OpenAM Release Notes

Version 11.0.3

Mark Craig
Gene Hirayama
Mike Jang

ForgeRock AS
33 New Montgomery St.,
Suite 1500
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

Abstract

Notes covering OpenAM prerequisites, fixes, known issues. OpenAM provides open source Authentication, Authorization, Entitlement and Federation software.

Table of Contents

Chapter 1

What's New in OpenAM 11.0.3

Important

OpenAM 11.0.3 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 OpenAM From 11.0*.

  Do *not* perform an upgrade by deploying the new version and then importing an existing configuration by running the **ssoadm import-svc-config** command. Importing an outdated configuration can result in a corrupted installation.

- 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:

- **Add option to enable debug logging of decrypted SAML assertions**. OpenAM now provides a debug logging option to decrypt SAML assertions when

OpenAM runs as a service provider and assertion encryption is enabled (OPENAM-1631).

- **DAS Supports goto URL Validation**. DAS now validates `goto` and `gotoOnFail` URLs (OPENAM-1773).

  When performing an upgrade, the old values are migrated across to the new settings. New installations should use the new settings.

- **Authentication Context extensibility support**. OpenAM supports the extensibility of authentication context classes as described in the SAMLv2 specification. (OPENAM-2238).

- **Password Reset Token Validation REST API**. OpenAM supports a single REST API action to check if the token for password reset is valid or not (OPENAM-3748).

- **Default Timelimit using Netscape SDK is Configurable**. The default timelimit for LDAP operations performed using the Netscape SDK is now configurable (OPENAM-5311).

1.2 OpenAM Documentation

You can read the following additional product documentation for OpenAM 11.0.0 online at http://docs.forgerock.org/.

- OpenAM 11.0.0 Release Notes
- OpenAM 11.0.0 Installation Guide
- OpenAM 11.0.0 Upgrade Guide
- OpenAM 11.0.0 Administration Guide
- OpenAM 11.0.0 Developer's Guide
- OpenAM 11.0.0 Reference
- OpenAM 11.0.0 Javadoc

Chapter 2

Before You Install OpenAM 11.0.3 Software

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

Note

The content of this chapter has not changed since OpenAM 11.0.0.

2.1 Java Requirements

This release of OpenAM requires Java Development Kit 6 or Java Development Kit 7. ForgeRock recommends the most recent update of Java 6 or 7 to ensure you have the latest security fixes.

ForgeRock has tested this release of OpenAM primarily with Oracle Java SE JDK, and also tested OpenAM on WebSphere with IBM JDK.

OpenAM Java SDK requires Java Development Kit 6 or 7.

2.2 Web Application Container Requirements

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

- Apache Tomcat 6, 7 (ForgeRock's preferred web container for OpenAM)

- GlassFish v2, v3
- IBM WebSphere 8.0, 8.5
- JBoss Enterprise Application Platform 5, 6

  JBoss Application Server 7
- Jetty 7 (7.6.13 or later)

  Jetty 8 (8.1.13 or later)
- Oracle WebLogic Server 11g (10.3.5)

  Oracle WebLogic Server 12c (12.1.1)

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

2.3 Data Store Requirements

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

- Embedded (using ForgeRock OpenDJ for the data store)
- External ForgeRock OpenDJ data store

  The CTS is supported on OpenDJ versions 2.6.0 and later.

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

- Embedded (using ForgeRock OpenDJ for the data store)

  When using the embedded configuration store for CTS or configuration, you must deploy OpenAM on a local file system and not on an NFS-mounted file system.
- External ForgeRock OpenDJ data store

  ForgeRock recommends updating to the latest stable release.
- External Oracle Unified Directory 11g or later
- External Oracle Directory Server Enterprise Edition data store, version 6.3 or later

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

- ForgeRock OpenDJ

- Microsoft Active Directory (tested by ForgeRock on Windows Server 2008 R2 and 2012)
- IBM Tivoli Directory Server 6.3
- OpenDS, version 2 or later
- Oracle Directory Server Enterprise Edition, version 6.3 or later

