Release Notes

OpenAM 10.1

Mark Craig
VanessaRichie

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

Chapter 1
What's New in OpenAM 10.1.0

> **Important**
>
> On February 8, 2014 OpenAM 10.1.0 reached End of Service Life (EOSL).
>
> ForgeRock customers must upgrade their OpenAM in order to receive continued support.

OpenAM 10.1.0 fixes a number of issues, and provides the following additional features.

> **Important**
>
> OpenAM 10.1.0 is a milestone release from the main development branch of the product. The Xpress release contains selected key features and all current fixed issues. An Xpress release undergoes important functional testing but not the complete testing cycle that is done for a full Enterprise release.
>
> Xpress releases are supported through ForgeRock subscriptions and are upgradeable to the Enterprise version, which has long term support.
>
> The goal of an Xpress release is to enable you to start build phases earlier, with the most recent features, instead of having to wait for the Enterprise release date. Fixes to issues that are discovered in an Xpress release are delivered as patches to ForgeRock customers, and are guaranteed to be delivered in the Enterprise release that follows. Xpress releases are supported for a grace period after the Enterprise version has been released.
>
> With the exception of these Release Notes, the official documentation for this release is still in progress.

Major New Features

- OpenAM now provides further support for OAuth 2.0. In addition to playing the role of client and resource server, OpenAM can now also play the role of OAuth 2.0 authorization server. See *Managing OAuth 2.0 Authorization* in the *Administration Guide* for explanations, instructions, and examples.
- Session failover has been modified to be simpler to deploy (OPENAM-625). OpenAM 10.0.1 and earlier required the use of Open Message Queue and Berkeley DB Java Edition, which increased the complexity and amount of time required to get session failover working. OpenAM now writes session data to the configuration data store instead. This implementation also can be used to make sessions persist across restart for single OpenAM servers. The current implementation requires that you use OpenDJ for the configuration data store.

  This new implementation is designed to operate on a local site network. Cross-site session failover and session failover across wide area networks (WANs) are not supported.

- IBM® WebSphere® 8.0 is now a supported platform. See *Preparing IBM WebSphere* in the *Installation Guide* in the *Installation Guide* for details on how to setup WebSphere 8.0 and 8.5 before deploying OpenAM.
- Legacy naming conventions have been changed to conform to the current product name, OpenAM. This includes the OpenAM bootstrap file (OPENAM-1555). `$HOME/.openamcfg/` is the new name for `$HOME/.openssocfg/`. If you upgrade, OpenAM still supports use of `$HOME/.openssocfg/`, and does not rename the folder. For new OpenAM installs, OpenAM creates the directory with the new name, `$HOME/.openamcfg/`, at configuration time. Other files, such as the `openam.war` file, and paths have been modified to ensure consistency with the naming conventions.
- OpenAM now supports Open Authentication (OPENAM-727). The module provides the user with a one-time password based either on a HMAC one-time password or a time-based one-time password. OATH lets you determine which type of one-time password is best for your users when they need to login with a password generating device. Devices can range from a smartphone to a dedicated device, such as YubiKey or any other OATH compliant device.

  With OATH, OpenAM now supports YubiKey® authentication. The YubiKey simplifies the process of logging in with a One Time Password token as it does not require the user to re-type long pass codes from a display device into the login field of the computer. The YubiKey is inserted in the USB-port of any computer and the OTP is generated and automatically entered with a simple touch of a button on the YubiKey, and without the need of any client software or drivers.

Additional New Features

- OpenAM now provides an account expiration post authentication plugin to set an account expiration date on successful login.
- OpenAM now bundles OpenDJ 2.4.6 (OPENAM-1954).
- The AMLoginModule now lets authentication modules retrieve the list of current session tokens for a user (OPENAM-1721).
- OpenAM's IDPAdapter now provides additional hooks for customization. This improvement introduces changes to the API that affect custom IDPAdapters (OPENAM-1623).
- When running as a Service Provider, OpenAM no longer requires that you enable module-based authentication (OPENAM-1470).
- OpenAM now has better support for using a reverse proxy for federation when DAS is also deployed (OPENAM-1454).
- OpenAM now allows use of a read-only data store with a non-transient NameID during SAML 2.0 federation (OPENAM-1427).
- The ssoadm command now includes a get-sub-cfg subcommand (OPENAM-1348).
- The REST authenticate command now has a parameter to specify the client IP address (OPENAM-1048).

