Release Notes

OpenAM 10

Mark Craig

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

1.1. New in 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*.

1.1.1. 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. New in 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*.

1.2.1. 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

1.3. New in 10.0.0

OpenAM 10.0.0 fixes a number of issues, and provides the following additional features.

Major New Features

- OpenIG, the ForgeRock Identity Gateway, is a high-performance reverse proxy server with specialized session management and credential replay functionality. OpenIG integrates well with OpenAM, and there is no need to modify the target application or the container in which it runs.

  OpenIG also includes the Federation Gateway, which enables federation capabilities for applications that cannot be modified to use the Fedlet and SAML 2.0.

- OpenAM now uses OpenDJ 2.4.5 as the embedded data store (OPENAM-960).

  OpenAM now also uses the OpenDJ LDAP SDK.[1]

- OpenAM now provides JSON output through the identity services REST interface (OPENAM-940).

- OpenAM now supports adaptive risk authentication (OPENAM-846). You configure the adaptive risk authentication module to assess risks, and then you add the module into an authentication chain. The module determines whether to require further authentication processing based on assessment of the risk involved during authentication. Adaptive risk authentication lets you require more from users when they login from an unfamiliar location, from a new device, after a long period during which the account remained idle, and so forth.

- OpenAM supports a new SAML 2.0 IdP Adapter plug-in for additional flexibility. The adapter lets the system handle situations that arise when the identity provider needs to perform additional processing before releasing the assertion, or when interaction with the user is needed before releasing it. The IdP Adapter class implementing the plugin can be configured through the console (OPENAM-700).

- OpenAM now provides an OAuth 2.0 Client authentication module (OPENAM-679).

- Multiple improvements in the OpenAM upgrade process streamline the move to the new version (OPENAM-626).

- OpenAM now supports interoperability with LDAP servers that implement the (Behera) Internet-Draft, Password Policy for LDAP Directories (OPENAM-613).

Additional New Features

- Setup wizards make it easier to use OpenDJ as the identity repository.

- OpenAM now allows you to differentiate Login UI buttons using CSS (OPENAM-977).

- OpenAM now allows authentication modules to be installed as a single .jar file (OPENAM-916).

- OpenAM has improved console configuration for handling services such as Authentication Core Settings and Identity Repositories (OPENAM-887).

[1] The Java EE deployment container in which OpenAM runs can potentially expose leaks in OpenDJ LDAP SDK (OPENDJ-388).

- The **ssoadm** command now provides subcommands to manage entitlement application types: **create-appl-type**, **delete-appl-types**, **list-appl-types** (OPENAM-872).
- OpenAM console now includes many more helpful hints and built-in documentation (OPENAM-805).
- OpenAM now lets you fetch maximum session time, time remaining, and idle time when querying attributes over the REST interface (OPENAM-801).
- OpenAM now supports a `refresh` parameter to reset session idle time to 0 when querying attributes over the REST interface (OPENAM-800).
- OpenAM now supports time zone policy settings using the RFC 822 format, +/-0000 (OPENAM-791).
- OpenAM session service now lets you set the maximum session time, maximum idle time, and maximum caching time when assigning service to the user through the console (OPENAM-785).
- OpenAM now returns a load balancer cookie, if configured, to an authentication request over the REST interface (OPENAM-766).
- OpenAM ClusterStateService now works with HTTPS endpoints (OPENAM-759). When using HTTPS endpoints, set `com.sun.identity.urlchecker.dorequest=false`.
- OpenAM now bundles `click-nodeps.jar` (OPENAM-646).
- OpenAM now provides additional statistics related to session failover (OPENAM-641).
- The OpenAM **amsfo** script now starts the session database only after the message queue is up and running (OPENAM-624).
- OpenAM .NET fedlets now support encrypted assertions (OPENAM-604).
- The Administration Tools setup script now has better default settings (OPENAM-577).
- The OpenAM console configuration wizard now suggests better values for cookie domains (OPENAM-576).
- OpenAM .jar files now contain standard MANIFEST entries (OPENAM-570).
- The **ssoadm** can now decode an encrypted password stored in the password file (OPENAM-569).
- You can now configure the HOTP authentication module email from address using OpenAM console (OPENAM-513).
- The OpenAM console page `Debug.jsp` (such as `http://openam.example.com:8080/openam/Debug.jsp`) now can set the log level for any debug instance (OPENAM-511). See the Debug instances drop-down list at the top of the page.
- OpenAM now provides a property, `openam.authentication.ignore_goto_during_logout`, to set whether to ignore logout `goto` URLs, and instead display the Logout page (OPENAM-494).

