Release Notes

OpenAM 11

David Goldsmith
Gene Hirayama
Chris Lee

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 in OpenAM 11.0.0

OpenAM 11 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.

1.1. What's New in OpenAM 11.0.3

OpenAM 11.0.3 is a maintenance release that introduces new features and enhancements to OpenAM.

- **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).

- **New goto/gotoOnFail URL Validation Service**. OpenAM now provides a new "Validation Service" for URL whitelisting. OpenAM uses the Validation Service during the authentication process on the server and DAS-side for `goto` and `gotoOnFail` URLs, and during the SAML authentication process on the server and fedlet-side for Relay State URLs.

  You can set the `goto`/`gotoOnFail` URL lists on the OpenAM console via Access Control > *realm* > Services > Validation Service. The new property for the Validation Service is "`openam-auth-valid-goto-resources`."

  The Validation Service also uses a new delegation policy that grants the necessary permissions to the agent accounts, which allows them to access the valid `goto` URL domain lists.

  The `goto` URL validation logic has been extracted out to a separate class called `RedirectUrlValidator`, which can be used from both `openam-core` and `openam-federation-library`.

  This feature is not supported as a patch and is only available by means of a new installation or an upgrade. The upgrade wizard ensures the migration of existing valid `goto` and `gotoOnFail` domains to the new service and ensures that the new delegation policy is added to the system. (OPENAM-1773).

Note

You must check that the `goto` and `gotoOnFail` redirects are still working after an upgrade if your `goto` and `gotoOnFail` URL lists are not fully formed.

- **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 now allows for the verification of password reset tokens through the REST API. For more information, see (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. What's New in OpenAM 11.0.2

OpenAM 11.0.2 is a maintenance release that introduces new features and enhancements to OpenAM.

- **OAuth 2.0 Refresh Token Renewal**. OpenAM now issues a new refresh token when an access token is refreshed (OPENAM-3951).
- **Quicker UI Customization**. While customizing the UI, you can set the advanced server property, `org.forgerock.openam.core.resource.lookup.cache.enabled`, to `false` to allow OpenAM immediately to pick up changes to the files as you customize them (OPENAM-3989). You can set advanced server properties in OpenAM Console under Configuration > Servers and Sites > *Server Name* > Advanced. For production servers, leave this set to the default, `true`.
- **Whitelist for Custom Login URIs**. OpenAM now includes a property that specifies a whitelist for custom login URIs so that the CDCServlet and the Distributed Authentication UI (DAS) can check login URI values against those in the whitelist.

  The property name is `org.forgerock.openam.cdc.validLoginURIs`. If you use custom login URIs in your deployment, add them to the whitelist, separating URIs with commas, setting `org.forgerock.openam.cdc.validLoginURIs` to `/UI/Login,/customLoginURI` for example. You can set this property in OpenAM console under Configuration > Servers and Sites > Default Server Settings > Advanced. The default value is `/UI/Login`.

  The CDCServlet and DAS accept only `loginURI` values that match one of the values in the whitelist. OpenAM strips query strings from `loginURI` values before comparing them with the values in the whitelist, so only include the URIs, not query string parameters.
- **Configurable DN Cache for LDAP Data Stores**. OpenAM now has the capability to enable and disable DN caching. DN caching helps avoid DN lookups that can happen in bursts during authentication. (OPENAM-3822).

You can configure this feature as part of a Data Store profile. To configure DN caching in OpenAM console, browse to Access Control > *Realm Name* > Data Stores > *Data Store Name* > Cache Control.

- **CTS Connection Management Improvement** (OPENAM-3219).
- **Debug Log Improvements**. AMSetupServlet now displays all configuration parameters in debug logs when the log level is set to ERROR (OPENAM-2089).

  Debug log improvements have also reduced spurious stack traces that were logged during authentication processing (OPENAM-371).
- **Attributes Populated on Dynamic User Creation**. When creating users dynamically, OpenAM now populates all attributes that are provided and mapped for SAML 2.0 federation (OPENAM-474).
- **Policies Support Additional HTTP Operations**. Policies now support all types of HTTP operations, not just GET and POST (OPENAM-336).

