OpenAM 10.0.2 Release Notes

Mark Craig

Software release date: December 16, 2013

Publication date: December 10, 2013

Copyright © 2011-2013 ForgeRock AS

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 10.0.2

OpenAM 10.0.2 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.

- The changes for OPENAM-3330 and OPENAM-3353 affect the service configuration LDAP and Active Directory authentication modules.

  The `iplanet-am-auth-ldap-server-check` property has been removed.

  The following properties have been added:

  `openam-auth-ldap-heartbeat-interval`
      LDAP Connection Heartbeat Interval

  `openam-auth-ldap-heartbeat-timeunit`
      LDAP Connection Heartbeat Time Unit

  `openam-auth-ldap-operation-timeout`
      Timeout setting for requests to the directory service

- OPENAM-3190: IdP Adapter should have an extension point that can manipulate the SAML response, and OPENAM-1623: Improve the IDPAdapter functionality

  OpenAM's IDPAdapter now provides additional hooks for customization. This improvement introduces changes to the API that affect custom IDPAdapters.

- OPENAM-2767: The default IDP attribute mapper should provide a way to Base64 encode binary attributes

In order to have the default IDP attribute mapper Base64 encode binary attributes when adding them to the SAML attributes, use the `;binary` postfix for the attribute name, as in the following example:

```
objectGUID=objectGUID;binary
```

This maps the local binary attribute `objectGUID` to a SAML attribute called `objectGUID` that is Base64 encoded.

The default IDP attribute mapper also supports NameFormat URI format as shown in the following example:

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri|objectGUID=objectGUID;binary
```

- OPENAM-2765: DirectoryManagerImpl, IdRepoJAXRPCObjectImpl and SMSJAXRPCObjectImpl should return cluster unique IDs when registering notification URLs

- OPENAM-2604: Password reset should have configurable mail attribute

- OPENAM-2580: Allow DAS on JBoss to find its configuration after a restart

The Distributed Authentication UI (DAS) now supports a new JVM property that indicates the location of the DAS configuration file. This is useful for containers such as JBoss that change the file system location of the content unpacked from the .war file. Set the JVM property as in the following example:

```
openam.das.bootstrap.file=/home/openam/das/AMDistAuthConfig.properties
```

- OPENAM-2425: OAuth2 Consumer needs the name of the parameter to hold the value of the token when accessing the profile service

- OPENAM-2354: Zero Page Login should be configurable

This change automatically disables Zero Page Login with GET requests to prevent user credentials from being logged in access log files. To enable Zero Page Login, in OpenAM Console brows to Access Control > *Realm Name* > Authentication > All Core Settings, and then enable "Zero Page Login".

For the Distributed Authentication UI (DAS), set the following property in the configuration file:

```
openam.auth.zero.page.login.enabled=true
```

- OPENAM-2184: Provide a mechanism to supply static attribute values in IDP and SP SAML2 attribute mappings

The default IDP mapping implementation allows you to add static values in addition to values taken from the user profile. You add a static value by enclosing the profile attribute name in double quotes ("), as in the following example.

To add a static SAML attribute called `nameID` with a value of `staticNameIDValue` with a name format of `urn:oasis:names:tc:SAML:2.0:attrname-format:uri`, add the following mapping.