- OpenAM now provides support for multiple failover servers in the RADIUS authentication module (OPENAM-477).
- OpenAM now provides a mechanism to control which session properties are copied during session upgrade (OPENAM-462).
- OpenAM now provides session timeout notification (OPENAM-457). The improvement implements a hook for timeout into the session service on the server side. It listens for timeouts on all sessions.
- The OpenAM authentication service now can map HTTP headers when forwarding requests (OPENAM-453). This applies both to the distributed and centralized authentication services. See configuration properties `openam.retained.http.headers` and `openam.forbidden.to.copy.headers`.
- The OpenAM session service now lets you extend quota exhaustion actions with a plugin (OPENAM-433).

  To add a new plugin, update the `amSession.properties` files with the appropriate internationalization keys, and place your plugin class either in `WEB-INF/classes` or `WEB-INF/lib` where you deployed OpenAM. Next, add your implementation using the **ssoadm** command.

  ```
  $ ssoadm
   set-attr-choicevals
   --servicename iPlanetAMSessionService
   --schematype Global
   --attributename iplanet-am-session-constraint-handler
   --adminid amadmin
   --password-file .pass
   --add
   --choicevalues mykey=demo.Clazz
  ```

  Here, *mykey* is the internationalization key you added to `amSession.properties` files, and *demo.Clazz* is the fully qualified class name for your plugin class.

  You can remove the plugin using the **ssoadm remove-attr-choicevals** command, and list quota exhaustion actions using the **ssoadm get-attr-choicevals** command.
- OpenAM now tracks monitoring information for LDAP connection pools (OPENAM-410). OpenAM monitoring exposes the minimum size of the pool, the maximum size of the pool, the high water mark of the pool, the current size of the pool, the number of connections retrieved, the number of connections created, and the number of connections destroyed.
- OpenAM Windows Desktop SSO now provides a mechanism to fail attempted authentication when Kerberos-authenticated user has no profile in the OpenAM data store (OPENAM-403).
- OpenAM now handles Active Directory password expiration responses properly (OPENAM-258).
- OpenAM password reset now uses realm aliases to find realms for end users, eliminating the need to add a realm parameter to the URL (OPENAM-192).
- OpenAM now allows time-based rotation, and also file name prefixes and suffixes for regular and debug logs. (OPENAM-41, OPENAM-42)

- For cross domain single sign on and SAML 2.0 authentication, users were presented with a blank login page during authentication, in fact a page containing forms with hidden fields used to process authentication. OpenAM now provides templates so you can show users something besides than blank pages, such as for example a page with an animated .gif progress bar (OPENAM-9).

  For cross domain single sign on, edit a copy of the file `config/federation/default/cdclogin.jsp` where you unpacked the OpenAM web application (for example `/path/to/tomcat/webapps/openam/config/federation/default/cdclogin.jsp`). You can change the presentation as appropriate for your deployment. Make sure you retain the form and JavaScript to ensure requests are processed properly. Then replace `config/federation/default/cdclogin.jsp` with your version.

  For SAML 2.0, modify the templates `saml2login.template` and `saml2loginwithrelay.template` to change the presentation, retaining the form and JavaScript. Then copy your templates under the `WEB-INF/classes/` directory where you unpacked the OpenAM web application (for example `/path/to/tomcat/webapps/openam/WEB-INF/classes/`).

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.

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

Important

If you are still using OpenAM 10, upgrade as soon as possible to a supported version of ForgeRock Access Management that includes the latest security fixes.

Update OpenAM 10 installations to the latest maintenance release as described here. 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

If you have already installed OpenAM, follow these steps.

1. Download and unzip the OpenAM maintenance release.
2. If you have made any customizations, apply them to the .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. (Optional) 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 the latest supported version of ForgeRock Access Management.

1. Download the release from https://backstage.forgerock.com/downloads.
2. Follow the installation instructions for that version.

Chapter 4

OpenAM Changes & Deprecated Functionality

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

4.1. Major Changes to Existing Functionality

- The following web policy agents are compatible with OpenAM 10.0.0.
  - Apache 2.0
  - Apache 2.2
  - Microsoft IIS 6
  - Microsoft IIS 7

  The following J2EE policy agents are compatible with OpenAM 10.0.0.
  - 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 10.0.0.

- 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 10.0.0 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 the time of release.