1.3. What's New in OpenAM 11.0.1

OpenAM 11.0.1 is a maintenance release that introduces new features and enhancements to OpenAM.

Product Enhancements

- OpenAM REST API now allows logout with a restricted token (OPENAM-3484).
- Restricted token `asString` values now use a hash in order to limit their size (OPENAM-3414).
- The SAML 2.0 IDP Adapter interface now includes a `preSignResponse` method (OPENAM-3190).

  This method makes it possible to adjust the content of a SAML response in order to add a custom SAML extension for example. The method is called after the SAML Response object is created but before the SAML Response is signed or encrypted.
- The default SAML 2.0 IDP attribute mapper implementation now provides a way to Base64 encode binary attributes (OPENAM-2767).

  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
```

- The `AttributeQueryUtil.getAttributeMapForFedlet` method now handles failure status codes received from the IDP (OPENAM-1749).

1.4. What's New in OpenAM 11.0.0

OpenAM 11.0.0 is a major release that introduces new features and enhancements to OpenAM.

Product Enhancements

- 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* in the *Administration Guide* 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* in the *Administration Guide* 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 the *Developer's Guide* 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* 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

Security Advisories in OpenAM 11

ForgeRock issues security advisories in collaboration with our customers and the open source community to address any security vulnerabilities transparently and rapidly. ForgeRock's security advisory policy governs the process on how security issues are submitted, received, and evaluated as well as the timeline for the issuance of security advisories and patches.

For more information on ForgeRock's security advisory policy, click the following link: http://www.forgerock.com/services/security-policy/

2.1. Security Advisories in OpenAM 11.0.3

- **Issue #201502-01: Authorization bypass via path traversal**. It is possible to gain unauthorized access to policy protected resources if multi-level wildcards (“*”) are being used within policies and certain endpoints are protected with a strong policy and the attacker has access to a less protected resource.

  Severity: **Critical**

  For more information, see OpenAM Security Advisory #201502-01.

- **Issue #201502-02: XML Signature Wrapping in SAML 1.x**. It is possible for attackers to construct SAML 1.x protocol messages with arbitrary content that will be considered valid by OpenAM’s XML Signature verification logic. Note that this mainly affects deployments where OpenAM acts as a SAML 1.x Relying Party.

  Severity: **High or Critical (if OpenAM acts as a Relying Party)**

  For more information, see OpenAM Security Advisory #201502-02.

- **Issue #201503-01: Cross Site Request Forgery**. When “Prompt user for old password” feature is disabled (which is the default value) it is possible for a skilled attacker to change the user’s password without their knowledge.

  Severity: **Critical**

  For more information, see OpenAM Security Advisory #201503-01.

- **Issue #201404-01: Denial of Service vulnerability – CVE-2014-7246**. In environments where more than one OpenAM server has been configured, it is possible that an authenticated attacker can

construct and send a single request that triggers an infinite loop, occupying one or more instances in the deployment until the affected instances are restarted.

Severity: **Critical**

For more information, see OpenAM Security Advisory #201404-01.

- **Issue #201502-03: Authentication bypass in WS-Federation**. When OpenAM acts as a WS-Federation Identity Provider and more than one realm has been configured it is possible to obtain access to Relying Parties that have been configured in a different realm than the current session's realm.

  Severity: **High**

  For more information, see OpenAM Security Advisory #201502-03.

- **Issue #201502-04: Denial of Service**. It is possible to cause a denial of service by accessing a specific OpenAM endpoint.

  Severity: **High**

  For more information, see OpenAM Security Advisory #201502-04.

- **Issue #201502-05: Authorization bypass in the REST API**. When self registration is enabled it is possible to use the sent out `tokenId` and `confirmationId` to register end-users in different realms than originally intended.

