OpenAM 11.0.0 Release Notes

Mark Craig
Vanessa Richie
Mike Jang

Software release date: November 08, 2013

Publication date: February 20, 2014

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 11.0.0

OpenAM 11.0.0 fixes a number of issues, and provides the following additional features.

Important

This release contains fixes that resolve security issues within 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.

Major New Features

- This release uses the new OpenAM Core Token Service (CTS), with a more generalized token storage format for sessions, SAML Tokens, and OAuth Tokens. The LDAP schema have been extended for the CTS objects.
- OpenAM now fully supports OAuth 2.0 and OpenID Connect 1.0 as well as the required building blocks such as WebFinger, and JWT and related emerging standards.

  In addition to playing the role of OAuth 2.0 client and resource server, OpenAM can play the role of OAuth 2.0 authorization server. See *Managing OAuth 2.0 Authorization* for explanations, instructions, and examples.

  OpenAM support for OpenID Connect 1.0 extends OAuth 2.0 capabilities so clients can verify claims about the identity of the end user, get profile information for the end user, and manage end user sessions. OpenAM plays the role of OpenID Provider. See *Managing OpenID Connect 1.0 Authorization* for details.
- New, more modern RESTful web services are available for authentication, identity management, profile management, session management, Integrated Windows Authentication, and more. New endpoints are available under the URI `/json` where OpenAM is deployed, and are demonstrated in the *Developer Guide* chapter on *Using RESTful Web Services* in OpenAM.
- OpenAM adaptive authentication capabilities now include the Device Print authentication module (OPENAM-1375). The Device Print module uses characteristics of a system, including installed fonts, screen resolution, timezone, and also geolocation to uniquely identify the system. The Device Print module includes all of the functionality associated with the HOTP authentication module.

- OpenAM now supports Open Authentication (OATH, OPENAM-727). The module provides the user with a one-time password based either on a HMAC one-time password or a time-based one-time password. OATH lets you determine which type of one-time password is best for your users when they need to login with a password generating device. Devices can range from a smartphone to a dedicated device, such as YubiKey or any other OATH compliant device.

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

- OpenAM now fully supports Internet Protocol version 6 (IPv6) in addition to IPv4.

- OpenAM now fully supports Java 7 environments.

- OpenAM Session failover has been modified to be simpler to deploy (OPENAM-625). OpenAM 10.0.1 and earlier required the use of Open Message Queue and Berkeley DB Java Edition, which increased the complexity and amount of time required to get session failover working. OpenAM now writes session data to the configuration data store instead. This implementation also can be used to make sessions persist across restart for single OpenAM servers. The current implementation requires that you use OpenDJ for the configuration data store.

- OpenAM now includes a preview of the cloud Dashboard service, part of allowing user self-management of web based applications. (OPENAM-2019).

- OpenAM now bundles OpenDJ 2.6.

- A new UI is available for experimental, non-production use. Informally known as the XUI, this JavaScript based UI uses LESS CSS for UI configuration.

Additional New Features

- The Persistent Cookie module has been added to support configuration of cookie lifetimes, based on requests and a maximum time.

- IBM WebSphere 8 is now a supported platform. See *Preparing IBM WebSphere* in the *Installation Guide* for details on how to setup WebSphere 8.0 and 8.5 before deploying OpenAM.

- The policy tree index has been updated so that resources first check the root level of a realm first. The tree will be created from this level, and any subsequent referrals will create another tree specific to the realm where the referral was retrieved. This conserves memory and reduces the amount of time required to load the tree. An intelligent indexing model now assists with quickly identifying relevant policy rules for the resource being authorized.
- The zero page login has been modified so that administrators can disable the functionality. The zero page login process is the ability of the user to login using only GET parameters, which presents a possible security issue. Zero page login is now disabled by default (OPENAM-2354).
- OpenAM now provides an account expiration post authentication plugin to set an account expiration date on successful login.
- Remote clients that register notification URLs with OpenAM can now successfully deregister on shutdown (OPENAM-2766, OPENAM-2765), preventing OpenAM from trying to notify applications that are no longer running.
- OpenAM now lets you configure the profile attribute name for email used by the password reset module (OPENAM-2604).
- OpenAM now provides a mechanism for Identity Providers to use private key passwords that differ from the password stored in OpenAM's `.keypass` file (OPENAM-2306).
- OpenAM Java Fedlet `SPACSUtils` can now find the `metaAlias` in either the URI or the query string parameters (OPENAM-2258).
- OpenAM now provides a mechanism to supply static values when setting up attribute mapping for a SAML 2.0 Identity Provider or Service Provider (OPENAM-2184).
- OpenAM's LDAP authentication module now supports Samba 4 LDAP response codes (OPENAM-1826).
- OpenAM's OATH authentication module's minimum password length is now configurable (OPENAM-1765).
- The AMLoginModule now lets authentication modules retrieve the list of current session tokens for a user (OPENAM-1721).
- OpenAM Console again includes a generic LDAP data store option (OPENAM-1656).
- OpenAM's IDPAdapter now provides additional hooks for customization. This improvement introduces changes to the API that affect custom IDPAdapters (OPENAM-1623).

