grant Type Removed**

  OpenAM does no longer implement section 2.1 of the JSON Web Token Profile for OAuth 2.0 Client Authentication and Authorization Grants.

OpenAM 13.5

- **REST Endpoints Removed**

  The following REST endpoints have been removed from OpenAM 13.5.0:

  - `/json/[_realm/_]referrals`
  - `/ws/1/entitlement/decision`
  - `/ws/1/entitlement/decisions`
  - `/ws/1/entitlement/entitlement`
  - `/ws/1/entitlement/entitlements`
  - `/ws/1/entitlement/listener`
  - `/ws/1/entitlement/privilege`
  - `/ws/1/token`

  For more information on deprecated and removed endpoints, see How Do I know which endpoint to use for REST calls in new versions of OpenAM/AM? in the *ForgeRock Knowledge Base*.

- **Server configuration property removed**. The following server configuration property has been removed from OpenAM:

  - `com.sun.am.event.connection.idle.timeout`

- **Network Security Services for Java (JSS) and Native Support for FIPS Removed**

  Network Security Services for Java (JSS) has been removed from OpenAM. As a result, OpenAM no longer provides native support for Federal Information Processing Standard (FIPS) mode.

  For more information on FIPS mode support, see Are ForgeRock products FIPS 140-2 compliant? in the *ForgeRock Knowledge Base*.

- **OAuth2 v1.0 Removed**

  OpenAM's implementation of OAuth v1.0 has been removed.

- **Administrative Service Remove**

  The Administration Service has been removed.

Chapter 5

Fixes, Limitations, and 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 13.5.2-15.

5.1. Key Fixes

5.1.1. Key Fixes in OpenAM 13.5.2

The following important issues were fixed in this release:

- OPENAM-1167: WindowsDesktopSSOConfig ClassCastException on saving configuration in admin UI
- OPENAM-4448: Allow custom Audiences in SAML Assertions
- OPENAM-5152: AMAuthLevelManager miscalculates auth level
- OPENAM-5153: Auth modules should call setAuthLevel after successful login
- OPENAM-5865: AuthLevelCondition will not retrieve request auth level for a capital-letter realm.
- OPENAM-6032: ssoadm command line help and ssoadm.jsp are inconsistent with the product
- OPENAM-6252: Sporadic error on ssoadm commands
- OPENAM-7523: Can't create realm in Internet Explorer 11
- OPENAM-7781: persistent cookie auth module does not allow to change cookie name by default
- OPENAM-7911: Improve Error Message: "Invalid Suffix"
- OPENAM-8602: Configurable Failure Retry attempts for OTP Authentication modules
- OPENAM-8771: "Unknown Error: Please contact your administrator", shown with FacebookSocialAuthentication option "Prompt for password setting and activation code" (org-forgerock-auth-oauth-prompt-password-flag)
- OPENAM-8807: RsaJWK is unable parse single x5c element in jwksContents
- OPENAM-8983: introspect endpoint shouldn't be limited to the same client as token

- OPENAM-9429: Update JWT usage as a result of COMMONS-98
- OPENAM-9717: TimerPool deadlock on ssoadm shutdown (client SDK)
- OPENAM-10039: TokenInfo endpoint doesn't work for Stateless tokens
- OPENAM-10129: OAuth2 Device flow - user code verification is case insensitive
- OPENAM-10221: 'subject/subjects' field in the policy creation response is unordered
- OPENAM-10233: Authentication failing when multiple datastores in realm
- OPENAM-10346: Audit logging entries missing if federation changes are done using ssoadm command in sub-realms.
- OPENAM-10430: CTS fail-back does not work properly
- OPENAM-10525: Some endpoints returning 500 with no error message or response body
- OPENAM-10578: Stateless access token doesn't contain the grant type
- OPENAM-10591: Generate more debug details about the JSON that is failing when JsonPolicyParser throws a UNABLE_TO_SERIALIZE_OBJECT exception
- OPENAM-10603: Login page error "Maximum sessions limit reached or session quota has exhausted" with restricted tokens and session quotas
- OPENAM-10619: Post Authentication Plugin not run during session upgrade
- OPENAM-10673: SAML2 authentication module fails to redirect to IDP after failing DeviceID match module
- OPENAM-10782: endSession with an id_token generated from a refresh_token request does not destroy the session
- OPENAM-10874: Adding a new server (site) requires a Restart on all the old servers
- OPENAM-10933: DeviceIdSave auth module fails with NullPointerException if the storage attribute is not already present
- OPENAM-10970: logout response binding should be selected based on the capabilities of the SP
- OPENAM-10997: "Authentication by Module Instance" will fail in cluster
- OPENAM-11070: Need OAuth2 authentication to work in Android with implied consent
- OPENAM-11101: Social Auth links do not contain the goto url
- OPENAM-11115: Push authentication should use alias attributes to find identities
- OPENAM-11154: Memory leak in SMSEventListenerManager#subNodeChanges