  Severity: **High**

  For more information, see OpenAM Security Advisory #201502-05.

- **Issue #201502-06: Unauthorized access** . A bug in the policy evaluation framework makes it possible for an authenticated user to gain unauthorized access to certain resources regardless of the policy evaluation mode (self/subtree). The issue may occur if there is a policy rule defined in the format of `http*://example.com:*/index.html`. In this case the last wildcard may match the URI as well, not just the port number.

  Severity: **High**

  For more information, see OpenAM Security Advisory #201502-06.

- **Issue #201502-07: Cross Site Scripting**. OpenAM is vulnerable to cross-site scripting (XSS) attacks which could lead to session hijacking or phishing.

  As part of an automated scan it has been detected that the following endpoints are vulnerable against cross-site scripting and/or open redirect attacks:

  Affecting 9-9.5.5, 10.0.0-10.0.2, 10.1.0-Xpress and 11.0.0-11.0.2:

  /openam/WSFederationServlet (Core Server, Server Only)

/openam/task/CreateRemoteIDP (Core Server)
/openam/task/CreateRemoteSP (Core Server)
/openam/federation/ImportEntity (Core Server)
openam/UI/Login (Core Server, Server Only, DAS)
/openam/console/ajax/AjaxProxy.jsp (Core Server)

Severity: **High**

For more information, see OpenAM Security Advisory #201502-07.

- **Issue #201503-02: Cross Site Scripting**. OpenAM is vulnerable to cross-site scripting (XSS) attacks which could lead to session hijacking or phishing. It has been detected that the following endpoint is vulnerable to cross-site scripting attacks:

  /openam/oauth/registerconsumer.jsp (Core Server, Server Only)

  Severity: **High**

  For more information, see OpenAM Security Advisory #201503-02.

- **Issue #201502-08: Information leakage**. It is possible to obtain information about the deployment by sending well crafted requests to OpenAM.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-08.

- **Issue #201502-09: Insecure password storage**. It has been discovered that the following passwords were stored in plain text in the configuration:

  com.sun.identity.crl.cache.directory.password
  org.forgerock.services.cts.store.password

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-09.

- **Issue #201502-10: Open Redirect**. Due to a bug in the goto URL validation subsystem it was possible to perform Open Redirect attacks by sending the end-users to specifically constructed URLs that were considered valid by the goto URL validator.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-10.

- **Issue #201502-11: Login CSRF**. It is possible to perform login CSRF attacks using the built-in authentication endpoints.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-11.

- **Issue #201502-12: Login CSRF in OAuth2 authentication module**. The OAuth2 authentication module is vulnerable to Login CSRF attacks.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-12.

- **Issue #201502-13: Business Logic Vulnerability**. If more than one realm is configured in OpenAM, it is possible for an end-user in one realm to access an existing OAuth2 access token from a different realm's end-user who shares the same username.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201502-13.

- **Issue #201503-03: Password recorded as plain text during install**. When performing new installations of OpenAM 11.0.2 and 12.0.0 the installation properties are recorded in the install log at the end of the OpenAM installation process to aid diagnostic analysis. In the case of configuring OpenAM to use an external user store, the user data store's LDAP password will be stored in plain text in the installation log file.

  Severity: **Medium**

  For more information, see OpenAM Security Advisory #201503-03.

- **Issue #201502-14: Business Logic Vulnerability**. It is possible to perform self registration with existing `tokenId` and `confirmationId` values after self registration has been disabled (as long as the tokens remain valid).

  Severity: **Low**

  For more information, see OpenAM Security Advisory #201502-14.

Chapter 3

Before You Install OpenAM 11.0.0 Software

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

3.1. 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.

3.2. 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.

3.3. 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.

3.4. 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