- OpenAM is now built with Maven. Maven artifacts continue to be uploaded to the ForgeRock Maven repository (OPENAM-739).
- You can now prevent OpenAM from caching subject evaluations for policy decisions (part of the fix for OPENAM-24).

  In most cases you do not need to turn off caching, as OpenAM now clears cache when group membership changes. Before turning off caching in production, first test the setting to ensure that the performance impact is acceptable for your deployment.

  To turn off caching, set Access Control > *Realm Name* > Services > Policy Configuration > Subjects Result Time to Live to 0. The equivalent **ssoadm** property for the `iPlanetAMPolicyConfigService` is `iplanet-am-policy-config-subjects-result-ttl`.

Chapter 2

Before You Install OpenAM 10.1.0 Software

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

2.1. Java Requirements

This release of OpenAM requires Java Development Kit 1.6, at least 1.6.0_10. ForgeRock recommends the most recent release of Java 6 to ensure you have the latest security fixes.

ForgeRock has tested this release of OpenAM primarily with Oracle Java SE JDK.

OpenAM Java SDK requires Java Development Kit 1.5 or 1.6.

2.2. Web Application Container Requirements

This release of OpenAM runs in the following web application containers.

- Apache Tomcat 6.0.x, 7.0.x (ForgeRock's preferred web container for OpenAM)
- GlassFish v2
- IBM WebSphere 8.0, 8.5
- JBoss Enterprise Application Platform 4.x, 5.x

  JBoss Application Server 7.x
- Oracle WebLogic Server 11g (10.3.5)

  Oracle WebLogic Server 12c (12.1.1)

If running as a non-root user, the web application container must be able to write to its own home directory, where OpenAM stores configuration files.

2.3. Data Store Requirements

This release of OpenAM works with the following configuration data stores.

- Embedded (using ForgeRock OpenDJ for the data store)

  When using the embedded configuration store, you must deploy OpenAM on a local file system and not on an NFS-mounted file system.

- External ForgeRock OpenDJ data store

  ForgeRock recommends updating to the latest stable release.

- External Sun OpenDS data store, version 2 or later

- External Oracle Directory Server Enterprise Edition data store, version 6.3 or later

This release of OpenAM works with the following user profile data stores.

- ForgeRock OpenDJ

- Microsoft Active Directory (tested by ForgeRock on Windows Server 2008 R2)

- IBM Tivoli Directory Server 6.3

- OpenDS, version 2 or later

- Oracle Directory Server Enterprise Edition, version 6.3 or later

OpenAM also works with other LDAPv3 compliant directory servers. Some features of OpenAM depend on features supported by your directory service, such as the following:

- Extensible LDAP schema, required to extend the schema for OpenAM. First, install OpenAM to use a fresh instance of OpenDJ, such as the embedded OpenDJ server. After installation, study the custom schema definitions from the OpenDJ file, `config/schema/99-user.ldif`, to see what schema definitions you must add to your directory. You might need to adapt the schema definition format before adding the definitions to your directory.

- The persistent search request control (OID: `2.16.840.1.113730.3.4.3`).

- The Behera Internet-Draft Password Policy for LDAP Directories (in the context of the LDAP authentication module only)

If you plan to deploy with OpenLDAP or other LDAPv3 directory for user data, make sure you test your solution before you deploy to ensure all OpenAM features that you use work as expected.

2.4. Browsers Tested

ForgeRock has tested many browsers with OpenAM console and end user pages, including the following browsers.

- Chrome and Chromium 16 and later

- Firefox 3.6 and later
- Internet Explorer 7 and later
- Safari 5 and later

2.5. Platform Requirements

ForgeRock has tested this release of OpenAM on the following platforms.

- Linux 2.6, 3.0
- Microsoft Windows Server 2003, 2008 R2
- Oracle Solaris 10

2.6. Hardware Requirements

You can deploy OpenAM on any hardware supported for the combination of software required. Deploying OpenAM requires a minimum of 1 GB free RAM over and above the RAM used by all other software on the system.