```
urn:oasis:names:tc:SAML:2.0:attrname-format:uri|nameID="staticNameIDValue"
```

• OPENAM-1749: AttributeQueryUtil.getAttributeMapForFedlet eats non-Success StatusCode from IDP

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 10.0.2.

    Find a link to the OpenAM download page from http://forgerock.com/download-stack/.

2. If you have made any customizations, apply them to the 10.0.2 .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. Skip this step if you are not using session failover, or if you are upgrading from OpenAM 9.5.5 or OpenAM 10.0.1.

    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.

6. If you have deployed other components, such as the Distributed Authentication UI (DAS), Core Server only (no console), or the **ssoadm** command, also update those components.

Procedure 3.2. To Install OpenAM

If you have not yet installed OpenAM, install this release instead of OpenAM 10.0.0 or 10.0.1.

1. Download and unzip OpenAM 10.0.2.

    Find a link to the OpenAM download page from http://forgerock.com/download-stack/.

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 10.0.2.

  - Apache 2.0

  - Apache 2.2

  - Microsoft IIS 6

  - Microsoft IIS 7

  The following J2EE policy agents are compatible with OpenAM 10.0.2.

  - 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 10.0.2.

- 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 10.0.2 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 10.0.2.

5.1. Fixes

The following issues were fixed in release 10.0.2.

- OPENAM-3353: LDAP auth does not set operation timeout; OpenAM freeze

- OPENAM-3330: Backport of LDAP Auth failover code

- OPENAM-3269: create-agent-grp or adding groupconfig in OpenAM console fails with NPE for subrealms

- OPENAM-3259: StackOverflowError when invalid pcookie is presented

- OPENAM-3252: LoginServlet reroute logic should consider AMAuthCookie as request parameter

- OPENAM-3226: Creating a realm may cause duplicate delegation privilege entries to be written to datastore if multiple servers are running

- OPENAM-3225: SAML authentication throws NPE with IDP metadata showing certain characteristics

- OPENAM-3217: JSP compilation error in Java Fedlet

- OPENAM-3210: In CDSSO scenario no Logout is triggered when choosing 'yes' on 'new_org.jsp'

- OPENAM-3189: IdP Proxy should invoke SP Adapter when sending the proxied SAML request

- OPENAM-3165: NPE during export-svc-cfg

- OPENAM-3160: AuthContext failover doesn't work

- OPENAM-3105: CachedSubEntries.getSubEntries() shouldn't sort LDAPSearchResults

- OPENAM-3057: DAS /UI/Logout does not work.

- OPENAM-3005: Exported IdP entity cannot be imported back via console

- OPENAM-2953: After upgrade export-svc-cfg + import-svc-cfg stops working

- OPENAM-2948: RESTful read performance: identityExists() is called twice before searching user entry

- OPENAM-2947: Missing statement close in DBHandler can lead to database resource issues.

- OPENAM-2922: SP initiated SLO can fail with IllegalStateException

- OPENAM-2875: Invalid group name error when group does not exist in LDAP

- OPENAM-2764: IdRepoJAXRPCObjectImpl and DirectoryManagerImpl notification URL cache can contain duplicate URLs

- OPENAM-2760: Validation of gotoOnFail URLs

- OPENAM-2757: PrivilegeEvaluator might deadlock if there was a referral privilege added during evaluation

- OPENAM-2737: ReplayPasswd fails in chain auth if PasswordCallback is not available in the last executed auth module

- OPENAM-2719: OAuth2 Consumer sends the OAuth2 token as an Authorization header and as a URL param.

- OPENAM-2689: OAuth2 Client module does not work when used with SAML

- OPENAM-2686: ServiceSchemaManagerImpl.isValid does unnecessary search against config store

- OPENAM-2682: DBFormatter re-generate timestamp causing inaccurate timestamp

- OPENAM-2671: LDAPConnectionPool.getConnFromPool could lead to ArrayIndexOutOfBoundsException

- OPENAM-2644: Cannot resolve element with ID "s2..."

- OPENAM-2628: Case insensitivity for realms is not enforced in AuthenticateToRealmCondition.getConditionDecision

- OPENAM-2619: OpenAM is not verbose enough for installation failures

- OPENAM-2616: Zero page login restriction is too strong

- OPENAM-2612: Personal password reset questions cannot be set

- OPENAM-2596: ssoadm show-privileges result misleading if no identity with given type exists

- OPENAM-2544: OpenAM with Internal Server Error after upgrade

- OPENAM-2530: RemoteHttpServletRequest should store headers in CaseInsensitiveHashMap

- OPENAM-2514: Remove-privileges command doesn't handle All Authenticated Users role correctly in subrealms