3.5. 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

3.6. 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* in the *Administration Guide*.

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

3.7. Supported Upgrade Paths

ForgeRock supports upgrades from the following versions to this version of OpenAM:

Table 3.1. Supported Upgrades

Version	Upgrade Supported?
OpenAM 9.0.x	No
OpenAM 9.5.x	Yes
OpenAM 10.0.x	Yes
OpenAM 11.0.x	Yes

For more information, see Checking your product versions are supported in the *ForgeRock Knowledge Base*.

3.8. 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 4

Installing or Upgrading

This chapter covers installing and upgrading OpenAM 11 software.

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

- If you are installing OpenAM for the first time, see the Installation Guide.
- If you have already installed OpenAM, see the Upgrade Guide.

  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.

Chapter 5

OpenAM Changes & Deprecated Functionality

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

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

5.1. Important Changes to Functionality in OpenAM 11

The following functionality has been changed in OpenAM 11:

5.1.1. Important Changes to Existing Functionality in OpenAM 11.0.3

These changes are new in OpenAM 11.0.3.

- **Agent Group Membership Information**. The agent group membership information is now stored in the agent's `agentgroup` attribute. When configuring agents, make sure that the referenced agent group already exists in the configuration.

  For details, see the explanation in (OPENAM-718).

- **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).

- **New goto/gotoOnFail URL Validation Service**. OpenAM now provides a new "Validation Service" for URL whitelisting. OpenAM uses the Validation Service during the authentication process on the server and DAS-side for `goto` and `gotoOnFail` URLs, and during the SAML authentication process on the server and fedlet-side for Relay State URLs.

You can set the `goto`/`gotoOnFail` URL lists on the OpenAM console via Access Control > *realm* > Services > Validation Service. The new property for the Validation Service is "`openam-auth-valid-goto-resources`."

The Validation Service also uses a new delegation policy that grants the necessary permissions to the agent accounts, which allows them to access the valid `goto` URL domain lists.

The `goto` URL validation logic has been extracted out to a separate class called `RedirectUrlValidator`, which can be used from both `openam-core` and `openam-federation-library`.

This feature is not supported as a patch and is only available by means of a new installation or an upgrade. The upgrade wizard ensures the migration of existing valid `goto` and `gotoOnFail` domains to the new service and ensures that the new delegation policy is added to the system. (OPENAM-1773).

Note

You must check that the `goto` and `gotoOnFail` redirects are still working after an upgrade if your `goto` and `gotoOnFail` URL lists are not fully formed.

- **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 now allows for the verification of password reset tokens through the REST API using the single REST API action: `/json/users?_action=confirm`. (OPENAM-3748).

- **Proxying Passive SAML Authentication Requests**. OpenAM acting as an IdP proxy is now able to proxy passive SAML authentication requests and replay `NoPassive` responses. (OPENAM-4248).

- **We should no longer redistribute the RSA SecurID library**. OpenAM no longer redistributes the RSA SecurID library. This means that if you are upgrading OpenAM, SecurID authentication will fail unless your obtain the library directly from RSA and place it in your classpath. (OPENAM-4380).

- **Specifying Trusted Realms using the WindowsDesktopSSO Authentication Module**. The WindowsDesktopSSO authentication module now allows you to specify a list of trusted realms. When the setting is specified, Kerberos tokens issued by those realms will only be accepted. (OPENAM-4923).

- **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>`.

5.1.2. Important Changes to Existing Functionality in OpenAM 11.0.2

These changes are new in OpenAM 11.0.2.

- Valid loginURIs are now set using a property that specifies a whitelist for custom login URIs so that the CDCServlet and the Distributed Authentication UI (DAS) can check login URI values against those in the whitelist.