Minimum requirements are enough to start and to evaluate OpenAM. Recommended hardware resources depend on your specific deployment requirements. For more information, see the *Administration Guide* chapter on *Tuning OpenAM* in the *Administration Guide*.

ForgeRock has tested this release of OpenAM primarily on x86 and x64 based systems.

2.7. Special Requests

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

Chapter 3
OpenAM Changes & Deprecated Functionality

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

3.1. Major Changes to Existing Functionality

- When you create a new OpenAM custom configuration that uses an external LDAP directory server for the configuration data store, you must use a root suffix DN with at least two domain components, such as `dc=example,dc=com`.

- Legacy naming conventions have been changed to conform to the current product name, OpenAM.

  `$HOME/.openamcfg/` is the new name for `$HOME/.openssocfg/`. If you upgrade, OpenAM still supports use of `$HOME/.openssocfg/`, and does not rename the folder. For new OpenAM installs, OpenAM creates the directory with the new name, `$HOME/.openamcfg/`, at configuration time.

  Other files, such as the `openam.war` file, and paths have been modified to ensure consistency with the naming conventions.

- OpenAM now ships with multiple .war files. You no longer have to build custom .war files for core server-only or distributed authentication UI installations for example.

- In earlier versions the default root suffix DN for OpenAM configuration and profile data was `dc=opensso,dc=java,dc=net`. The default root suffix is now `dc=openam,dc=forgerock,dc=org`.

3.2. Deprecated Functionality

The following functionality is deprecated in OpenAM 10.1.0, and is likely to be removed in a future release.

- With the implementation of OAuth 2.0 in this release, OAuth 1.0 has been deprecated. OAuth 1.0 support was originally provided in OpenAM 9.

- The Netscape LDAP API is to be removed from OpenAM, with OpenAM using the OpenDJ LDAP SDK instead. This affects all classes in `com.sun.identity.shared.ldap.*` packages.

- OpenAM currently uses Sun Java System Application Framework (JATO). JATO is deprecated and is likely to be replaced in a future release.

3.3. Removed Functionality

- For OpenAM 10.1.0, the use of the previous session failover implementation has been removed.
- With the updated session failover, SAML 2 and session persistence have changed. The methods used prior to OpenAM 10.1.0 are no longer available.
- Support for Liberty Identity Web Services Framework (ID-WSF) has been removed.

Chapter 4
OpenAM Fixes, Limitations, & Known Issues

OpenAM issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM. This chapter covers the status of key issues and limitations at release 10.1.0.

4.1. Key Fixes

The following bugs were fixed in release 10.1.0. For details, see the OpenAM issue tracker.

- OPENAM-1922: DAS doesn't handle a 302 from OpenAM
- OPENAM-1873: Auth module error messages can get lost
- OPENAM-1863: PLLRequestServlet should set Content-Length header on the response
- OPENAM-1858: Federated authentication does not clear authentication state when initiating authn multiple times
- OPENAM-1819: "IDP Session is NULL" when logging in to two different OpenAM servers within an IDP site configuration
- OPENAM-1788: Create-agent command always requires serverurl and agenturl properties
- OPENAM-1787: ConnectionPool related issues when using LDAP authentication module
- OPENAM-1779: REST interface should always set Cache-Control headers to prevent caching
- OPENAM-1736: NullPointerException causes TimerPool thread to fail
- OPENAM-1703: SP Single Logout Init returns HTTP 400 when no local session exists
- OPENAM-1696: Data code for AD_ACCOUNT_DISABLED is wrong
- OPENAM-1622: Remote Session validation can lead to heap accumulation
- OPENAM-1546: Logout/Idle Timeout does not clear Restricted Token Session objects if multiple Policy Agents are in use
- OPENAM-1545: Container shutdown might hang when using SFO
- OPENAM-1515: Possibility that LB Cookie is not set