- OPENAM-11157: Oauth2/OIDC Authentication redirect goto value wrong when behind reverse proxy
- OPENAM-11194: Goto url not used in the presence of a valid session or after a redirect callback
- OPENAM-11196: Incorrect debug logging level used in FMEncProvider.getEncryptionKey
- OPENAM-11217: SAML2 Authentication module is not invoking custom SP Adapter class implementing a preSingleSignOnRequest() method.
- OPENAM-11229: OpenAM create/leaks temp files when getting large REST response
- OPENAM-11263: Improve Embedded DJ logging to pick up replication configuration errors.
- OPENAM-11272: The OIDC RSA JWKS modulus has an extra octet
- OPENAM-11275: Ops tokens are stored for Oauth2 tokens without the OIDC scope
- OPENAM-11283: NPE in TimerPool#shutdown during shutdown
- OPENAM-11293: ODSEE ldif incorrectly identifies the pushDeviceProfile location
- OPENAM-11312: Attribute Mapping defined in wsfed remote SP should not be overridden by attribute mapping defined in wsfed OpenAM Hosted IDP
- OPENAM-11314: Upgrade from 12.0.4 is failing
- OPENAM-11321: When making a call to the /json/sessions endpoint with _action=validate and passing in a token whose related session is invalid OpenAM logs a very large stack trace
- OPENAM-11340: Password grant flow is failing after fix of OPENAM-10782
- OPENAM-11349: Assigning a service to ActiveDirectory user will throw NPE
- OPENAM-11350: SAML2 IDPEntry XML element contains content violates SAML2 XML schema
- OPENAM-11355: Missing Service tab when trying to configure dashboard with Active Directory datastore
- OPENAM-11362: Utilise standards-based org.forgerock.http.util.Uris methods for query parameter encoding/decoding
- OPENAM-11391: Requesting 'OAuth2.0/OIDC' auth module a second time results in display of AM's "Authentication Failed" page
- OPENAM-11402: OpenAM does not enforce OAuth2 spec for "Resource Owner Password Credentials Grant" flow
- OPENAM-11432: Extra space in Policy 's Resource Type will cause policy evaluation to fails
- OPENAM-11453: The OAuth2 Device Flow does not make effective use of the affinity based LB for the user_code

- OPENAM-11461: Issuing access token with authorisation code fails using openid scope
- OPENAM-11472: WS-Federation extended metadata import fails when using ssoadm
- OPENAM-11491: Upgrading OpenAM results in failure due to restSMS.xml
- OPENAM-11506: Device code polling the CTS
- OPENAM-11526: Realm Authentication chain post authentication classes PAP not triggered on chains with multiple modules
- OPENAM-11548: Improve Scope validator class loading error handling
- OPENAM-11564: Ops is always created, even if the option "Store Ops Tokens" is disabled.
- OPENAM-11565: Implicit grant flow is not generating an Ops token
- OPENAM-11578: ampassword throws Guice Injection error
- OPENAM-11584: Ssoadm policy-import/export throws Guice error
- OPENAM-11607: ssoadm import-svc-cfg fails with Guice errors
- OPENAM-11610: WindowSSO module broken in AM 5.1.1 after upgrade
- OPENAM-11630: id_token values are space trimmed
- OPENAM-11632: CDCServlet does not work with realm
- OPENAM-11708: ssoadm sub-command set-attr-defs is failing with a Guice error
- OPENAM-11759: Memory leak affecting policy evaluation for stateless sessions
- OPENAM-11789: User remains on 'Loading' page with 'OAuth2.0/OIDC' auth module if authId token expires before entering credentials
- OPENAM-11818: Oauth2 authn module incorrectly POST state parameter to token endpoint
- OPENAM-11834: Passwords being set to empty strings in tabbed forms in XUI
- OPENAM-11937: Federation UI does not allow empty NameIDMappingService
- OPENAM-11944: REST OAuth2 creation triggers objectClass=* search
- OPENAM-11956: SAML2 RelayState values are seen as invalid if they are not a URL which appears to go against the spec
- OPENAM-11966: saml2 SSO 'better' auth'n comparison fails with 'Invalid status code in response'
- OPENAM-11968: SAML2 Auth Module does not accept SAML2 AuthResponse with no SessionIndex