  The property name is `org.forgerock.openam.cdc.validLoginURIs`. If you use custom login URIs in your deployment, add them to the whitelist, separating URIs with commas, setting `org.forgerock.openam.cdc.validLoginURIs` to `/UI/Login,/customLoginURI`, for example. You can set this property in OpenAM console under Configuration > Servers and Sites > Default Server Settings > Advanced. The default value is `/UI/Login`.

  The CDCServlet and DAS accept only loginURI values that match one of the values in the whitelist. OpenAM strips query strings from loginURI values before comparing them with the values in the whitelist, so only include the URIs, not query string parameters.

- 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).

5.1.3. Important Changes to Existing Functionality in OpenAM 11.0.1

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.

5.1.4. Important Changes to Existing Functionality in OpenAM 11.0.0

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`.

5.2. Deprecated Functionality in OpenAM 11

The following functionality has been deprecated in OpenAM 11 and will likely be removed in a future release:

5.2.1. Deprecated Functionality in OpenAM 11.0.3

There are no deprecated functionality in OpenAM 11.0.3.

5.2.2. Deprecated Functionality in OpenAM 11.0.2

There are no deprecated functionality in OpenAM 11.0.2.

5.2.3. Deprecated Functionality in OpenAM 11.0.1

There are no new deprecated functionality for OpenAM 11.0.1.

5.2.4. Deprecated Functionality in OpenAM 11.0.0

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/logout

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

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

Table 5.1. REST End Points

Deprecated in the *Administration Guide* URIs	**Newer Evolving in the *Administration Guide* 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 the *Developer's Guide* 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.

5.3. Removed Functionality in OpenAM 11

The following functionality has been removed in OpenAM 11:

5.3.1. Removed Functionality in OpenAM 11.0.3

- The `sun-idrepo-ldapv3-config-connection-mode` property replaces `sun-idrepo-ldapv3-config-ssl-enabled`, which has been removed from the configuration schema (`sunIdentityRepositoryService`).

  For more information, see OPENAM-3714.

- The `openam-auth-ldap-connection-mode` property replaces `iplanet-am-auth-ldap-ssl-enabled`, which has been removed from the configuration schema (`sunAMAuthADService` and `iPlanetAMAuthLDAPService`).

  For more information, see OPENAM-5097.

5.3.2. Removed Functionality in OpenAM 11.0.2

There are no removed functionality in OpenAM 11.0.2.

5.3.3. Removed Functionality in OpenAM 11.0.1

There are no new removed functionality in OpenAM 11.0.1.

5.3.4. Removed Functionality in OpenAM 11.0.0

- 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 6

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 for OpenAM 11.

6.1. Key Fixes

6.1.1. Key Fixes in OpenAM 11.0.3

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-4380: We should no longer redistribute the RSA SecurID library
- 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

6.1.2. Key Fixes in OpenAM 11.0.2

The following bugs were fixed in release 11.0.2. For details, see the OpenAM issue tracker.

- OPENAM-4235: RestAuthorizationDispatcherFilter is not thread-safe in its usage of the AuthZFilter
- OPENAM-4176: Concurrent access of non-thread safe objects possible in DelegationPolicyImpl
- OPENAM-4138: SMS*Object implementations can cache entry presence incorrectly
- OPENAM-4111: IdP Proxy should use supported binding when connecting to the remote IdP
- OPENAM-4066: RedirectCallbackHandler should use AuthClientUtils instead of AuthUtils
- OPENAM-4044: RestSecurity is instantiated every time user makes REST JSON request
- OPENAM-4041: Session fails to recover deleted session gracefully if CTS compression enabled
- OPENAM-4023: Configurator should not ping the configuration store
- OPENAM-4005: REST logout session fails and does not produce a result message in 11.0.1
- OPENAM-3999: Adaptive module doesn't honor encoded cookies in user requests
- OPENAM-3995: Referral policies cannot be deactivated
- OPENAM-3993: CachingEntitlementCondition should call getState only once
- OPENAM-3989: ResourceLookup should cache results more aggresively
- OPENAM-3987: DAS fails to add cookie header from CAS when cookie.httponly=true
- OPENAM-3977: Review debug statements in IdServicesImpl and subclasses