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

- Extensible LDAP schema, required to extend the schema for OpenAM. First, install OpenAM to use a fresh instance of OpenDJ, such as the embedded OpenDJ server. After installation, study the custom schema definitions from the OpenDJ file, `config/schema/99-user.ldif`, to see what schema definitions you must add to your directory. You might need to adapt the schema definition format before adding the definitions to your directory.
- The persistent search request control (OID: `2.16.840.1.113730.3.4.3`).
- The Behera Internet-Draft Password Policy for LDAP Directories (in the context of the LDAP authentication module only)

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

2.4 Browsers Tested

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

- Chrome and Chromium 16 and later
- Firefox 3.6 and later
- Internet Explorer 7 and later
- Safari 5 and later

2.5 Platform Requirements

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

- Linux 2.6, 3.0

- Microsoft Windows Server 2008 R2, 2012
- Oracle Solaris 10, 11

2.6 Hardware Requirements

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

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

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

2.7 Special Requests

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

Chapter 3

Updating & Installing OpenAM

ForgeRock recommends that you update OpenAM 11.0 installations to this release. If you are installing OpenAM for the first time, you can use the same installation instructions as for 11.0.0.

Note

The content of this chapter has not changed since OpenAM 11.0.0.

Procedure 3.1. To Update From OpenAM 11.0

If you have already installed OpenAM, follow these steps.

1. Download and unzip OpenAM 11.0.3.

   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 11.0.3 .war file.

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

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

5. 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 11.0.0.

1. Download and unzip OpenAM 11.0.3.

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

2. Follow the instructions in the *OpenAM 11.0.0 Installation Guide*.

Chapter 4

OpenAM Changes & Deprecated Functionality

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

4.1 Important Changes to Existing Functionality

These changes are new in OpenAM 11.0.3.

- **Debug Logging Option to Decrypt SAML Assertions**. OpenAM now provides a debug logging option to decrypt SAML assertions when OpenAM runs as a service provider and assertion encryption is enabled.

  To enable the feature, go to the Debug.jsp page and select the sub page where you want debugging to occur. Then, at the top of the page, click the button to turn decoding on or off. This feature operates independently of the other debug logging options on the page, so you can click cancel or back after pressing the button and the setting is still set.

  For details, see the explanation in (OPENAM-1631).

- **Support for Auth Context Classes Extensibility**. OpenAM supports the extensibility of auth context classes as described in the SAMLv2 specification.

  Custom contexts are also now shown in console if included in the extended metadata but this change does not include the ability to add new contexts

via the console. Custom contexts still need to be loaded via ssoadm/extended metadata. (OPENAM-2238).

- **Password Reset Token Validation REST API**. OpenAM supports a single REST API action to check if the token for password reset is valid or not: `/json/users?_action=confirm`. (OPENAM-3748).
- **Default Timelimit using Netscape SDK is Configurable**. The default timelimit for LDAP operations performed using the Netscape SDK is now configurable (OPENAM-5311).

  To set the property, use `org.forgerock.openam.ldap.default.time= <time limit in milliseconds>`.
- **DAS Supports goto URL Validation**. DAS now validates `goto` and `gotoOnFail` URLs (OPENAM-1773).

The following changes were listed for OpenAM 11.0.2

- Attributes names in responses to REST API calls now preserve the original case used in the request (OPENAM-3159). In other words, if the request asks for `userName`, the response includes `userName`. If the request asks for `username`, the response includes `username`.

  If you prefer that responses always use lower case names, set the advanced server property, `org.forgerock.openam.idm.attribute.names.lower.case` to `true`.
- The `AttributeQueryUtil` class now uses the configured SP attribute mapper to map received attributes in the same way as they come as part of an assertion (OPENAM-1655).

The following changes were listed for OpenAM 11.0.1.

- Consistency has been improved in how OpenAM policy rules match resources. Policy rules are now interpreted more consistently in line with the documentation, and more consistently across platforms and across self and subtree modes. Before you upgrade, consider how these changes affect policy rules.