Note

This release contains fixes that resolve security issues within OpenAM. Older versions of OpenAM contain these security issues. It is recommended that you upgrade to this release to resolve these security issues. ForgeRock customers can contact support for details on the security issues.

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

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

The following issues were fixed in release 10.0.0.

- OPENAM-1238: inline help in auth modules is broken after upgrade
- OPENAM-1235: Merged debug log doesn't rotate
- OPENAM-1215: DAS forgets original login URL with multi-step modules
- OPENAM-1210: amsessiondb sets OS_ARCH twice, ignoring customization to the first property
- OPENAM-1209: DNS lookups in DNOrIPAddressListTokenRestriction should be truely optional
- OPENAM-1177: NullPointerException within FAMSTSImpl
- OPENAM-1172: Can't config User Status Active Value and User Status Inactive Value for Active Directory data store
- OPENAM-1135: The IdP does not sign the SAML2 Logout Response when using HTTP-POST binding when the SP has asked to sign them
- OPENAM-1132: Extensive logging in IdentityServicesImpl
- OPENAM-1125: Request serialization does not work in subrealm with DAS

- OPENAM-1123: LDAPException with -1 resultCode can cause MissingResourceException
- OPENAM-1121: Problem when a SAML2 Single Logout Request lands in the OpenAM that did not issue the original assertion
- OPENAM-1104: CDCServlet doesn't work if custom authentication was used
- OPENAM-1103: Client IP validation does not work with Federation
- OPENAM-1100: OAuth provider does not work with subrealms
- OPENAM-1086: The SAML2 IdP Adapter does not get called when using IdP Initiated SSO
- OPENAM-1083: Using Federation redirects with the valid goto URL whitelist causes problems
- OPENAM-1071: amadmin can't login when AM SDK cache is disabled
- OPENAM-1069: createSSOToken(request) does not honor client IP header settings
- OPENAM-1064: NPE when SDK cache is disabled
- OPENAM-1061: Deadlock in LDAPv3Repo
- OPENAM-1057: OpenAM Upgrade decision based on build date
- OPENAM-1049: Exceptions in IdRepo debug log after upgrade to OpenAM 10
- OPENAM-1047: isSessionQuotaReached does not work correctly if users session quota > 1
- OPENAM-1044: Collection of bugs related to Upgrade in OpenAM 10
- OPENAM-1043: Identity web-services update call always removes group memberships
- OPENAM-1041: Destroy Oldest Session action should actually destroy the _oldest_ session
- OPENAM-1029: 3 small fixes for OAuth module
- OPENAM-1028: ArrayIndexOutOfBoundsException in debug log message in AMLoginContext
- OPENAM-1018: Mixed up property names on console SDK page
- OPENAM-1006: Wildcards in referrals can be ignored due to invalid search filter
- OPENAM-1002: persistent cookie doesn't work for subrealm with different datastore than default realm
- OPENAM-999: Error Configuring Directory Server in enable replication during multi-server site deployment
- OPENAM-997: openam console front page has references that need to be changed or updated
- OPENAM-989: Create JDBC Datastore throws uncaught exception

- OPENAM-987: special character used in membership search filter should be escaped (rfc2254)
- OPENAM-985: LDAPv3Repo and associated classes can cause leak in the shutdown manager due to LDAP exceptions
- OPENAM-979: behera password policy displays wrong message for password-history-count check
- OPENAM-975: RuntimeException in Sufficient module breaks the chain
- OPENAM-971: behera password policy displays wrong message for max-password-length check
- OPENAM-961: Ensure that the FQDN is used when interacting with OpenDJ in order to ensure that certificate owner/issuer names are correct
- OPENAM-952: OpenAM Role Subject type does not work in console-only deployment
- OPENAM-941: behera password policy Change Password screen allows to grace logins to be 0
- OPENAM-933: Fedlet encounters error processing LogoutRequest as /saml2loginwithrelay.template is missing from the classpath
- OPENAM-923: IdRepo log is spammed with agent attributes
- OPENAM-922: Unable to set Active/Inactive userstatus values for several datastores
- OPENAM-917: When using Console only deployment, checking policies in a sub-realm throws a "java.lang.UnsupportedOperationException: Not supported" exception.
- OPENAM-906: ServiceTypeManager can return invalid tokens
- OPENAM-903: IdRepoListener missing from Javadoc
- OPENAM-897: NPE managing LDAP subject users
- OPENAM-896: Javascript and CSS bugs on userstore wizard screen
- OPENAM-895: Access to root realm after console deploy timeout occurs
- OPENAM-893: REST logout does not perform actual logout on auth context
- OPENAM-891: Relative (goto) redirects don't work with proxied requests
- OPENAM-888: SAML2 Authentication Authority entity bindings are verified as if they were in an SAML2 IDP entity, this causes an NPE
- OPENAM-886: Memory leak in REST API (RegExResourceName)
- OPENAM-885: After restoring backup OpenAM fails to load configuration
- OPENAM-883: PagePropertiesCallback ignores attribute and require lists