- OPENAM-3967: PerThreadCache: move initialValue() call outside of critical section
- OPENAM-3965: Use char[] version of Base64 decoding
- OPENAM-3964: SessionService#addInternalSessionListener should not persist the token if the notification URL was already registered
- OPENAM-3959: auth chain miscalculates auth level
- OPENAM-3947: Upgrade removes user-added Advanced Properties from Default Server Settings
- OPENAM-3920: Remote IDP MetaData Import fails with Unable to verify signature under element "EntitiesDescriptor".
- OPENAM-3871: Configurator fails if password contains '%'
- OPENAM-3864: Policy evaluation results differs between clean and upgraded OpenAM instances
- OPENAM-3841: Export metadata produces XML Parsing Error after upgrade to AM11.0.1
- OPENAM-3830: LDAPUtils heartbeat timeout needs to be updated to keep in line with opendj-sdk timeout setting.

- OPENAM-3826: WindowsDesktopSSO auth-module does not log details about GSSException
- OPENAM-3811: Possible CME while serializing InternalSessions
- OPENAM-3809: The final SLO response should be sent using appropriate binding
- OPENAM-3790: Spurious authentication cookie can prevent logout
- OPENAM-3739: configurator tool fails when AuthClientUtil is initialized before the tool
- OPENAM-3731: Sun JDK 1.6.0_43: some requests cause never-ending loop in SAML2Utils.decodeFromRedirect
- OPENAM-3683: Version number on upgrade wizard is wrong if using a language other than English
- OPENAM-3660: RedirectCallbackHander uses HttpServletRequest.getRequestURL to construct AM_REDIRECT_BACK_SERVER_URL
- OPENAM-3659: OAuth2 auth module uses HttpServletRequest.getRequestURL() to construct ORIG_URL cookie
- OPENAM-3651: LoA based SAML2IDPFinder fails with NPE if the AuthnRequest did not contain RequestedAuthnContext
- OPENAM-3646: REST endpoint frrest/oauth2/token reports tokenName access_token when given a refresh_token
- OPENAM-3640: StackOverFlowError in WebtopNaming
- OPENAM-3633: SystemConfigurationUtil returning wrong information while config is reloaded in rare condition
- OPENAM-3626: Changes to policy rules only take effect after restarting OpenAM
- OPENAM-3447: CTS update fails due to attribute conflict
- OPENAM-3239: OAuth 2 client properties randomly disappears after upgrade from OpenAM 10.1 to OpenAM 11
- OPENAM-3207: PLLRequestServlet should log an error if the configured maximum request size is exceeded
- OPENAM-3184: Insufficient error logging when 'agent profile' can not be found by CDCServlet
- OPENAM-3065: Working with realms/sub-realms in site setup is not working properly.
- OPENAM-2712: Adaptive.getIdentity prints 'More than one user found' when no user was found
- OPENAM-2532: deleting ActiveDirectory DataStore from subrealm deleting parent's referrals too.
- OPENAM-2460: Policy evaluation may hang with large number of matching referral privileges

- OPENAM-1655: AttributeQueryUtil ignores configured SPAttributeMapper
- OPENAM-1642: Chain based UI customization is not case insensitive
- OPENAM-752: AgentsRepo#getAttributes fails to get agent information occasionally leading to server restart
- OPENAM-294: ssoadm: create and update

6.1.3. Key Fixes in OpenAM 11.0.1

The following bugs were fixed in release 11.0.1. For details, see the OpenAM issue tracker.

- OPENAM-3742: Large amount of invalid search requests made against IdRepo
- OPENAM-3740: HttpOnly and Secure cookie flags not always honored in multiserver deployments
- OPENAM-3707: Error while retrieving NameIDKeyMap
- OPENAM-3678: OAuth2 restlet extension doesn't populate name and description on the OAuth2 consent page
- OPENAM-3666: In-memory account lockout does not work when using Data Store authentication module
- OPENAM-3648: SAML 1.x authenticationMethod should escape "|" characters
- OPENAM-3639: WS-Fed IP sends incorrectly encoded unicode characters
- OPENAM-3638: Policy rule with trailing wildcard denies access to a valid resource URL
- OPENAM-3632: Adaptive module does not honor httpOnly Secure cookie settings
- OPENAM-3623: LDAP auth-module connection pool does not correctly recover
- OPENAM-3607: Adaptive IP check fails when message level debug enabled
- OPENAM-3573: IDP Initiated federation with missing SPNameQualifier result in exception
- OPENAM-3572: MailServerImpl not properly handling mailservers without authentication
- OPENAM-3561: Special characters are incorrectly handled when using LDAP auth module
- OPENAM-3542: Possible NPE when sending SAML request without isPassive attribute