  Although the changes introduced by the improvements affect mainly edge cases, they do impact deployments relying on previous, inconsistent behaviors. The following points describe how OpenAM and policy agents behave following upgrade to OpenAM 11.0.1 or later and web policy agents 3.3.1 or later.

  - Policy agents configured to use subtree mode behave as they did prior to 3.3.0.
  - If you created your policies with OpenAM 11.0.0 and web policy agents 3.3.0, then note that trailing slashes are no longer stripped from resource names (OPENAM-3509).

In order to match a trailing slash, your rule must end in a slash, or a slash followed by a wildcard.

- When policy agents are configured to use self mode, trailing wildcards, except after `?`, match zero or more characters.
- When policy agents are configured to use self mode, previously a trailing wildcard after a slash, `/*`, matched one or more characters, whereas it now matches zero or more. This means that a resource ending in `/` previously would not match a rule ending in `/*`, whereas it now does.

  If you already have two rules to allow access, one ending in `/` and the other in `/*`, then you have nothing to do. Only the latter rule is now required.

  If however you have only rules ending in `/*` and intend these to deny access to resources ending in `/`, then add rules ending in `/` specifically to deny access to resources ending in `/`.
- When web policy agents are configured to use self mode, trailing wildcards after `?` match *one* or more characters. This means that a resource with a trailing `?` no longer matches a rule of the form `/*?*`, whereas it would have matched with earlier versions.

  To match the behavior of previous releases, when using self mode with resources having empty query strings, add additional rules without trailing wildcards as in `/*?` before you upgrade OpenAM.

- OpenAM now handles SAML single logout (SLO) requests differently when the user presents an invalid session (OPENAM-3437).

  In this scenario OpenAM no longer follows the `RelayState` without validation. To ensure that the `RelayState` validation succeeds, include the `metaAlias` request parameter when invoking the SLO JSPs.

- For LDAP and Active Directory data store configurations the settings for the Authentication Naming Attribute (`sun-idrepo-ldapv3-config-auth-naming-attr`) and the LDAP Users Search Attribute (`sun-idrepo-ldapv3-config-users-search-attribute`) now have the same effects as they did in versions prior to 11.0.0 (OPENAM-3428).

  The Authentication Naming Attribute is now used only to find the user when performing authentication. The LDAP Users Search Attribute is used in other cases when searching for users. When upgrading from OpenAM 11.0.0, make sure these attributes are correctly set in data store configurations.

- The fix for OPENAM-2327 adds a new `PrintWriter` argument to the `postSingleSignOnSuccess` method of the `SAML2ServiceProviderAdapter` class.

If you use a custom Service Provider adapter, then you must update its implementation.

The new `PrintWriter` argument takes the `PrintWriter` for presenting output. It fits between the `HttpServletResponse response` argument and the `Object session` argument.

The following changes were listed for OpenAM 11.0.0.

- The advanced server property used to set the HTTP header name, `com.sun.identity.authentication.client.ipAddressHeader`, has replaced the legacy OpenSSO property `com.sun.identity.session.httpClientIPHeader` (OPENAM-1879).

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

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

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

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

- In versions before OpenAM 10.1.0 the default root suffix DN for OpenAM configuration and profile data was `dc=opensso,dc=java,dc=net`. The default root suffix is now `dc=openam,dc=forgerock,dc=org`.

- The fix for OPENAM-1630 changes SAML metadata signing in OpenAM to better conform with the SAML 2.0 standard.

  - Metadata for hosted entities is signed using the `metadataSigningKey` configured for the realm, or inherited from the global configuration for the server.

  - OpenAM now signs the `EntityDescriptor` element that contains child `SPSSODescriptor` or `IDPSSODescriptor` elements.

  - When importing remote entity metadata with signatures, OpenAM does not modify the signatures, but instead returns them as they were when they were imported.

  - When OpenAM imports remote entity metadata that has no signature and signed metadata is requested on export, OpenAM signs the metadata with the `metadataSigningKey`.

- The default policy evaluation mode for new policy agent profiles is now self rather than subtree, in order to better scale for large numbers of policy rules.

  Upgrade does not change existing policy agent profile configurations, however. If you want to adopt the new default setting for existing policy agents, you must change the setting manually.