- OPENAM-1514: NullPointerException thrown if 'refresh' parameter is missing from 'attributes' SOAP call
- OPENAM-1439: Update *_ja.properties
- OPENAM-1438: Multiple failing null-callback sufficient modules can result in NPE
- OPENAM-1371: Server Debug level not hot-swappable in Console
- OPENAM-1364: During Session Failover, when an IDPSessionCopy is retrieved from the DB it is missing the NameID values that were saved after authentication.
- OPENAM-1356: Login pages submits form twice on IE
- OPENAM-1347: Multiple tabs setting not listed in validserverconfig
- OPENAM-1346: Saving WS-Fed IdP properties loses entity configuration data
- OPENAM-1342: Changing WS-Federation entity properties causes federation to fail with 403 error
- OPENAM-1340: ForceAuth results in NPE
- OPENAM-1333: SAML2 does not set content type when using HTTP-POST binding
- OPENAM-1329: EntitlementException locale files missing from ClientSDK
- OPENAM-1316: Size/time limit exceeded message typo
- OPENAM-1315: The IDPSSOUtil.getIDPAdapterClass call does not cater for an empty value coming from metadata lookup resulting in ClassNotFound exceptions in debug logs.
- OPENAM-1283: OpenAM does not return adequate SOAP faults during ArtifactResolution
- OPENAM-1261: Upgrade fails if .configParam file is missing
- OPENAM-1252: ssoadm loses exception causes
- OPENAM-1247: Password Reset service does not work in server-only deployment
- OPENAM-1246: More than 5 referral policies under a realm would hang PrivilegeEvaluator
- OPENAM-1226: JAX RPC calls generating "java.lang.InternalError: fillbuf: errors in OpenAM container log
- OPENAM-1221: WSSAgent can not sign request if security mechanism 'X509Token' and Signing Reference Type 'KeyIdentifier Reference' is configured in Web Service Client profile
- OPENAM-1205: Missing SAML2Exception handler in spAssertionConsumer.jsp means a 500 error page is shown rather than the configured OpenAM SAML error page.
- OPENAM-1133: SAML2 Entity import does not support EntityDescriptor elements contained in an EntitiesDescriptor element

- OPENAM-1108: DAUI does not get client IP address when behind proxying load balancers
- OPENAM-1007: Memory Leak in SMSNotificationManager when ldap error occurs
- OPENAM-995: using UTF-8 characters in policy names breaks the policy console
- OPENAM-972: Remote Session accumulates via CDCServlet
- OPENAM-808: OpenAM instances hung when starting at the same time.
- OPENAM-746: CDCServlet should only compute TokenRestriction if cookie hijacking prevention is configured
- OPENAM-732: encode issue in CDCServlet if url contains blank
- OPENAM-670: Entitlement evaluation throws org.json.JSONException when evaluating entitlements with resource attributes
- OPENAM-24: Identity Changes not propagating to policy decisions

4.2. Limitations

Some items present in earlier releases of OpenAM are not included in the new OpenAM distribution for this Xpress release.

- Policy agent C SDK libraries and samples are not delivered in this Xpress release (OPENAM-1709). Only the Java SDK library, `openam-clientsdk-10.1.0-Xpress.jar`, is part of this Xpress release.

  As a result the following chapters are not correct with respect to the Xpress release.

  - *Installing OpenAM Client SDK Samples* in the *Installation Guide* in the *Installation Guide*
  - *Using the OpenAM Java SDK* in the *Developer's Guide* in the *Developer's Guide*
  - *Handling Single Sign On Using OpenAM Java SDK* in the *Developer's Guide* in the *Developer's Guide*
  - *Requesting Policy Decisions Using OpenAM Java SDK* in the *Developer's Guide* in the *Developer's Guide*
  - *Using Secure Attribute Exchange* in the *Developer's Guide* in the *Developer's Guide*
  - *Using the OpenAM C API* in the *Developer's Guide* in the *Developer's Guide*
- The IDP discovery .war is not delivered in this Xpress release (OPENAM-1936).
- Resources for integrating OpenAM with third-party access and identity management software are not delivered with the distribution.

- Javadoc is no longer delivered with the distribution, but is available online.

Creating a user by sending an HTTP POST of the JSON representation of the user to `/json/users/?_action=create` is not supported in this Xpress release.

Deleting a user by sending an HTTP DELETE to `/json/users/user-id` is not supported in this Xpress release.

If you create a new realm, you must restart OpenAM before using the new identity management REST API to manage identities under the new realm. When you try to access users in the new realm before restarting OpenAM, OpenAM returns HTTP 404 Not found errors, even for users who exist.