- OPENAM-11987: SmsServerPropertiesResource removes password when unchanged.
- OPENAM-12002: The mutiple entries in "Primary LDAP Server" for Policy Configuration must be a single line.
- OPENAM-12037: Memory leak: LDAPFilterCondition creates new ShutdownManager listener on each request
- OPENAM-12040: OpenAMSettingsImpl#getServerKeyPair uses the same password for key password and store password
- OPENAM-12071: Error during upgrade with unindex search from UpgradeUtils.deleteService()
- OPENAM-12164: Google social auth fails when authorization code is double encoded
- OPENAM-12219: Resource leak in MonitoringAdapters#getMonAuthList
- OPENAM-12252: Delegated admin with Stateless Session, causes Admin Console failure.
- OPENAM-12319: Memory leak in accessing Jato Pages.

5.1.2. Key Fixes in OpenAM 13.5.1

The following important issues were fixed in this release:

- OPENAM-920: Monitoring fails to handle secondary site IDs
- OPENAM-2911: IdP initiated SSO with persistent identifier causes URLNotFoundException: Invalid service host name.
- OPENAM-3679: IDP Finder fails to validate relaystate
- OPENAM-4353: ClusterStateService throws NPE
- OPENAM-5096: Single Logout (SLO) via Proxy - active session partner in sendLastResponse()
- OPENAM-5191: IdP proxy uses the NameID-Format list from the Remote SP when returning an encrypted assertion, instead of the NameID-Format returned by the remote IdP
- OPENAM-5542: ServiceConfigImpl causes memory leak.
- OPENAM-5626: XUI not redirecting to console when no datastore in top realm
- OPENAM-5632: Occasional failure of OpenAM configurator tool
- OPENAM-5640: SAML SP ignore Conditions in Assertion.
- OPENAM-6708: Cannot set stateless session properties in PAP
- OPENAM-7437: Finish button of Identity Provider wizard doesn't work

- OPENAM-7860: Cannot setup 12.0.x with IBM JDK 7
- OPENAM-8063: Merge Debug Files feature does not work correctly
- OPENAM-8151: SAML SSO for subrealm does not correctly login user as it ignores the org param when XUI enabled
- OPENAM-8202: If the "Login Id" in the External Store Configuration(CTS) is set to incorrect value,CoreSystem debug log is full of duplicate error
- OPENAM-8251: RestletRealmRouter fails to route request to /<subrealm>/connect/checkSession
- OPENAM-8389: Audit Event Handler ignores realm-based log configurations
- OPENAM-8459: LDAPAuthUtils should set operations timeout in seconds
- OPENAM-8690: OIDC/OAuth2 client should always be able to request and obtain any scope they are configured for
- OPENAM-8813: insufficient debug logging in FMEncProvider
- OPENAM-8874: Policy Evaluation Rest API does not refresh SSO token Idle timeout
- OPENAM-8910: NPE if a null siteID is passed to Session.validateSessionID
- OPENAM-8971: currentGoto : null is received in XUI when a realm dns is being used for Federation and authentication is done via wdsso/kerberos auth module
- OPENAM-8998: Completing USS Forgot Password flow results in lost goto parameter on Return to Login Page link
- OPENAM-9012: LDAP connection heartbeat settings should be also added to policy configuration
- OPENAM-9027: IdServiceImpl logs message level data on warning level
- OPENAM-9083: DefaultIDPAuthnContextMapper selects highest auth-level configured
- OPENAM-9143: SAML IdP attribute mappers should work with profile attributes even when the user profile mode is set to dynamic
- OPENAM-9156: 'Not Found' error in UI when opening a custom auth module created with ssoadm with the name the same as type
- OPENAM-9283: When using ssoadm to create a batch of Federation entities, "Entity existed in the circle of trust" error is given when the entity does not exist
- OPENAM-9290: OpenAM should send a response to the SP in case of empty NameIdPolicy value in SAML Authn Request
- OPENAM-9334: 'Authentication Module Denied' is raised when SMSAuthModule login fails with invalid password