- Legacy naming conventions have been changed to conform to the current product name, OpenAM. This includes the OpenAM bootstrap file (OPENAM-1555). `$HOME/.openamcfg/` is the new name for `$HOME/.openssocfg/`. If you upgrade, OpenAM still supports use of `$HOME/.openssocfg/`, and does not rename the folder. For new OpenAM installs, OpenAM creates the directory with the new name, `$HOME/.openamcfg/`, at configuration time. Other files, such as the `openam.war` file, and paths have been modified to ensure consistency with the naming conventions.

- When running as a Service Provider, OpenAM no longer requires that you enable module-based authentication (OPENAM-1470).

- OpenAM now has better support for using a reverse proxy for federation when DAS is also deployed (OPENAM-1454).

- OpenAM now allows use of a read-only data store with a non-transient NameID during SAML 2.0 federation (OPENAM-1427).

- The ssoadm command now includes a get-sub-cfg subcommand (OPENAM-1348).

- OpenAM IDPs can now proxy all requests whether or not the SP allow the behavior (OPENAM-1266).

- When working with Salesforce.com as an SP, OpenAM can now perform SP-initiated SSO, can use any arbitrary URL for the entityID/default endpoint, and automatically selects the last attribute from the first page as the default Federation ID (OPENAM-1232).

- The REST authenticate command now has a parameter to specify the client IP address (OPENAM-1048).

- OpenAM is now built with Maven. Maven artifacts continue to be uploaded to the ForgeRock Maven repository (OPENAM-739).

- OpenAM's OATH module supports shared keys and counters (OPENAM-727).

- You can now prevent OpenAM from caching subject evaluations for policy decisions (part of the fix for OPENAM-24).

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

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

- The C SDK for OpenAM has been simplified. Nightly builds are all available as ZIP files, for Linux, Solaris x86, Solaris SPARC, and Windows operating systems, for both 32- and 64-bit varieties.

  For C SDK product versions and support offerings, contact info@forgerock.com.

Chapter 2. Before You Install OpenAM 11.0.0 Software

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

2.1. Java Requirements

This release of OpenAM requires Java Development Kit 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 (12.1.2)

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. OpenAM Changes & Deprecated Functionality

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

3.1. Important Changes to Existing Functionality

- When you create a new OpenAM custom configuration that uses an external LDAP directory server for the configuration data store, you must use a root suffix DN with at least two domain components, such as `dc=example,dc=com`.
- The way OpenAM matches URLs for policy rules now better reflects the behavior documented in the *Administration Guide* under *To Configure a Policy For a Web Site*.

  In particular, the `*` wildcard matches *one or more characters when used at the end of a rule*, or zero or more characters otherwise. Also, trailing slashes are not recognized as part of a resource name. With previous releases a policy rule for `http://example.com/*` would match `http://example.com/`. With this release, you need either two rules for this, one for `http://example.com/` and another for `http://example.com/*`, or else a rule such as `http://example.com*`.

  If you have policies that were created with an earlier version of OpenAM, check that use of wildcards in those policies indeed matches the documented behavior, and update policies as necessary.
- 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.

3.2. 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 3.1. 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* in 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.

3.3. 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 4. OpenAM Fixes, Limitations, & Known Issues

OpenAM issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM. This chapter covers the status of key issues and limitations at release 11.0.0.

Important

OpenAM 11.0.0 policy evaluation is designed for use with OpenAM policy agents version 3.3.0. Backward compatibility with earlier agents will be provided in a forthcoming maintenance release.

4.1. Key Fixes

The following bugs were fixed in release 11.0.0. For details, see the OpenAM issue tracker.