When session failover is configured to use external OpenDJ directory servers, OpenAM must access those directory servers through an LDAP load balancer that can fail over connections from OpenAM whenever a directory server goes offline. Otherwise, sessions could continue to persist after users logout of OpenAM.

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

Not all features of OpenAM work with IPv6.

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

By default OpenAM does not enforce session quotas when running in Site mode without session failover. To work around this behavior, set the server configuration property `openam.session.useLocalSessionsInMultiServerMode=true`. You can set this property in OpenAM console under Configuration > Servers and Sites > Servers > Server Name > Advanced.

4.3. Known Issues

The following important known issues remained open at the time release 10.1.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-2189: configuration failing with message ".../opt/openam is a directory"
- OPENAM-2183: Install of AM in WebLogic 12c container fails extracting OpenDJ files
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2167: Oracle iPlanet Web Server policy agent install instructions incorrect
- OPENAM-2154: cert-auth module does not succeed if CRL update fails
- OPENAM-2153: cert-auth module does not allow to disable CRL in-memory cache
- OPENAM-2152: cert-auth module does not allow storage of several CRLs for the same issuer
- OPENAM-2145: Memory leak in J2EE Agent 3.1.0-Xpress

- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2117: ssoadm create-agent command should not require serverurl/agenturl for web/j2ee agents
- OPENAM-2110: Upgrade fails if external configstore is using non-default user
- OPENAM-2097: Adaptive risk module does not describe which GeoIP client is used and where to obtain the GeoIP database file
- OPENAM-2085: Policy evaluation is inconsistent when several policies have mutually exclusive conditions of certain types
- OPENAM-2064: Missing forgerock-am-dashboard-service attribute to provision new Subject to non OpenDJ external user store
- OPENAM-2059: ssoadm export-svc-cfg throws NullPointerExecption if no SubConfiguration exists for a given service
- OPENAM-2050: URL Encoding the Redirect URI for the OAuth2 provider for OpenAM
- OPENAM-2023: Federation Connectivity Test fails with Account termination is not working
- OPENAM-1964: Performance issues when using AMIdentitySubject with groups
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1921: REST GET for user "*" returning first user listed
- OPENAM-1906: Common REST returning 404 when retrieving users from realms
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1852: Oauth2 auth-module can not be used with DistAuth
- OPENAM-1839: LDAPConnectionPool is not recovered
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1811: DAS response serialization is not working as expected when using PAP
- OPENAM-1739: HOTP module may ignore SMTP settings in the configuration
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1659: Default Authentication Locale is not used as fallback

- OPENAM-1642: Chain based UI customization is not case insensitive
- OPENAM-1630: SAML metadata signature code does not conform to SAML recommendations
- OPENAM-1563: Servers and Sites pages may display password in clear text
- OPENAM-1517: Inconsistency in getting Client IP
- OPENAM-1512: LDAPConnectionPool is not re-initialized correctly if failover server is down
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1496: People container name/value configs are not always correctly used
- OPENAM-1330: 'sharedState' in LoginContext should be thread safe
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents
- OPENAM-1269: Entitlements are incorrectly converted to policies
- OPENAM-1237: Property 'noSubjectKeyIdentifier' is missing in fmWSSecurity.properties
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1180: Login URL problems when using Federation
- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled
- OPENAM-1109: AdminTokenAction doesn't clear invalid SSOToken
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1083: Using Federation redirects with the valid goto URL whitelist causes problems
- OPENAM-1012: IDP initiated SAML2 SLO error when SP does not have SLO binding
- OPENAM-973: LDAPConnectionPool#decreaseCurrentConnection() could throw ArrayIndexOutOfBound exception
- OPENAM-774: Invalid characters check not performed.

- OPENAM-752: AgentsRepo#getAttributes fails to get agent information occasionally leading to server restart
- OPENAM-651: internalsession object can grow in size leading to non-linear scaling in the session failover db
- OPENAM-401: Missing response attribute on first logon after OpenAM restart
- OPENAM-294: ssoadm: create and update
- OPENAM-291: SelfWrite permissions are denied to sub realms
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings

Chapter 5
How to Report Problems & Provide Feedback

If you have found issues or reproducible bugs within OpenAM 10.1.0, 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 6
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/.