- OPENAM-881: empty passwords cause backup to fail during upgrade
- OPENAM-878: new_org.jsp doesn't work, when the second auth request contains extra parameters
- OPENAM-871: Configurator User Data Store selection not retrieving i18n values
- OPENAM-870: OpenAM Console Session list throwing an exception
- OPENAM-866: Upgrade fails to connect to external configuration store
- OPENAM-864: Upgrade on Windows fails to delete services fully
- OPENAM-863: A second GUI Configurator Exists
- OPENAM-862: Upgrading from 9.5.3 cause a NPE in generateShortReport
- OPENAM-861: Typo in Restart Instruction after Upgrade
- OPENAM-860: Upgrade possible to initialise on up-to-date server
- OPENAM-856: CLI Upgrade Causes issues in Authentication Module List
- OPENAM-848: Update references in OpenAM Configurator for Config/User Store to OpenDJ
- OPENAM-847: i18n Values for sunAMAuthHOTPSMTPFromAddress not present in resource files
- OPENAM-843: Exception handling in the REST interface
- OPENAM-841: Inconsistent formatting on OpenDS page.
- OPENAM-839: LDAP Auth Module doesn't remove terminated LDAP connection from pool and returns 401 error via REST interface
- OPENAM-833: Regression: Datastore auth with external directory doesn't work
- OPENAM-832: Character encoding problem on the password reset page
- OPENAM-831: QA Test Suite not providing useful results
- OPENAM-828: L10NMessageImpl can lose initCause
- OPENAM-827: Creating a Identity Membership Condition in a sub-realm does not use the correct Datastore
- OPENAM-825: Multiprotocol federation sample application failure
- OPENAM-824: LoginViewBean UI does not implement new_org.jsp functionality
- OPENAM-818: SFO scripts don't work on Debian GNU/Linux, because of /bin/awk path
- OPENAM-817: ShutdownManager gets stuck in waiting state causing the server to be unavailable

- OPENAM-814: Setup progress page is never closing the stream
- OPENAM-813: Session timeout branding is not working
- OPENAM-812: LDAPFilterCondition will try to bind using LDAPv2 even with LDAPv3 only servers
- OPENAM-811: AMIdentityMembershipCondition is missing information about who the user is which is required to make the decision
- OPENAM-807: In case of session upgrade requesting the page again can cause Session Timeout errors
- OPENAM-794: Successful access to LoginViewBean still creates a new session
- OPENAM-792: SAML2 Metadata for a remote service provider with Extensions breaks the console and Entity Providers no longer list under Federation
- OPENAM-790: LDAPFilter conditions are not using the correct Policy config when used in a sub-realm policy definition.
- OPENAM-789: amverifyarchive throws an NPE
- OPENAM-788: Combination of referral policy, self evaluation and super resource match fails to follow referral
- OPENAM-787: amtune fails to interpret ls -l output
- OPENAM-784: AMSetupServlet::getRemoteServerInfo fails if the first instance SSL certificate is invalid
- OPENAM-780: Config Wizard does not validate server URL successfully
- OPENAM-778: Config Wizard ignores server URL
- OPENAM-775: When a SAML2 Request does not contain an Authentication Context, the Default Authentication Context mapper maps a level=0
- OPENAM-767: Radius auth module typo (wrong server configuration check)
- OPENAM-743: Misspelling of Minimum in resource files
- OPENAM-738: Endless recursion in CachedRemoteServicesImpl
- OPENAM-734: AuthenticationFailureCount and AuthenticationFailureRate do not Update Correctly
- OPENAM-733: JDBC authentication module fails to initialize in JNDI mode
- OPENAM-730: LDAPConnectionPool has risk of dead lock
- OPENAM-726: Multi-threaded entitlement evaluation gives wrong result