  To do so for Java EE policy agents, set `com.sun.identity.policy.client.cacheMode=self`.

  For web policy agents, set `com.sun.identity.agents.config.fetch.from.root.resource=false`.

- You now specify rules for referrals in the same way as rules for policies.

  For example, with previous releases a referral rule for `http://example.com/` matched everything underneath. Now you would need three rules, `http://example.com/`, `http://example.com/*`, and `http://example.com/*?*`. When used at the end of a rule `*` matches one or more characters, rather than zero or more characters.

  When you upgrade OpenAM, the upgrade tool converts existing referral rules.

- The distributed authentication service (DAS) and cross-domain single sign-on (CDSSO) do not support the `iPSPCookie/DProPCookie` query string parameter to set a `DProPCookie` in the user-agent as a mechanism for cookie persistence. Neither DAS nor CDSSO retains `iPSPCookie=yes`.

4.2 Deprecated Functionality

The following functionality is deprecated in OpenAM 11.0.0, and is likely to be removed in a future release.

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

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

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

- With the implementation of the Persistent Cookie authentication module, the Core Authentication module persistent cookie options are deprecated and are likely to be removed in a future release.
- Older REST services relying on the following end points are deprecated.

  /identity/attributes
  /identity/authenticate
  /identity/create
  /identity/delete
  /identity/logout
  /identity/read
  /identity/search
  /identity/update

  The following table shows how legacy and newer end points correspond.

Table 4.1. REST End Points

Deprecated URIs	Newer Evolving URIs
/identity/attributes	/json/users
/identity/authenticate	/json/authenticate
/identity/create, /identity/delete, /identity/read, /identity/search, /identity/update	/json/agents, /json/groups, /json/realms, /json/users
/identity/logout	/json/sessions/?_action=logout
N/A	/json/dashboard
N/A	/json/serverinfo

Find examples in the *Developer Guide* chapter on *Using RESTful Web Services* OpenAM.

Support for the older REST services is likely to be removed in a future release in favor of the newer REST services. Older REST services will be removed only after replacement REST services are introduced.

4.3 Removed Functionality

- OpenAM Java SDK no longer supports JDK 5.
- The `iplanet-am-auth-ldap-server-check` property for LDAP and Active Directory authentication modules has been removed and replaced with a heartbeat mechanism configurable through the LDAP Connection Heartbeat Interval (`openam-auth-ldap-heartbeat-interval`) and LDAP Connection Heartbeat Time Unit (`openam-auth-ldap-heartbeat-interval`) properties for the modules.

  Set these new properties as necessary when you have firewalls or load balancers that drop connections that remain idle for too long.

- The advanced server property, `openam.session.destroy_all_sessions`, has been replaced by the built-in Global Session Service setting, `DESTROY_OLD_SESSIONS`.
- Javadoc for the client SDK is no longer delivered with the distribution, but instead is available online.

Chapter 5

OpenAM Fixes, Limitations, & Known Issues

Important

OpenAM 11.0.1 and later together with OpenAM web policy agents 3.3.1 and later address backward compatibility for policy evaluation. For details, make sure that you read the release notes section on *Important Changes to Existing Functionality*.

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

5.1 Key Fixes

The following bugs were fixed in release 11.0.3. For details, see the OpenAM issue tracker.

- 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-718: Agent group membership lost after backup/restore
- OPENAM-816: ssoadm authentication depends on the sunEnableModuleBasedAuth=true