- OPENAM-3112: REST authenticate resource should cope with charset provided with Content-Type header
- OPENAM-3105: CachedSubEntries.getSubEntries() shouldn't sort LDAPSearchResults
- OPENAM-3057: DAS /UI/Logout does not work.
- OPENAM-3050: Revisit default HBCF settings
- OPENAM-2989: Auth REST endpoint shows HTTP 500 for invalid JWT
- OPENAM-2982: AuthLoginException should call super constructor
- 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-2875: Invalid group name error when group does not exist in LDAP
- OPENAM-2806: Resource leak in IOUtils implementation

- OPENAM-2764: IdRepoJAXRPCObjectImpl and DirectoryManagerImpl notification URL cache can contain duplicate 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-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-2645: Should destroy session created by OAuth 2 Token generation in Client Credentials Grant flow and other flows.
- OPENAM-2644: unit test fail with JDK 1.6
- OPENAM-2633: Multivalued OAuth2 scope attributes - only one attribute value is being returned
- OPENAM-2628: Case insensitivity for realms is not enforced in AuthenticateToRealmCondition.getConditionDecision
- OPENAM-2610: Exception when trying to set binary attributes using ClientSDK
- OPENAM-2596: ssoadm show-privileges result misleading if no identity with given type exists
- OPENAM-2580: DAS loses its configuration on JBoss after a restart
- OPENAM-2535: NPE in AuthClientUtils if the IP address header does not exist
- OPENAM-2530: RemoteHttpServletRequest should store headers in CaseInsensitiveHashMap
- OPENAM-2514: Remove-privileges command doesn't handle All Authenticated Users role correctly in subrealms

- OPENAM-2505: Incorrect status code for locked account in AMLoginContext.java
- OPENAM-2502: show-privileges command returns incorrect values for subrealms
- OPENAM-2494: Request serialization fails on weblogic
- 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-2430: Persistent cookie authentication does not set authlevel
- OPENAM-2426: Calling Logout and passing a goto URL parameter with an expired session causes the goto URL to be ignored.
- OPENAM-2414: Session quota does not work when SFO is enabled
- 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-2383: AMRecordDataEntry shouldn't use commons codec Base64 implementation
- OPENAM-2369: Export Agent Configuration in the console fails with exception if locale is set to fr
- OPENAM-2358: AD authentication module: missing bundle string for insufficient password quality error
- OPENAM-2354: Zero Page Login should be configurable
- OPENAM-2351: Gradle build issues when using openam-core
- OPENAM-2347: The OAuth2 provider issues a null scoped access token on refresh_token
- OPENAM-2284: ReplayPasswd fails with NPE if request is not available

- OPENAM-2274: Default SP Account Mapper can't autofederate using the NameID
- OPENAM-2268: Unable to get LDAP attributes using the tokeninfo endpoint using OAuth2.
- 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-2257: WebSphere 8.5 Configurator failed at Reinitializing system properties
- OPENAM-2247: After upgrading on Windows the SFO suffixes are not created in the configstore
- OPENAM-2242: The OAuth2 ClientVerifiyerImpl should always use the application module when authenticating an oauth2 client.
- OPENAM-2231: OAuth2 users in subrealms are not authenticated correctly when using the class UserIdentityVerifier.java
- OPENAM-2229: OAuth2 schema is not applied to external configuration store
- OPENAM-2224: Deadlock in LDAPv3EventService
- OPENAM-2212: AMHostnameVerifier does not work if no keystore is defined
- OPENAM-2208: Document the new feature of enclosing the profile attribute name in double quotes to make it a static value.
- OPENAM-2183: Install of AM in WebLogic 12c container fails extracting OpenDJ files
- OPENAM-2167: Oracle iPlanet Web Server policy agent install instructions incorrect
- OPENAM-2154: cert-auth module does not succeed if CRL update fails
- OPENAM-2153: cert-auth module does not allow to disable CRL in-memory cache
- OPENAM-2152: cert-auth module does not allow storage of several CRLs for the same issuer
- OPENAM-2134: IDPProxy fails to redirect to IDP with an exception. NameIDPolicy is not available in the AuthRequest from remote SP

- OPENAM-2132: REST isTokenValid should return false when the passed in token is not valid
- 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-2102: LDAPConnection does not handle unsolicited extended responses
- OPENAM-2097: Adaptive risk module does not describe which GeoIP client is used and where to obtain the GeoIP database file
- OPENAM-2081: Document JMX service URL for RMI monitoring
- OPENAM-2064: Missing forgerock-am-dashboard-service attribute to provision new Subject to non OpenDJ external user store
- OPENAM-2059: ssoadm export-svc-cfg throws NullPointerExecption if no SubConfiguration exists for a given service
- OPENAM-2053: Log Number of History files count is ignored when log rotation is based on time
- OPENAM-2050: URL Encoding the Redirect URI for the OAuth2 provider for OpenAM
- OPENAM-2032: OAuth 2.0 client agent Export Configuration can lose list values
- OPENAM-2018: EntitltmentThreadPool has a risk of infinite loop during web container shutdown
- OPENAM-1985: RuntimeException occurs when clicking 'Local Site Properties' button
- 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-1934: SAML2 passive authentication requests handled incorrectly