- OPENAM-716: Shutting down DS when "sun-idrepo-ldapv3-config-idletimeout" is other than 0 (zero) can result in loop
- OPENAM-688: REOPEN -LDAP Error 80 can result in build up of LDAPv3EventService::RetryTask objects
- OPENAM-684: LDAPv3EventServicePolling can enter RetryTask loop if LDAP encounters a problem at the same time as the persistent searches are restarted
- OPENAM-675: updateSiteNameToIDMappings will leave siteNameToIdTable null if sites are not configured
- OPENAM-673: CachedSubEntries::getSubEntries returns the actual reference to the cache entry
- OPENAM-668: AuthClientUtils::sendAuthRequestToOrigServer does not handle server errors
- OPENAM-667: Persistent Cookie should only be set on success and not on AMAuthCookie
- OPENAM-664: OpenAM complains about invalid character when the FedCOTMemberName has '=' in it
- OPENAM-656: jaxrpc xml parser can introduce corruption in the output when parsing
- OPENAM-652: amsessiondb should run with tx no sync in bdb
- OPENAM-644: amsessiondb error messages are going to System.err and are getting lost
- OPENAM-643: amsessiondb does not shutdown properly if the DB/MQ is broken
- OPENAM-642: amsessiondb does not recover from db errors and can break the MQ
- OPENAM-639: DAUI shutdown is not releasing resources correctly
- OPENAM-633: Infinite loop in LoginViewBean during login using Membership login module
- OPENAM-622: changing the debug level from message to error is ignored by the entitlements engine
- OPENAM-616: Error while trying to import service configuration into OpenDJ
- OPENAM-615: Session upgrade does not work if the second login is on a different server
- OPENAM-612: LoginState looks up LDAP profile attributes for the session service when it doesn't need to.
- OPENAM-608: javax.servlet.ServletException: missing jspFile on start up
- OPENAM-586: Certificate module has a problem with OCSP validation if JCE is used
- OPENAM-584: rest authentication interface does not differentiate between inactive and locked accounts

- OPENAM-583: maximum session limit during rest authentication results in 200 and null return
- OPENAM-581: Debug error log gets "unable to locate message ID object for FSAssertionManager" when using CDSSO
- OPENAM-580: GOT_ALL_HOSTED_ENTITIES audit log is erroneously logged
- OPENAM-529: SecurID Authentication in New PIN mode and Change PIN mode fails in English locale
- OPENAM-528: OpenAM distribution includes unittest JSPs and libary
- OPENAM-527: OpenAM console is displaying a Sun-branded favicon
- OPENAM-523: HOTP authentication module: If sms and/or email could not be sent no error is shown for the user
- OPENAM-521: HOTP authentication module: Missing properties in resource bundle leads to internal authentication error
- OPENAM-520: When a SAML2 Authentication Request is sent to an IdP with the IsPassive flag set to true and no valid session is present, the RelayState is dropped by the IdP
- OPENAM-519: SecurID authentication exception: Logindisplay:Null
- OPENAM-518: DAS configurator does not store OpenAM deployment URI
- OPENAM-509: AuthUtils.isLocalServer method gets confused with the server URI when used on the DAS
- OPENAM-508: lb cookie set on the DAS is used incorrectly in the PLLClient
- OPENAM-506: Not every admin tool ignores version check by default
- OPENAM-491: Running in non c66encode mode can lead to dual URL decoding issue in the CDCClientServlet to CDCServlet communications
- OPENAM-489: Multiple windows during SAML2 sign-on can lead to NPE
- OPENAM-488: Multiple browser access can cause invalid redirects during SAML2 sign-on
- OPENAM-487: In case of zero page session upgrade DAS does not set session cookie expiration
- OPENAM-486: amMasterSessionTableStats can be negative in some cases
- OPENAM-485: SAML validator.jsp breaks with NPE if it was unable to create ValidateSAML2
- OPENAM-482: create-server command returns success state when invalid properties were supplied
- OPENAM-478: AuthClientUtils should forward requests with the same method in case of failover