- OPENAM-1563: Servers and Sites pages may display password in clear text
- OPENAM-1631: Add option to enable debug logging of decrypted SAML assertions
- OPENAM-1773: DAS does not handle goto whitelisting
- OPENAM-2238: Support extensibility of auth context classes as described in the SAMLv2 spec
- OPENAM-2348: set-realm-svc-attrs: "Not a supported type: realm"
- OPENAM-3152: CTS -- External Store Passwords configured in default server settings shown in clear text elsewhere
- OPENAM-3296: ssoadm uses LDAP auth module first to authenticate amadmin
- OPENAM-3748: Password Reset Token Validation REST API
- OPENAM-3825: Mismatch log is recorded when a user fails to change password in LDAP authn process
- OPENAM-3877: Changing password through new REST endpoint fails if default AuthN chain needs more than just the password to authenticate
- OPENAM-4159: OpenAM does not log root cause of PolicyException
- OPENAM-4195: SAML2token saved in CTS with hex tokenId but read without converting to hex
- OPENAM-4213: Root cause of MetaData import is lost when debug level is set to 'error'
- OPENAM-4215: ScopingImpl#makeImmutable should perform null checks
- OPENAM-4218: JAVA_HOME is not set correctly when installing admin tools (ssoadm, ampassword, amverifyarchive)
- OPENAM-4225: Unable to modify some parts of policies in OpenAM console when not using amAdmin account. Unable to replace policy <policy_name> in organization dc=<org>
- OPENAM-4227: Set Password as Administrator does not work using AD-LDS (ADAM) User Store
- OPENAM-4229: Change Password as User does not work using AD-LDS (ADAM) User Store
- OPENAM-4235: RestAuthorizationDispatcherFilter is not thread-safe in its usage of the AuthZFilter

- OPENAM-4236: CookieUtils.addCookieToResponse only sends Max-Age attribute
- OPENAM-4248: Proxying SAML Passive Requests
- OPENAM-4252: StatusCode SAML response missing space
- OPENAM-4262: IDP Proxy should set destination depending on the Binding
- OPENAM-4320: NotificationServlet does not check for null before closing writer in finally block
- OPENAM-4346: Invalidating session on console in a multiserver setup fails if SFO is enabled
- OPENAM-4413: Agent sessions are affected by active session quotas when com.iplanet.am.session.agentSessionIdleTime is used
- OPENAM-4473: Couldn't find subschema errors in debug/Configuration
- OPENAM-4505: The rest oauth/access_token endpoint does not accept the realm as data in a POST request
- OPENAM-4587: Non Success StatusCode for SAML SLO results in HTTP 400
- OPENAM-4614: MergeAll Option cause a desynchronisation of the log rotation
- OPENAM-4644: Log file rotation isn't respected
- OPENAM-4764: REST Json response characterEncoding should be set to UTF-8
- OPENAM-4768: MigrateValidGotoSetting does not add new validation policy if there were no goto URL's to migrate.
- OPENAM-4773: OpenID Connect JWT typ header should be uppercase
- OPENAM-4804: SAE fails with No_App_Attrs:https error
- OPENAM-4856: HOTP auth module can not be used in auth chain if the username in sharedstate map does not 'match' the search attribute of the data store
- OPENAM-4919: DNMapper.realmNameToAMSDKName logic adding extra = when checking against orgAttr
- OPENAM-4923: Windows Desktop SSO module accepts Kerberos ticket from any realm/KDC
- OPENAM-4943: amUtilMsgs resource bundle missing from Fedlet distribution

- OPENAM-5034: Legacy password pages unable to handle special characters in username
- OPENAM-5040: ClusterStateService.checkServerUp() should get Input stream from connection
- OPENAM-5065: PLLClient should call getErrorStream() to get response body on IOException.
- OPENAM-5082: DJLDAPv3Repo setAttributes may add unnecessary objectclasses to modifyRequest.
- OPENAM-5120: SAML2 SP in a sub-realm not fully functional after OPENAM-474
- OPENAM-5148: URL links in email sent from REST forgotPassword or register is not URLEncoded
- OPENAM-5176: wscompile does not respect the java source and target versions
- OPENAM-5192: ErrorCode not set for the MessageLoginException
- OPENAM-5208: SAML2 SLO error on IDP with Session Synchronization when SP does not support SOAP binding
- OPENAM-5237: OAuth2 authorization consent page uses absolute URL in FORM tag
- OPENAM-5241: DN cache is never enabled since OPENAM-3822
- OPENAM-5260: Not possible to only sign the Response when using HTTP-POST binding
- OPENAM-5311: Default timelimit in Netscape SDK should be configurable
- OPENAM-5312: Initialization of a ServiceSchemaManager may block retrieval of already cached instances
- OPENAM-5472: NPE in #setAttributes when IdRepo fails to read directory schema

5.2 Limitations

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

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

OpenAM allows you to delete a referral policy even if policies depending on the referral still exist in the target realm. Deleting a referral policy that other policies depend on can cause problems during policy evaluation. You must therefore make sure that no policies depend on any referrals that you delete.