- OPENAM-1933: ReplayPasswd only supports passwords with max 16 characters
- OPENAM-1906: Common REST returning 404 when retrieving users from realms
- OPENAM-1816: ssoadm comand to create a realm may cause duplicate entries to be written to embedded LDAP if multiple servers are running
- OPENAM-1655: AttributeQueryUtil ignores configured SPAttributeMapper
- OPENAM-1641: LoginState paramHash is not always correctly initialized when using request serialization
- OPENAM-1630: SAML metadata signature code does not conform to SAML recommendations
- OPENAM-1607: After Session Expire OpenAM throws SSOException: Session state invalid
- OPENAM-1569: Remove objectclass=ldapsubentry from LDAP requests
- OPENAM-1544: Request headers are not proxied for GET requests
- OPENAM-1517: Inconsistency in getting Client IP
- OPENAM-1512: LDAPConnectionPool is not re-initialized correctly if failover server is down
- OPENAM-1511: closing of LDAPConnection in LDAPConnectionPool is not synchronized
- OPENAM-1496: People container name/value configs are not always correctly used
- OPENAM-1288: Registered Authentication Post Processors are not called during SAML single logout
- OPENAM-1245: Configuring datastore for failover with persistent search enabled causes exception logging loop
- OPENAM-1180: Login URL problems when using Federation
- OPENAM-1110: ssoadm fails with NullPointerException and does not terminate
- OPENAM-1083: Using Federation redirects with the valid goto URL whitelist causes problems

- OPENAM-973: LDAPConnectionPool#decreaseCurrentConnection() could throw ArrayIndexOutOfBound exception
- OPENAM-844: If Directory Server is started after OpenAM, LDAPv3Repo will never recover
- OPENAM-808: OpenAM instances hung when starting at the same time.
- OPENAM-751: It should be possible to disable 'X-DSAMEVersion' http-header
- OPENAM-507: Adding to existing deployment fails for non-default Org. Auth. configuration
- OPENAM-340: Failed to create new Authentication Context error when zero page login fails on DAS
- OPENAM-299: LDAPv3Repo tries to query attributes for non-existing users too

4.2. 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.

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).

4.3. Known Issues

The following important known issues remained open at the time release 11.0.0 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-3408: Fix for OPENAM-2626 leads to concurrent modification exception
- OPENAM-3283: CTS Reaper fails to restart
- OPENAM-3270: openam/.version not updated after upgrade
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3239: OAuth 2 client properties randomly disappears after upgrade from OpenAM 10.1 to OpenAM 11
- OPENAM-3230: When I make Upgrade from AM 955 to AM 11 upgrade report show me incorrect version of an existing instance
- OPENAM-3227: OAuth2 Authentication Module does not utilise com.sun.identity.shared.encode.CookieUtils when creating new cookies.
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3216: CTS Token timeout incorrect after changing token idle time
- OPENAM-3210: In CDSSO scenario no Logout is triggered when choosing 'yes' on 'new_org.jsp'
- OPENAM-3207: PLLRequestServlet should log an errror if the configured maximum request size is exceeded
- OPENAM-3205: Missing labels in OAuth2 "Register a Client" page
- OPENAM-3204: Goto URL validation can choke on relative URLs
- OPENAM-3202: RelayState is validated as a URL
- OPENAM-3184: Insufficient error logging when 'agent profile' can not be found by CDCServlet

