OpenAM 10.0.1 Release Notes

Mark Craig

Software release date: December 13, 2012

Publication date: December 13, 2012

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 in OpenAM 10.0.1 1
2. Before You Install OpenAM Software 3
3. Updating & Installing OpenAM 7
4. OpenAM Changes & Deprecated Functionality 9
5. OpenAM Fixes, Limitations, & Known Issues 11
6. How to Report Problems & Provide Feedback 15
7. Support 17

Chapter 1. What's New in OpenAM 10.0.1

OpenAM 10.0.1 is a maintenance release that resolves a number of issues, including security issues in OpenAM. It is strongly recommended that you update to this release to make your deployment more secure, and to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

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

- If you have already installed OpenAM, see *To Update From OpenAM 10.0.0*.
- If you are installing OpenAM for the first time, see *To Install OpenAM*.

1.1. Product Enhancements

In addition to fixes, this release includes the following limited product enhancements.

- OPENAM-1721: New method in AMLoginModule to allow customers to determine other user sessions
- OPENAM-1470: Running OpenAM as an SP should not require enabling module based auth
- OPENAM-1454: Improve RP support for federation when using DAS
- OPENAM-1348: Implement get-sub-cfg ssoadm command
- OPENAM-1266: Configure option in OpenAM IDP to Proxy all the requests, regardless if the SP allows or not.
- OPENAM-1048: Add client parameter to REST authenticate command

1.2. OpenAM Documentation

You can read the following additional product documentation for OpenAM 10.0 online at docs.forgerock.org

- OpenAM 10.0.0 Release Notes
- OpenAM 10.0.0 Installation Guide
- OpenAM 10.0.0 Administration Guide
- OpenAM 10.0.0 Developer's Guide

- OpenAM 10.0.0 Reference
- OpenAM 10.0.0 Javadoc

Chapter 2. Before You Install OpenAM Software

This chapter covers software and hardware prerequisites for installing and running OpenAM software. If you have a special request to support a component or combination not listed here, contact ForgeRock at info@forgerock.com.

Note

The content of this chapter has not changed since OpenAM 10.0.0.

2.1. Java Requirements

This release of OpenAM requires Java Development Kit 1.6, at least 1.6.0_10. ForgeRock recommends that you use at least version 1.6.0_27 due to 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
- GlassFish v2
- JBoss Enterprise Application Platform 4.x, 5.x

  JBoss Application Server 7.x
- Jetty 7
- Oracle WebLogic Server 11g

  Oracle WebLogic Server 12c

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 2.4.5 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
- External Sun OpenDS data store
- External Oracle Directory Server Enterprise Edition data store

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

- ForgeRock OpenDJ
- Microsoft Active Directory
- IBM Tivoli Directory Server
- OpenDS
- Oracle Directory Server Enterprise Edition

OpenAM also works with OpenLDAP and 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 (for OpenAM password reset, for example)

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
- 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.

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

Chapter 3. Updating & Installing OpenAM

ForgeRock recommends that you update OpenAM 10.0.0 installations to this release. If you are installing OpenAM for the first time, you can use the same installation instructions as for 10.0.0.

Procedure 3.1. To Update From OpenAM 10.0.0

If you have already installed OpenAM, follow these steps.

1. Download and unzip OpenAM 10.0.1.

   The download page is http://forgerock.org/openam.html.

2. If you have made any customizations, apply them to the 10.0.1 .war file.

3. Redeploy the .war file to your web container, using the web container administration console or deployment command.

   If you are using session failover, do not yet restart OpenAM.

4. If you are using session failover, you must ensure the session failover database is cleared as part of the update to OpenAM. OpenAM's internal representation of session objects has changed in this release. The session failover database must be restarted before starting the updated OpenAM.

   To clear OpenMQ, run **amsfo stop** and then run **amsfo start**.

5. Start OpenAM, and run the upgrade process for the server.

Procedure 3.2. To Install OpenAM

If you have not yet installed OpenAM, install this release instead of OpenAM 10.0.0.

1. Download and unzip OpenAM 10.0.1.

   The download page is http://forgerock.org/openam.html.

2. Follow the instructions in the *OpenAM 10.0.0 Installation Guide*.

Chapter 4. OpenAM Changes & Deprecated Functionality

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

Note

The content of this chapter has not changed since OpenAM 10.0.0.

4.1. Major Changes to Existing Functionality

- The following web policy agents are compatible with OpenAM 10.0.1.
  - Apache 2.0
  - Apache 2.2
  - Microsoft IIS 6
  - Microsoft IIS 7

  The following J2EE policy agents are compatible with OpenAM 10.0.1.
  - GlassFish v2 & v3
  - JBoss v4.2 & v5.x
  - Jetty v6.1 & v7
  - Tomcat v6
  - WebSphere v6.1
  - WebLogic v10
- Prior to OpenAM 9.5.2, trailing slashes (`/`) were ignored when matching resource names in policy evaluation. Therefore, `/-*-` matched `/secret`, but also `/secret/`, short for `/secret/index.html` on most web servers.