When deploying OpenAM components on Microsoft Windows in an IPv6 environment, you must use the Java 7 Development Kit on Windows (due to JDK-6230761, which is fixed only in Java 7).

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.

The XUI is experimental and not supported for production use. The only language locale available for the XUI at this time is US English, in the `/path/to/openam/webapps/XUI/locales` directory.

On hosts with pure IPv6 networks, OpenAM configuration has been seen to fail while starting the embedded OpenDJ directory server (OPENAM-3008).

5.3 Known Issues

The following important known issues remained open at the time release 11.0.3 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-110: Attribute name comparison in AttributeQueryUtil.isSameAttribute()
- OPENAM-774: Invalid characters check not performed.
- OPENAM-1105: Init properties sometimes don't honor final settings
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled
- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE

- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1456: Change of the agent group in the J2EE policy agent profile causes profile corruption
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1563: Servers and Sites pages may display password in clear text
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1755: the .NET fedlet uses invalid constants "True" "False" for some boolean XML attributes
- OPENAM-1773: DAS does not handle goto whitelisting
- OPENAM-1789: .NET Fedlet creates SAML2 IDs with incorrect format
- OPENAM-1811: DAS response serialization is not working as expected when using PAP
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1852: Oauth2 auth-module can not be used with DistAuth
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-2085: Unreliable policy evaluation results with com.sun.identity.agents.config.fetch.from.root.resource enabled

- OPENAM-2090: OPENAM_HOME/.version file is not updated
- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2155: Non printable characters in some files. Looks like most should be copyright 0xA9
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2170: Configure OAuth2 wizard fails to create policy in sub-realm
- OPENAM-2262: Configure OAuth2 wizard always enables refresh tokens
- OPENAM-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- OPENAM-2464: HOTP auth module sends 2 HOTP codes, if "Request new code" is clicked.
- OPENAM-2469: IdP initiated SSO endpoints should honor RelayState even when they're POSTed
- OPENAM-2537: SAML AuthContext mapper auth level setting inconsistencies
- OPENAM-2564: resource-based authentication with DistAuth not working
- OPENAM-2608: Restricted Token validation does not work in legacy REST API
- OPENAM-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-2777: Default user profile name field in device print page is unused
- OPENAM-2874: The OpenID Connect client registration endpoint does not set idTokenSignedResponseAlg to its default
- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-3056: Retrieving roles may fail when using more than one data store
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3152: CTS -- External Store Passwords configured in default server settings shown in clear text elsewhere
- OPENAM-3205: Missing labels in OAuth2 "Register a Client" page

- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3314: Hosted IDPs/SPs in COTs with Spaces
- OPENAM-3390: Japanese translation for OpenAM 11.0
- OPENAM-3442: CTS TokenType is missing an index
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3513: wrong l10n key in code, ssoadm delete-auth-instance fails on error reporting
- OPENAM-3547: Typos and errors of 11.0 additional fields
- OPENAM-3548: Items on the device print authn page are disordered
- OPENAM-3758: OAuth2 save consent when no scope is present is not working
- OPENAM-3780: Max number and percentage of tolerated difference between installed fonts is replaced by each other
- OPENAM-3783: Device print check of installed plugins and fonts does not work
- OPENAM-3825: Mismatch log is recorded when a user fails to change password in LDAP authn process
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3924: XUI is ignoring iplanet-am-admin-console-password-reset-enabled and requesting user password be entered anytime password is changed
- OPENAM-3969: 403 on using /json/<realm>/policies?_action=evaluate
- OPENAM-4003: Implement jwks_uri endpoint for OpenID connect service discovery
- OPENAM-4213: Root cause of MetaData import is lost when debug level is set to 'error'
- OPENAM-4215: ScopingImpl#makeImmutable should perform null checks
- OPENAM-4218: JAVA_HOME is not set correctly when installing admin tools (ssoadm, ampassword, amverifyarchive)