- OPENAM-9352: ResourceOwnerSessionValidator should validate session to refresh idletime
- OPENAM-9357: Upgrading to 13.x does not populate Subject Type in OAuth2Client config, causing an NPE
- OPENAM-9364: Authentication error codes are not made available correctly to SAML2 extensions
- OPENAM-9432: SAML2 authentication module not functioning as expected when SAML2 Failover is enabled
- OPENAM-9443: "ID Token Signing Algorithms supported" values are missing in OAuth2 service after upgrade.
- OPENAM-9465: Missing policy 's subjects after upgrading from OpenAM 11 to OpenAM 13.5
- OPENAM-9475: request binding chosen for SP initiated SSO should be based on the capabilities of the IdP
- OPENAM-9482: The provided Access Control Instruction (ACI) target expression DN value "dc=openam,dc=forgerock,dc=org" is invalid.
- OPENAM-9483: Delegated realm admin cannot edit realm property using REST API
- OPENAM-9507: OAuth2 consent page does not work with wap display mode
- OPENAM-9515: XUI does not enable Secure cookie flags for SSO tracking cookie on 13.5.0
- OPENAM-9526: Compiling the source code without git repo fails at openam-clientsdk module
- OPENAM-9533: DNS alias overrides the realm query parameter passed in the URL when requesting OAuth2 access token
- OPENAM-9597: Goto URL with multiple query string parameters incorrectly decoded
- OPENAM-9610: XUI login page fails on first load using iOS with "Unknown error. Please contact your administrator."
- OPENAM-9611: InvalidStatusCodeSaml2Exception breaks the SAML2 SP Error handling in a non IDP-proxy environment.
- OPENAM-9614: OpenAM 13.5 upgrade fails to correctly remove DevicePrintModule
- OPENAM-9628: Strange 400 response after changing advanced default server properties from site URL
- OPENAM-9629: OAuth2 flow creates GENERIC CTS tokens that never expire
- OPENAM-9644: Redirect callback flow doesn't set the AM_REDIRECT_BACK_SERVER_URL cookie
- OPENAM-9648: Invalid Session that causes CDATA[null] response make Web Agent not reauthenticate

- OPENAM-9685: SSOAdmin is slow with a site configured
- OPENAM-9689: OpenAM can not be configured if TLSv1.2 external configuration data store and user data store are used
- OPENAM-9695: PLL request is returning an empty policy/decision set in local webagent configuration
- OPENAM-9703: Remove deprecated ssoadm policies commands
- OPENAM-9705: Show floating point value for average rate of deleted tokens per CTS Reaper Run
- OPENAM-9719: session upgrade fails in combination with SAML-based SSO
- OPENAM-9731: Occasional failure to find server from ID in Webtop/Naming
- OPENAM-9753: root cause for IdRepoException in SessionService.isSuperUser() is lost
- OPENAM-9813: Policy with Subject exclusive set is lost on upgrade
- OPENAM-9849: isActive check should fail if the user is inactive in any of the configured data stores
- OPENAM-9859: ACR_Values not working if the user is login in more than one chain
- OPENAM-9885: Oauth2 load: Tomcat keeps logging "WARNING: Addition of the standard header "Pragma" is discouraged as a future version of the Restlet API will directly support it."
- OPENAM-9891: NPE in ssoadm due to modification of WebtopNaming
- OPENAM-9893: WindowsDesktop SSO auth module broken when XUI is used
- OPENAM-9919: IDP Proxy fails if Assertion is Encrypted
- OPENAM-9957: SAML2 authenticationStep cookie does not get set if platform cookie domains list is empty
- OPENAM-9979: Authentication chain post authentication classes are not used if realm level PAP setting exists
- OPENAM-9992: Unable to set realm DNS alias for Push auth/reg URLs
- OPENAM-10087: Set of character for user code in OAuth2 device flow should not contain confusing characters (such as 0 and O).
- OPENAM-10102: insufficient progress information during configuration
- OPENAM-10103: output from re-indexing action during initial configuration is lost
- OPENAM-10115: NPE thrown if redirect_uri was missing from authorization code
- OPENAM-10135: Classic UI customizations not found due to incorrect defaultOrg format