  Now, `/-*-` matches `/secret`, but not `/secret/`.
- Since OpenAM 9.5.3, application shutdown hooks are no longer registered by default. This change only has an effect on standalone and web applications that use the OpenAM Client SDK. The changes do not affect OpenAM, distributed authentication services, or the Java EE policy agents.

For Java EE applications, ensure the OpenAM client SDK shuts down successfully by including the following context listener in your application's `web.xml` file.

```
<listener>
 <listener-class>
  com.sun.identity.common.ShutdownServletContextListener
 </listener-class>
</listener>
```

For standalone applications, set the following JVM property.

```
-Dopenam.runtime.shutdown.hook.enabled=true
```

4.2. Deprecated Functionality

The following functionality is deprecated in OpenAM 10.0.1.

- 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.
- Support for Liberty Identity Web Services Framework (ID-WSF) is deprecated. The functionality is likely to be removed in a future release.
- OpenAM currently uses Sun Java System Application Framework (JATO). JATO is deprecated and is likely to be replaced in a future release.

4.3. Removed Functionality

OpenAM 10.0.1 does not include the **amtune** command.

OpenAM console only mode is no longer supported. Console only mode is likely to be replaced with a different solution in a future release.

The Test Beta Console has been removed. Its functionality is currently available through the **ssoadm** command.

OpenAM no longer includes the SafeWord and Unix authentication modules.

Chapter 5. 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 10.0.1.

5.1. Fixes

The following issues were fixed in release 10.0.1.

- 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-1544: Request headers are not proxied for GET requests

- OPENAM-1515: Possibility that LB Cookie is not set
- OPENAM-1514: NullPointerException thrown if 'refresh' parameter is missing from 'attributes' SOAP call
- OPENAM-1478: OpenAM installation console does not populate the port on second installation. Showing value of "null"
- 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-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-1326: Deadlock in PeriodicRunnable (side effect of OPENSSO-5377)
- 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-1307: Goto validation not carried out on Logout if there is no SSO session
- OPENAM-1285: Incorrect JAVA EE API usage in FileUpload.jsp
- OPENAM-1283: OpenAM does not return adequate SOAP faults during ArtifactResolution
- OPENAM-1280: Persistent cookies only works when debug is at Message Level
- OPENAM-1261: Upgrade fails if .configParam file is missing

- OPENAM-1252: ssoadm loses exception causes
- OPENAM-1246: More than 5 referral policies under a realm would hang PrivilegeEvaluator
- OPENAM-1241: Upgrade fails due to ArrayOutOfBoundsException
- 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-1168: Rest/SOAP interface no longer returns the error message for cases where a HTTP 401 is generated
- OPENAM-1108: DAUI does not get client IP address when behind proxying load balancers
- OPENAM-1083: Using Federation redirects with the valid goto URL whitelist causes problems
- OPENAM-1007: Memory Leak in SMSNotificationManager when ldap error occurs
- 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-507: Adding to existing deployment fails for non-default Org. Auth. configuration
- OPENAM-24: Identity Changes not propagating to policy decisions

5.2. Limitations

Note

The content of this section has not changed since OpenAM 10.0.0.

ForgeRock supports the stable software releases that you can download from ForgeRock, not nightly builds or pre-release software. ForgeRock OpenAM downloads do not include OpenAM extensions. Therefore, ForgeRock

does not support OpenAM extensions. If you have a special request for capabilities not currently in a software release, contact ForgeRock at info@forgerock.com.

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, the REST and SOAP APIs return different responses depending on whether the user name provided is valid or invalid. This behavior could allow an attacker to build list of valid user names, after which only passwords would be required to gain access to user account details. To prevent this risk, set the server configuration property `openam.auth.soap.rest.generic.authentication.exception=true`. You can set this property in OpenAM console under Configuration > Servers and Sites > Servers > Server Name > Advanced.

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.

5.3. Known Issues

OpenAM 10.0.1 has a number of outstanding issues that have been noted in the OpenAM bug tracker. Check https://bugster.forgerock.org/jira/browse/OPENAM for the latest list of issues.

Chapter 6. How to Report Problems & Provide Feedback

Note

The content of this chapter has not changed since OpenAM 10.0.0.

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 10.0.1, 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
- Machine type, operating system version, web container and version, Java version, and OpenAM release version, including 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. Support

Note

The content of this chapter has not changed since OpenAM 10.0.0.

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://www.forgerock.com/partners.html.