- OPENAM-2502: show-privileges command returns incorrect values for subrealms

- OPENAM-2494: Request serialization fails on weblogic

- OPENAM-2490: Sessions tab on console makes HTTP request to local server as well

- OPENAM-2478: Checking if stats are being collected in NetworkMonitor loads Entitlement configuration on every call.

- OPENAM-2472: SubjectConfirmationImpl.toXMLString processing not compliant with SAML2 core spec processing rules for SubjectConfirmationType

- OPENAM-2462: extended information in console about property 'Trusted Remote Hosts' for cert auth is incorrect

- OPENAM-2426: Calling Logout and passing a goto URL parameter with an expired session causes the goto URL to be ignored.

- OPENAM-2408: It is not possible to edit all Properties defined in a Current Session Property condition if more than one is defined.

- OPENAM-2402: Unable to delete Property Items in a Current Session Property Condition

- OPENAM-2400: Agent property inheritance does not work as expected

- OPENAM-2370: OpenAM cannot identify the property: com.sun.am.replaypasswd.key

- OPENAM-2369: Export Agent Configuration in the console fails with exception if locale is set to fr

- OPENAM-2274: Default SP Account Mapper can't autofederate using the NameID

- OPENAM-2266: Special chars in ResponseSet XML causing parse errors

- OPENAM-2265: Entitlement Conditions may be evaluated multiple times for a single policy evaluation

- OPENAM-2224: Deadlock in LDAPv3EventService

- OPENAM-2212: AMHostnameVerifier does not work if no keystore is defined

- 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-2134: IDPProxy fails to redirect to IDP with an exception. NameIDPolicy is not available in the AuthRequest from remote SP

- OPENAM-2117: ssoadm create-agent command should not require serverurl/agenturl for web/j2ee agents

- OPENAM-2112: ssoadm add-privileges does not work for All Authenticated Users role

- OPENAM-2110: Upgrade fails if external configstore is using non-default user

- OPENAM-2104: noconsole/headless 10.0.1 war doesn't function properly after restart

- OPENAM-2102: LDAPConnection does not handle unsolicited extended responses

- OPENAM-2093: Cleaned up remote sessions shouldn't have destroyed state

- OPENAM-2059: ssoadm export-svc-cfg throws NullPointerExecption if no SubConfiguration exists for a given service

- OPENAM-2057: OpenSSOPrivilege.evaluate() should not return null

- OPENAM-2053: Log Number of History files count is ignored when log rotation is based on time

- OPENAM-1981: Mis-translated French property items for Agent Console page

- OPENAM-1980: HTTP Redirect SAML requests are incorrectly inflated when they are longer than the configured buffer length

- OPENAM-1964: Performance issues when using AMIdentitySubject with groups

- OPENAM-1933: ReplayPasswd only supports passwords with max 16 characters

- OPENAM-1791: When in message level debug, amUpgrade file logs entries on every request to OpenAM console

- OPENAM-1739: HOTP module may ignore SMTP settings in the configuration

- OPENAM-1655: AttributeQueryUtil ignores configured SPAttributeMapper

- OPENAM-1641: LoginState paramHash is not always correctly initialized when using request serialization

- OPENAM-1569: Remove objectclass=ldapsubentry from LDAP requests

- OPENAM-1512: LDAPConnectionPool is not re-initialized correctly if failover server is down

- OPENAM-1511: closing of LDAPConnection in LDAPConnectionPool is not synchronized

- OPENAM-1453: The read RESTful interface returns an NPE instead of ObjectNotFound when trying to query a nonexistent user

- OPENAM-1180: Login URL problems when using Federation

- OPENAM-1098: During installation I found a link to Oracle

- OPENAM-1083: Using Federation redirects with the valid goto URL whitelist causes problems

- OPENAM-1051: SessionActiveCount also count agent user sessions

- OPENAM-1012: IDP initiated SAML2 SLO error when SP does not have SLO binding

- OPENAM-973: LDAPConnectionPool#decreaseCurrentConnection() could throw ArrayIndexOutOfBound exception

- OPENAM-844: If Directory Server is started after OpenAM, LDAPv3Repo will never recover

- OPENAM-688: REOPEN -LDAP Error 80 can result in build up of LDAPv3EventService::RetryTask objects

- OPENAM-340: Failed to create new Authentication Context error when zero page login fails on DAS

- OPENAM-6: wantLogoutResponseSigned incorrectly evaluated

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 10.0.2 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 10.0.2, 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

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/.