- OPENAM-10151: persistent search connections to external OpenAM configuration data store can become stale
- OPENAM-10165: User self service does not respond on locale parameter in http request.
- OPENAM-10190: JWT bearer flow on OpenID failed with a server error
- OPENAM-10223: Extra / in the getEndpoint when using jwt OAuth2 flow
- OPENAM-10270: DefaultFedletAdapter should not contain methods implementation
- OPENAM-10290: OAuth2PostAuthnPlugin fails to retrieve "logoutBehaviour" and throws NPE
- OPENAM-10317: OpenAM 13.5.x openam-ui-ria does not build on Windows and Linux
- OPENAM-10322: Authorize flow with maxAge returns an error instead of the login page
- OPENAM-10332: Quota constraints exceeded - Interim Fix
- OPENAM-10333: The OAuth2 client property "id_token_signed_response_alg" affects the jwt signature check
- OPENAM-10336: oauth2/connect/register expecting a String instead of a Json for the jwks field.
- OPENAM-10353: JWKs list in Jwks_uri is only loading the "Token Signing RSA public/private key pair" certificate
- OPENAM-10380: XUI doesn't send goto parameter to /sessions/{token}?_action=logout
- OPENAM-10389: Passing an invalid SAMLResponse parameter to fedletapplication Fedlet endpoint generates a NullPointerException
- OPENAM-10390: ClientSDK no longer receives warning after upgrade from 11.x to 12.0.3
- OPENAM-10421: Unable to authenticate to XUI when username contains special characters
- OPENAM-10423: ID token signature and encryption is always using X509 certificate
- OPENAM-10425: The KID of the encrypted JWT ID token is not correct
- OPENAM-10475: Stateless JWT access token doesn't add the kid
- OPENAM-10562: Audit log 'Configuration' entries are not written when using external configuration store
- OPENAM-10614: OIDC consent page not working with HttpOnly iPlanetDirectoryPro cookie
- OPENAM-10756: setSucessModuleNames in AMLoginModule calls AuthModule's getPrincipal multiple times
- OPENAM-10800: Persistent search not automatically restarted after network disconnection to LDAP server

- OPENAM-10852: Configuration store LDAP causes authentication and psearch failures even after recovery
- OPENAM-10931: IdentitySubject not adding isMember() result to cache after entry has changed.
- OPENAM-10965: Stateless OAuth2 can't verify access and refresh token
- OPENAM-10971: FR-OATH 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

5.1.3. Key Fixes in OpenAM 13.5

The following important issues were fixed in this release:

- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-3095: When a SP sends an unsigned Authn Request using SAML ECP OpenAM sees it as a wrong message
- OPENAM-5264: Can't login to OpenAM with no cookies set in the platform service
- OPENAM-6362: HOTP and OATH auth-modules do not set 'failureUserID' when throwing InvalidPasswordException, this breaks OpenAM account lockout
- OPENAM-6878: OpenAM forgot password search hard coded for UID
- OPENAM-7002: The email attribute property defined in the email service is not used when sending e-mail in forgotten password flow
- 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-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-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-8125: IE 9/10: can't create policy resource
- OPENAM-8142: OAuth2 Access Tokens are inaccessible if the OAuth2 Client contains a space in their name

- 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-8225: Reading binary attributes, for example objectGUID, from the IdRepo cache not always returning valid values
- OPENAM-8282: Password Reset questions are not randomly chosen when resetting password
- OPENAM-9370: Configuration dialog stuck after successful configuration on weblogic

5.2. Limitations

The following limitations and workarounds are for OpenAM 13.5.2:

- **Realm Creation Not Working using Internet Explorer 11**. Realms cannot be created when using Internet Explorer 11 due to an IE scripting configuration.

  Workaround: Use another browser, such as Google Chrome, when creating realms.

The following limitations and workarounds are for OpenAM 13.5.1:

- **JCEKS Keystore Support for User Self-Services**. In OpenAM 13.0.0, OpenAM's 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 OpenAM 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 solves 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 to OpenAM 13.5.

  Note that for users of the IBM JDK on Websphere must generate their own JCEKS keystore to replace the default installation. Currently, the IBM JDK cannot load a JCEKS keystore created from a Sun/Oracle JDK on Websphere.

  For specific instructions to configure the JCEKS keystore, see "Configuring the Signing and Encryption Key Aliases" in the *Administration Guide*.