- OPENAM-475: SAML2 HTTPPOST Profil: Assertion not signed when response is signed
- OPENAM-473: Build can't handle spaces in directory names
- OPENAM-470: DAS LogoutViewBean should not accept invalid gotoURL's
- OPENAM-468: HttpURLConnectionManager should set a connect timeout for the provided connections
- OPENAM-459: Log file "amAuthentication.error" is not created
- OPENAM-446: When changing the DNS alias in a realm, the Realm Alias Referrals are not updated until restart when using external configuration store
- OPENAM-440: Agent inheriting Location of Agent Configuration Repository from Agent Group causes error
- OPENAM-407: Missing files while creating console/noconsole wars
- OPENAM-398: OpenAM's servlet API version does not officially support the included JSTL 1.1
- OPENAM-393: If the Session DB is offline, AMLoginModule::isSessionQuotaReached malfunctions
- OPENAM-370: LoginViewBean NPE
- OPENAM-333: Custom Response Providers are ignored by the Entitlements Framework
- OPENAM-318: It is not possible to assign a Post Authentication Class plugin to a service chain with the ssoadm
- OPENAM-312: OpenAM LDAP schema should conform to the expected structural objectclass usage
- OPENAM-298: Distributed authentication UI not able to do resource based authentication
- OPENAM-269: Blank in form can break fedlet creation
- OPENAM-261: SAML2.0 isPassive attribute in the AuthnRequest is ignored by the IdP
- OPENAM-247: Distributed Authenticaion UI Login URL not accepted
- OPENAM-191: Remote SessionRequest.setProperty causes HTTP 500 for null property/value
- OPENAM-188: SetupDistAuthWAR does not support the ability to set the lb value
- OPENAM-171: "Authentication by Module Chain" fails when used in a sub-realm
- OPENAM-109: updating service to include new PluginSchems, ssoadm command is counterintuitive
- OPENAM-107: j2eeagents README is out of date for WebLogic v10.3
- OPENAM-90: Default top-level realm privileges block SMS access to policy agents

- OPENAM-87: SessionCount.getDeploymentMode uses site rather than server count to determine multi server mode
- OPENAM-77: SAML2 service provider initiated SSO does not check that the realm of the authenticated user matches the realm of the COT
- OPENAM-74: RuntimeException does not updates the failureModuleSet in LoginState
- OPENAM-34: Naming of Nightly Bild Files
- OPENAM-28: No way of configuring CDC and federated authentication without writing custom code
- OPENAM-25: Some classes of Policy Changes are not propagating to the agent
- OPENAM-20: ssoadm versioncheck fails with encoded contents
- OPENAM-16: Deadlock when making Entitlements REST requests

5.2. Limitations

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 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 has a number of outstanding issues. To retrieve the list, query the issue tracker for OpenAM 10.0.2 Known Issues.

The following important known issues remained open at the time release 10.0.0 became available.

- OPENAM-1253: Multi-server OpenAM instances fail to connect after configuration
- OPENAM-1252: ssoadm loses exception causes

- OPENAM-1250: Installation failing on Websphere 8
- 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-1245: Configuring datastore for failover with persistent search enabled causes exception logging loop
- OPENAM-1243: OpenAM fails to start on JBoss AS 7.1.1 (see link to workaround in bug report)
- OPENAM-1242: OpenAM default configuration fails on Jetty 7 (Mac OS X)
- OPENAM-1241: Upgrade fails due to ArrayOutOfBoundsException (Mac OS X)
- OPENAM-1240: Attributes referred by SAML service are not part of the LDAP schema
- OPENAM-1234: ssoadm embedded-status can't connect to the embedded config store when SSL is enabled in Tomcat
- OPENAM-1226: JAX RPC calls generating java.lang.InternalError: fillbuf: errors in OpenAM container log
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1214: Session timeout in Membership module can result in invalid login URL
- OPENAM-1211: Agent profile attribute description for override properties are insufficient on the console
- OPENAM-1204: Creation of xamcl policy (entitlement) with cli ssoadm tool fails when using Secure Logging
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1185: amadmin unable to log in if global session quota reached
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1180: Login URL problems when using Federation
- OPENAM-1133: SAML2 Entity import does not support EntityDescriptor elements contained in an EntitiesDescriptor element
- OPENAM-1119: no way to specify namespace for DigitalSignature element
- OPENAM-1114: Meta-bug for issues relating to Login UI update
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled

- OPENAM-1110: ssoadm fails with NullPointerException and does not terminate
- OPENAM-1109: AdminTokenAction doesn't clear invalid SSOToken
- OPENAM-1108: DAUI does not get client IP address when behind proxying load balancers
- OPENAM-1107: LDAPv3Repo: isExists() call returns false although uses exists in the datastore
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1094: Edit User page in console throws misleading exception if some attributes can not be retrieved from data store
- OPENAM-1093: Authentication fails if session-service attributes are not stored in user entry in Active Directory
- OPENAM-1073: OpenAM deployment in Oracle 11g has some webservices libraries conflicts
- OPENAM-1072: OpenAM crashes when using log rotation
- OPENAM-1068: In case of session upgrade the SAML IDPCache can lose the ssotoken sessionindex mapping
- OPENAM-1062: VERSION button in jboss 7.0.2 results in uncaught exception page
- OPENAM-1059: Support multiple "signing" certificates in idp.xml
- OPENAM-1054: MySQL (JDBC) IdRepo shares configurations in all realms in the wrong
- OPENAM-1053: JSON string is not properly transformed to PolicyDecision
- OPENAM-1051: SessionActiveCount also count agent user sessions
- OPENAM-1038: openfedlib: Missing properties for libSAML2, libSAML2Meta...
- OPENAM-1026: Goto parameter is missing when using loadbalancing and ws-federation
- OPENAM-1023: Erroneous XACML policy decision unless actions saved using standard console
- OPENAM-1016: XACML policy obligation expressions are silently discarded on import
- OPENAM-1013: Privileged Sub-Realms Admin Users fail to retrieve user information using Identity Services
- OPENAM-1008: Unable to authorize user using x500Name due to NullPointerException
- OPENAM-1007: Memory Leak in SMSNotificationManager when ldap error occurs
- OPENAM-995: using UTF-8 characters in policy names breaks the policy console
- OPENAM-986: LDAP Auth failover not switching to secondary ldap server

- OPENAM-983: ssoConfigurator leaks connections
- OPENAM-982: ssoadm cli tool chokes on many policies
- OPENAM-976: NPE in Datastore module
- OPENAM-974: Custom schema attribute validators are not invoked
- OPENAM-973: LDAPConnectionPool.decreaseCurrentConnection() could throw ArrayIndexOutOfBound exception
- OPENAM-972: Remote Session accumulates via CDCServlet
- OPENAM-955: Persistence cookie with TTL does not work on UI LoginViewBean
- OPENAM-953: Call PostProcessing classes for REST auth
- OPENAM-951: IP address doesn't work on Agent URL
- OPENAM-944: Missing amUtilMsgs_en.properties prevents fedlet from starting up.
- OPENAM-943: Default attributeMap of *=* prevents AttributeQuery from working.
- OPENAM-921: Monitoring tries to export SAML entries with the same id sometimes
- OPENAM-920: Monitoring fails to handle secondary site IDs
- OPENAM-919: LoginState fails to initialize AuthenticationPrincipalDataRetriever
- OPENAM-844: If Directory Server is started after OpenAM, LDAPv3Repo will never recover
- OPENAM-836: Unable to get account linking to work between two OpenAM instances
- OPENAM-808: OpenAM instances hung when starting at the same time.
- OPENAM-799: problem with embedded opends replication for openam clustering
- OPENAM-776: Character "\" in UID not processed correctly, two differend UIDs stored in DS entery.
- OPENAM-774: Invalid characters check not performed.
- OPENAM-753: OpenAM Fedlet HTTP Artifact binding not working wioth HTTPS
- OPENAM-752: AgentsRepo.getAttributes fails to get agent information occasionally leading to server restart
- OPENAM-751: It should be possible to disable 'X-DSAMEVersion' http-header
- OPENAM-744: /ssoadm.jsp?cmd=delete-policies execution time grows linearly with the number of submitted delete-policies calls

- OPENAM-742: Policy Evaluation Issue
- OPENAM-740: During Agent authentication agent profile is searched in all configured datastores
- OPENAM-732: encode issue in CDCServlet if url contains blank
- OPENAM-710: AttributeQuery signature is optional
- OPENAM-698: Upgrade the RSA Authentication API
- OPENAM-681: STS WSDL at http://localhost:8080/opensso/sts?wsdl failing to update security mechanism changes
- OPENAM-670: Entitlement evaluation throws org.json.JSONException when evaluating entitlements with resource attributes
- OPENAM-651: internalsession object can grow in size leading to non-linear scaling in the session failover db
- OPENAM-645: EmbeddedOpenDS with bootstrap.properties
- OPENAM-640: Java Fedlet can not handle errors when SAML artifact cannot be retrieved
- OPENAM-637: Submitted namecallback values disappear from UI after errorhandling during rendering the previous page
- OPENAM-611: Java Fedlet AuthnRequest always specifies SPNameQualifier
- OPENAM-609: An empty attributestatement in a saml2 assertion generates an error on post
- OPENAM-587: Null Pointer Exception when setting up monitoring authentication file (configuring with OpenDJ 2.4.1)
- OPENAM-522: Password Reset Options -> Force Change Password on Next Login does not work
- OPENAM-507: Adding to existing deployment fails for non-default Org. Auth. configuration
- OPENAM-504: No method to turn off the RelayState being sent in a SAML 2.0 assertion POST
- OPENAM-500: XML FactoryClass newInstance() methods must need to be cached
- OPENAM-436: spring2provider extension policy evaluation excludes port resolution when incoming request is port 80
- OPENAM-434: The SAML 2.0 profile support of XACML 2.0 is outdated
- OPENAM-417: J2EE agents build script does not recompile sources included in openssoclientsdk.jar
- OPENAM-401: Missing response attribute on first logon after OpenAM restart
- OPENAM-392: STS request with no AppliesTo should use default Web Service Provider agent - wsp