- OPENAM-3166: Need better control for cookies when using postToAppLogout feature
- OPENAM-3165: NPE during export-svc-cfg
- OPENAM-3160: AuthContext failover doesn't work
- OPENAM-3113: DJLDAPv3Repo should properly set the LDAP error codes on IdRepoException
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3065: Misconfiguring CTS causes issues with IDRepo unable to read realms
- OPENAM-3056: Retrieving roles may fail when using more than one data store
- OPENAM-3048: RESTful authentication using curl doesn't work on the WebLogic 12c (12.1.1.0)
- OPENAM-2922: SP initiated SLO can fail with IllegalStateException
- OPENAM-2874: The OAuth2 client registration endpoint does not set idTokenSignedResponseAlg to its default
- OPENAM-2846: The REST auth API should provide a way to set the client IP address in a secure way
- OPENAM-2760: Validation of gotoOnFail URLs
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-2712: Adaptive.getIdentity prints 'More than one user found' when no user was found
- OPENAM-2705: People container name/value configs are not always correctly used - backport
- OPENAM-2656: PrefixResourceName#compare() strips off trailing backslash in PathInfo
- OPENAM-2626: Synchronization causes lock contention in IdRepoJAXRPCObjectImpl
- OPENAM-2608: Restricted Token validation does not work in legacy REST API
- OPENAM-2564: resource-based authentication with DistAuth not working

- OPENAM-2537: SAML AuthContext mapper auth level setting inconsistencies
- OPENAM-2469: IdP initiated SSO endpoints should honor RelayState even when they're POSTed
- OPENAM-2460: Policy evaluation may hang with large number of matching referral privileges
- OPENAM-2409: Special characters in alternative naming attribute are unescaped
- OPENAM-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- OPENAM-2262: Configure OAuth2 wizard always enables refresh tokens
- OPENAM-2170: Configure OAuth2 wizard fails to create policy in sub-realm
- OPENAM-2168: Authentication Success Rate and Authentication Failure Rate are always 0
- OPENAM-2155: Non printable characters in some files. Looks like most should be copyright 0xA9
- OPENAM-2137: DSConfigMgr can hide exception root causes
- OPENAM-2085: Unreliable policy evaluation results with com.sun.identity.agents.config.fetch.from.root.resource enabled
- OPENAM-2023: Federation Connectivity Test fails with Account termination is not working
- OPENAM-1946: Password change with AD does not work when old password is provided
- OPENAM-1945: Default Configuration create invalid domain cookie
- OPENAM-1921: REST GET for user "*" returning first user listed
- OPENAM-1892: Only Accept certificate for authentication if KeyUsage is correct
- OPENAM-1886: Session invalidated on OpenAM server is not deleted from SFO datastore
- OPENAM-1852: Oauth2 auth-module can not be used with DistAuth
- OPENAM-1839: LDAPConnectionPool is not recovered

- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- OPENAM-1811: DAS response serialization is not working as expected when using PAP
- OPENAM-1739: HOTP module may ignore SMTP settings in the configuration
- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1642: Chain based UI customization is not case insensitive
- OPENAM-1563: Servers and Sites pages may display password in clear text
- OPENAM-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1330: 'sharedState' in LoginContext should be thread safe
- OPENAM-1323: Unable to create session service when no datastore is available
- OPENAM-1317: With ssoadm create-agent, default values are handled differently for web agents and j2ee agents
- OPENAM-1269: Entitlements are incorrectly converted to policies
- OPENAM-1237: Property 'noSubjectKeyIdentifier' is missing in fmWSSecurity.properties
- OPENAM-1219: SAML 2 metadata parsing breaks in glassfish 3.1.2
- OPENAM-1194: Unable to get AuthnRequest error in multiserver setup
- OPENAM-1181: Improperly defined applications cause the policy framework to throw NPE
- OPENAM-1137: Error message raised when adding a user to a group
- OPENAM-1111: Persistent search in LDAPv3EventService should be turned off if caching is disabled
- OPENAM-1109: AdminTokenAction doesn't clear invalid SSOToken
- OPENAM-1105: Init properties sometimes don't honor final settings

- OPENAM-774: Invalid characters check not performed.
- OPENAM-752: AgentsRepo#getAttributes fails to get agent information occasionally leading to server restart
- OPENAM-688: REOPEN -LDAP Error 80 can result in build up of LDAPv3EventService::RetryTask objects
- OPENAM-651: internalsession object can grow in size leading to non-linear scaling in the session failover db
- OPENAM-401: Missing response attribute on first logon after OpenAM restart
- OPENAM-294: ssoadm: create and update
- OPENAM-291: SelfWrite permissions are denied to sub realms
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings

Chapter 5. How to Report Problems & Provide Feedback

If you have 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 11.0.0, report them in https://bugster.forgerock.org.

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

- Description of the problem, including when the problem occurs and its impact on your operation
- Description of the environment, including the following information:
  - Machine type
  - Operating system and version
  - Web server or container and version
  - Java version
  - OpenAM version
  - Any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any relevant access and error logs, stack traces, or core dumps

Chapter 6. Support

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