  Note

  This procedure is not necessary for the following users:

- Users upgrading from versions prior to OpenAM 13.0 are not impacted.
- Users who upgrade from OpenAM 13.0 and do not enable the user self-services feature are not impacted.
- Users who do a clean install of OpenAM 13.5.1 are not impacted.

5.3. Known Issues

5.3.1. Known Issues in OpenAM 13.5.2

The following important issues remained open when OpenAM 13.5.2 became available:

- OPENAM-11401: Access token issues via Password Grant is failing
- OPENAM-11413: XUI does not load if the parameters are not properly ordered
- OPENAM-11485: Session upgrade is not working in Chrome
- OPENAM-11565: Implicit grant flow is not generating an Ops token
- OPENAM-11624: Can't login as amadmin after session cookie domain change
- OPENAM-11822: NPE after invalid value of "The SAML2 issuer Id" in STS Instance configuration
- OPENAM-12137: Disabling audit log does not always work
- OPENAM-12223: Google social auth button doesn't redirect on first click
- OPENAM-12224: default WS-Fed configuration tab is IDP instead of general
- OPENAM-12288: Oauth2 rfc6749 - client has more than one redirection URI and the redirect_uri parameter is not set, do not inform the resource owner of an invalid_request error
- OPENAM-12302: Improve error response for Device Code flow - missing user code.
- OPENAM-12306: oauth2/authorize redirect_url missing parameter regression
- OPENAM-12310: parameters are sent as part of query string for OAuth response_mode=form_post
- OPENAM-12326: OAuth wizards allow creation of more a Service even if one already exists
- OPENAM-12380: client ip audit logging is not storing as IP but a list of IPs
- OPENAM-12542: amadmin session failover returns unauthorized on first request
- OPENAM-12544: wrong session idle time in session failover scenario

5.3.2. Known Issues in OpenAM 13.5.1

The following important issues remained open when OpenAM 13.5.1 became available:

- OPENAM-9738: Enable CTS segregation to allow each token type to write to a different CTS instance
- OPENAM-10191: Add Skew to NotOnOrAfter and NotBefore Assertion Conditions
- OPENAM-11229: OpenAM create/leaks temp files when getting large REST response
- OPENAM-11308: OAuth2 Account Mapping Failing

5.3.3. Known Issues in OpenAM 13.5

The following important issues remained open when OpenAM 13.5 became available:

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- 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-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-2911: IdP initiated SSO with persistent identifier causes URLNotFoundException: Invalid service host name.
- OPENAM-9307: Significant number of internal errors while generating access_token load
- OPENAM-9357: Upgrading to 13.x does not populate Subject Type in OAuth2Client config, causing an NPE
- OPENAM-9358: Default Microsoft Social Auth login configuration fails

Chapter 6

How to Report Problems or 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 13.5.2-15, 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

Chapter 7
Documentation Updates

The following table tracks changes to the documentation set following the release of OpenAM 13.5:

Documentation Change Log

Date	Description
2019-04-01	Added a new OAuth 2.0 access token claim, `"grant_type"`. For more information, see OpenAM 13.5.2.
2018-06-12	Initial release of OpenAM 13.5.2, which includes the following documentation updates: • Removed references to the Federation Connectivity Test, which no longer exists. • 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*. • An OAuth 2.0 provider URL, `/oauth2/customers/access_token`, was fixed in the documentation. For more information, see "OpenAM OAuth 2.0 Endpoints" in the *Administration Guide*. • Variables in the access log reference were updated. For more information, see "Access Log Format" in the *Reference*. • The OpenAM Installation Guide was updated with the removal of a section on Oracle WebLogic 11g, which is not supported. • The OpenAM Administration Guide was updated with emended text about using external log rotation tools for the audit logs. The audit logs do not support external log rotation tools. For more information, see "About the Audit Logging Service" in the *Administration Guide*. • The Release Notes were updated to show REST endpoints that were removed from OpenAM 13.5. They were incorrectly listed under the "Deprecated Functionality" section. For more information, see the "Removed Functionality" section in the OpenAM 13.5 Release Notes. • The MIB to monitor policy evaluation performance over SNMP was corrected. For more information, see "SNMP Monitoring for Policy Evaluation" in the *Administration Guide*. • The online help for Policy Configuration was updated to read:

Date	Description
	`` Make sure to place the multiple entries on a single line and separate the hostname:port URLs with a space. For example, openam.example.com|opendj.example.com:1389 opendj.example.com:2389 ``` • The diagram for CDSSO was updated with a corrected steps (20, 21, and 22). For more information, see "*Configuring Cross-Domain Single Sign-On*" in the *Administration Guide*. • A new property, `org.forgerock.policy.subject.evaluation.cache.size` was added. It controls the size of the `SubjectEvaluationCache` cache. For more information, see "Advanced" in the *Reference*. • The LDAPS Server Protocol Version property `openam-idrepo-ldapv3-config-secure-protocol-version` is no longer available. • The step to import `cts-add-multivalue.ldif` was removed from the Installation Guide. The file does not apply to this version of OpenAM. For more information, see the "Import CTS Files" in the *Installation Guide*. • The step to import `cts-add-multivalue.ldif` was removed from the Installation Guide. The file does not apply to this version of OpenAM. For more information, see the "Import CTS Files" in the *Installation Guide*. • The Release Notes were updated to show REST endpoints that were removed from OpenAM 13.5. They were incorrectly listed under the "Deprecated Functionality" section. For more information, see the "Removed Functionality" section in the OpenAM 13.5 Release Notes.
2017-07-14	Initial release of OpenAM 13.5.1, which includes the following documentation updates: • Created 13.5.1 specific sections in the Release Notes for additional information about the release. • Removed the .NET Fedlet section from the documentation. For more information, see "Important Changes to Existing Functionality". • Added the following release notes for OpenAM 13.5: • New `csrf` Parameter Requied By the `/oauth2/authorize` Endpoint • The default WS-Fed and SAML v2.0 IdP attribute mapper now support Base64-encoded binary values for NameID • Added a step to restart OpenAM or the container where it is installed when performing a silent upgrade, in "To Upgrade From a Supported OpenAM Version" in the *Upgrade Guide*. • Updated the Session Token Validation section with additional information about specifying the session token in the header. For more information, see "Validating Sessions" in the *Developer's Guide*.

Date	Description
	• Expanded information about the Profile Attribute Name property under the Adaptive Risk Authentication Module. For more information, see "Hints for the Adaptive Risk Authentication Module" in the *Administration Guide*. • Added information about `ForceAuth=true` use case when configuring the Windows Desktop SSO Authentication Module. For more information, see "Hints for the Windows Desktop SSO Authentication Module" in the *Administration Guide*. • Expanded information about implementing post-authentication plugins. For more information, see, "Post-Authentication Plugins" in the *Administration Guide*. • Added information about OpenAM requiring cookies for configured realms when using DNS aliases. For more information, see "*Configuring Realms*" in the *Administration Guide*. • Updated the information about how to create policy sets using the console to match the XUI style, and the output returned from the endpoint. For more information, see "To Configure a Policy Set Using the OpenAM Console" in the *Administration Guide* and "RESTful Authorization and Policy Management Services" in the *Developer's Guide*. • The `/oauth2/access_token` endpoint can take an additional parameter, `auth_chain=`*`authentication-chain`*. For more information, see "OAuth 2.0 Client and Resource Server Endpoints" in the *Developer's Guide*. • Updated the procedure to import the CTS schema into an external data store with steps for OpenDJ 3.5 and 4.0. For more information, see "To Import the CTS Configuration" in the *Installation Guide*. • Updated the description of the Blacklist Poll Interval property required when configuring stateless OAuth 2.0 token blacklisting. For more information, see "To Configure Stateless OAuth 2.0 Token Blacklisting" in the *Administration Guide*. • Added RFC links for OAuth 2.0 token revocation and for the JWT profile for OAuth 2.0 client authentication and authorization grants. For more information, see "*Supported Standards*" in the *Reference*. • Updated the path to the `.mib` files specified for monitoring CTS tokens using SNMP. For more information, see "Monitoring CTS Tokens" in the *Administration Guide*. • Added information about setting valid got URLs over REST. For more information, see "REST Goto URL Validation" in the *Developer's Guide*. • Updated the description of the advanced server property `com.sun.embedded.sync.servers`. For more information, see "Advanced" in the *Reference*. • The `openam.auth.soap.rest.generic.authentication.exception` advanced property was removed in OpenAM 13 with several `/identity/` endpoints but was still mentioned in the *OpenAM Administration Guide*. This mention has been removed.