- OPENAM-4225: Unable to modify some parts of policies in OpenAM console when not using amAdmin account. Unable to replace policy <policy_name> in organization dc=<org>
- OPENAM-4227: Set Password as Administrator does not work using AD-LDS (ADAM) User Store
- OPENAM-4229: Change Password as User does not work using AD-LDS (ADAM) User Store
- OPENAM-4236: CookieUtils.addCookieToResponse only sends Max-Age attribute
- OPENAM-4248: Proxying SAML Passive Requests
- OPENAM-4252: StatusCode SAML response missing space
- OPENAM-4262: IDP Proxy should set destination depending on the Binding
- OPENAM-4264: IDPAccountMapper.getNameID() does not receive the SP Entity ID if there is no SPNameQualifier in the SAML request
- OPENAM-4320: NotificationServlet does not check for null before closing writer in finally block
- OPENAM-4340: Configurator is unable to handle special characters in passwords
- OPENAM-4346: Invalidating session on console in a multiserver setup fails if SFO is enabled
- OPENAM-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-4432: OpenAM upgrade fails when there is IP address/DNS condition set in policy
- OPENAM-4473: Couldn't find subschema errors in debug/Configuration
- OPENAM-4495: Agent profile attribute mapping does not allow to map the same profile attribute to different header names
- OPENAM-4496: REST sessions logout returns HTTP-403 Forbidden
- OPENAM-4498: SAML2MetaUtils.getMetaAliasByUri(...) does not use SAML2MetaManager.NAME_META_ALIAS_IN_URI
- OPENAM-4505: The rest oauth/access_token endpoint does not accept the realm as data in a POST request
- OPENAM-4517: GUI installer crashes and restarts in Safari

- OPENAM-4587: Non Success StatusCode for SAML SLO results in HTTP 400
- OPENAM-4768: MigrateValidGotoSetting does not add new validation policy if there were no goto URL's to migrate.
- OPENAM-4773: OpenID Connect JWT typ header should be uppercase
- OPENAM-4784: OpenID Connect support for RS256 in id_token_signing_alg_values_supported
- OPENAM-4943: amUtilMsgs resource bundle missing from Fedlet distribution
- OPENAM-5040: ClusterStateService.checkServerUp() should get Input stream from connection
- OPENAM-5183: CTS port settings are reverted to default when doing upgrade from AM 11 to AM 12
- OPENAM-5197: OAuth2 client fails to add access_token to tokeninfo call
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- OPENAM-5237: OAuth2 authorization consent page uses absolute URL in FORM tag
- OPENAM-5243: REST HTTP codes are different for some actions in AM 11.0.2 and AM 12
- OPENAM-5321: Cross realm session upgrade not handled properly by XUI
- OPENAM-5562: Users can't change password via XUI/REST API after OPENAM-3877 when using embedded
- OPENAM-5575: OpenAM install/upgrade page contains old year "Copyright © 2008-2014"
- OPENAM-5584: Proper function of session failover is disrupted by exceptions and browser refresh is needed

Chapter 6

How to Report Problems & Provide Feedback

If you have questions regarding OpenAM which are not answered by the documentation, there is a mailing list which can be found at https://lists.forgerock.org/mailman/listinfo/openam where you are likely to find an answer.

If you have found issues or reproducible bugs within OpenAM 11.0.3, report them in https://bugster.forgerock.org.

When requesting help with a problem, include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:
  - Machine type
  - Operating system and version
  - Web server or container and version
  - Java version
  - OpenAM version
  - Any patches or other software that might be affecting the problem

- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps

Chapter 7

Support

You can purchase OpenAM support subscriptions and training courses from ForgeRock and from consulting partners around the world and in your area. To contact ForgeRock, send mail to info@forgerock.com. To find a partner in your area, see http://forgerock.com/partners/find-a-partner/.