- OPENAM-385: OpenAM 9.5 STS SAMLV2 wsp not retrieving membership data.
- OPENAM-352: Configuration fails if plugin config can not be read on Sun Directory Server Identity Repository
- OPENAM-343: OpenAM Session Service should be able to cope if the JMQ session failover system is down
- OPENAM-340: Failed to create new Authentication Context error when zero page login fails on DAS
- OPENAM-334: STS requires a nonce for UsernamePassword authentication, but this is optional
- OPENAM-327: User attribute mapping to Session attribute functionality goes to LDAP for every attributes
- OPENAM-306: STS WSDL can not be used with JAX WS wsimport tool
- OPENAM-299: LDAPv3Repo tries to query attributes for non-existing users too
- OPENAM-291: SelfWrite permissions are denied to sub realms
- OPENAM-290: IdRepo tries to write back empty attributes rather than removing the attribute
- OPENAM-281: OpenAM STS Endpoint does not look up users by X.509 Subject Name when X509Token is used as Security Mechanism
- OPENAM-280: OpenAM STS fails to create AttributeStatement
- OPENAM-279: Oracle DB as DataStore create user error
- OPENAM-273: com.sun.identity.policy.PolicyManager, when used in client API, does not work across multiple SSO sessions in a single JVM instance
- OPENAM-272: Unable to edit a policy in the realm Policies tab when policy name contains a colon
- OPENAM-268: OpenSSO Web Service Security not working
- OPENAM-236: SharePoint 2010 Integration Fails
- OPENAM-224: OpenAM not returning LDAP error message after password update failure
- OPENAM-174: OpenAM fails to connect to an SSL directory server when installing on Glassfish 2.1.1p6 with NSS security
- OPENAM-149: Allow signing ArtifactResponse's "Response" element instead of Assertion
- OPENAM-139: Retrieving binary attributes via AMIdentity.getBinaryAttributes() in OpenAM is broken
- OPENAM-130: random 'No plug-ins configured for this operation' error when using ssoadm to update iplanet-am-auth-login-success-url

- OPENAM-123: SAML SSO federation - failure to check URL policy during federated SSO post initial authentication.
- OPENAM-120: NPE in IdRepoJAXRPCObjectImpl if caching is disabled
- OPENAM-119: Concurrent access of non-thread safe objects possible in IdRepoJAXRPCObjectImpl
- OPENAM-115: Provide 'read only' privilage for Identity Services
- OPENAM-112: SMS event mechanism copes with schema update notifications, but service configuration updates are missed
- OPENAM-111: LDAPv3 fetches the schema multiple times for LDAPModifications
- OPENAM-105: Restricted tokens cause PA logout to fail.
- OPENAM-103: incomplete information about sessions in SNMP
- OPENAM-84: Unable to save state to multiple choice attribute with ChoiceValue
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-61: SAML2 appliesTo not being HTML character-encoded
- OPENAM-43: Embedded datastore disables event service
- OPENAM-37: Realm names in referrals written inconsistently by the two graphical user interfaces.
- OPENAM-36: Policy created with JATO IDE is incompatible with entitlements managed by JSF IDE.
- OPENAM-33: Startup Errors on GlassFish V3, Conflict Metro RmAssertionCreator.class with RxAssertionCreator.class
- OPENAM-24: Identity Changes not propagating to policy decisions
- OPENAM-6: wantLogoutResponseSigned incorrectly evaluated

Chapter 6

How to Report Problems & Provide Feedback

If you have found issues or reproducible bugs within OpenAM 10.0.0, 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
- 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.