Date	Description
	• Added information about the way OpenAM determines the redirection URL, basing the decision on authentication success or failure. For more information, see "Redirection URL Precedence" in the *Administration Guide*. • Added a list of endpoints deprecated in OpenAM 13.5 release that were incorrectly flagged as removed in OpenAM 13. For more information, see OpenAM 13.5.0. • Updated information about usage of post-authentication plugins. For more information, see "Configuring Your Post Authentication Plugin" in the *Developer's Guide*. • User self-registration flow was updated in 13.5.1. For more information about the new flow using the REST APIs, see "To Register a User with the REST APIs (13.5.1 or later)" in the *Developer's Guide*.
2016-11-21	OpenAM 13.5.0 documentation refresh 1, which includes the following updates: • Revised and clarified "To Set Up Administration Tools" in the *Installation Guide*. • Corrected the example Elasticsearch index in "To Prepare for Elasticsearch Audit Logging" in the *Administration Guide*. Elasticsearch indexes must be all lower case, and the example had an index with some upper case characters. • Corrected the description of the Mobile Carrier Attribute Name in "Hints for the HOTP Authentication Module" in the *Administration Guide*. • Added a new section, "Managing Scripts With the ssoadm Command" in the *Administration Guide*, which provides **ssoadm** command examples of script management. • Revised "Preparing Oracle WebLogic" in the *Installation Guide*, to provide additional guidance for deploying OpenAM into WebLogic and removed outdated information. There is now a new section with steps to perform before deploying OpenAM in WebLogic. • Modified example paths in "To Prepare an External OpenDJ Identity Repository With Manual Schema Updates" in the *Installation Guide* that could lead to confusion. • Corrected the example SSL connector in "To Set Up OpenAM With HTTPS and Self-Signed Certificates" in the *Administration Guide* to add the `keystoreType` property and to update the `protocol` property to the default used by Apache Tomcat8.x. • Corrected and clarified the steps to change the `amadmin` user's password in "Administering the amadmin Account" in the *Administration Guide*. The section now contains a procedure to change the `amadmin` user's password when the configuration store is in the embedded OpenDJ server, and another procedure to change the password when the configuration store is in an external OpenDJ server.

Date	Description
	• Revised "*Managing Certificates and Keystores*" in the *Administration Guide* to provide more information about key aliases and keystores in OpenAM. Added new procedures to configure the keystore and to change the user self-service key aliases. The procedure to change the signing key is also updated. • Updated the documentation set to reflect that OpenAM 13.5 defaults to JCEKS keystore instead of to JKS keystore. • Revised and clarified "*Backing Up and Restoring OpenAM Configurations*" in the *Administration Guide*. • Updated "*Localization*" in the *Reference* to include XUI localization support information. • Updated the file descriptor section with some additional instructions for daemon processes. See "Setting Maximum File Descriptors" in the *Installation Guide*. • Updated the Configuring the Core Token Service with small fixes to the instructions in "*Configuring the Core Token Service*" in the *Installation Guide*. • Updated the list of distribution files in the OpenAM Deployment Planning Guide in "OpenAM Server Overview" in the *Deployment Planning Guide*. • Removed the `com.sun.am.event.connection.idle.timeout` from the OpenAM Reference Guide. • Added a link to create a configuration store backend in "To Custom Configure OpenAM" in the *Installation Guide*. • Added ability to use UTF-8 encoded user names and passwords during REST authentication. See "Authentication and Logout" in the *Developer's Guide*. • Added Microsoft Edge to the list of supported browsers, and changed references in the documentation from "Internet Explorer" to "Internet Explorer and Microsoft Edge." • Revised the chapter on CTS OIDs to include the OIDs' data types, and corrected several entries in the CTS OIDs diagram. See "*Core Token Service (CTS) Object Identifiers*" in the *Reference*. • Updated Active Directory Hints section to indicate that `cn` gets its value from the `uid` or `username` and `sn` gets its value from `givenName` in "Hints for Configuring Active Directory Data Stores" in the *Administration Guide*. • Updated the HMAC One-Time-Password (HOTP) hints with a note about configuring login page session timeouts in "Hints for the HOTP Authentication Module" in the *Administration Guide*. • Updated the information on cookie domain values, which can now be empty strings for host-only cookies or any non-top level domain in "Preparing a Fully Qualified Domain Name" in the *Installation Guide*.
2016-07-20	Initial release of OpenAM 13.5.0.

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/.