- OPENAM-3531: new_org.jsp doesn't work when SAML request was sent using HTTP-POST binding
- OPENAM-3522: Special LDAP characters in the data store's naming attribute are not escaped
- OPENAM-3520: OAuth2 read/delete throws NPE if SSOToken doesn't belong to the same realm as token's realm

- OPENAM-3509: PolicyEvaluation strips off trailing '/' from resource resulting in wrong enforcement on agent side
- OPENAM-3506: OAuth2 grant_type=client_credentials read/delete fail with NPE
- OPENAM-3499: LoginServlet is NOT enforcing strict session timeouts on DAS
- OPENAM-3482: ForgotPassword REST API should escape username used in confirmationLink
- OPENAM-3465: Parsing output of Embedded OpenDJ dsconfig list-replication-server command fails due to change since v2.6.0
- OPENAM-3458: SAML federation can fail in multiserver deployments
- OPENAM-3444: Incorrect NameIdentifier generated when using both default and non-default NameIDFormat with SAML 1.x
- OPENAM-3437: RelayState validation fails during SLO
- OPENAM-3428: DJLDAPv3Repo breaks Active Directory when using sAMAccountName as naming attribute with the DN being the CN
- OPENAM-3413: Update federation attribute mapping documentation with details of new binary attribute mapping feature
- OPENAM-3408: Fix for OPENAM-2626 leads to concurrent modification exception
- OPENAM-3401: The token generated by the forgotPassword REST API should be a one time password
- OPENAM-3385: DJLDAPv3Repo Error Unexpected Results Returned when searching Active Directory users from the root
- OPENAM-3353: LDAP auth does not set operation timeout; OpenAM freeze
- 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-3237: Updating a user entry with an empty attribute fails if the attribute didn't exist in the entry before
- 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-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-3210: In CDSSO scenario no Logout is triggered when choosing 'yes' on 'new_org.jsp'
- OPENAM-3204: Goto URL validation can choke on relative URLs
- OPENAM-3202: RelayState is validated as a URL
- OPENAM-3190: IdP Adapter should have an extension point that can manipulate the SAML response
- 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-3156: web.xml should not have <distributable/>
- OPENAM-3113: DJLDAPv3Repo should properly set the LDAP error codes on IdRepoException
- OPENAM-2922: SP initiated SLO can fail with IllegalStateException
- OPENAM-2760: Validation of gotoOnFail URLs
- OPENAM-2327: OpenAM JSP violate JSP 2.0 spec
- OPENAM-2322: NULL pointer exception in windowsdesktopsso.java file when doing kerberos service ticket authenticaiton with Openssoclientsdk.jar client program - backward compatibility broken
- OPENAM-2294: Errors during federation can result in displaying Redirect.jsp
- OPENAM-2273: Help text on console for auto federation is misleading
- OPENAM-2145: Possible memory leaks around remote Session objects
- OPENAM-1957: NPE ERROR: Error creating logFailed message
- OPENAM-1739: HOTP module may ignore SMTP settings in the configuration
- OPENAM-1109: AdminTokenAction doesn't clear invalid SSOToken
- OPENAM-1012: IDP initiated SAML2 SLO error when SP does not have SLO binding
- OPENAM-688: REOPEN -LDAP Error 80 can result in build up of LDAPv3EventService::RetryTask objects

- OPENAM-119: Concurrent access of non-thread safe objects possible in IdRepoJAXRPCObjectImpl

6.1.4. Key Fixes in OpenAM 11.0.0

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

6.2. Limitations

6.2.1. Limitations in OpenAM 11.0.3

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).

6.2.2. Limitations in OpenAM 11.0.2

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).

6.2.3. Limitations in OpenAM 11.0.1

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).

6.2.4. Limitations in OpenAM 11.0.0

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).

6.3. Known Issues

6.3.1. Known Issues in OpenAM 11.0.3

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-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
- OPENAM-5617: Debug file rotation doesn't respect the rotation period
- OPENAM-5629: openam/oauth/registerconsumer.jsp endpoint returns inconsistent messages
- OPENAM-5638: The exceptions catched by the REST API aren't printed in the OpenAM debug logs
- OPENAM-5664: WS Federation Entity Provider shows content of Genral tab, but it is marked IDP(SP) tab
- OPENAM-5665: RealmSelection page is out of date
- OPENAM-5666: SAML 1.x Web SSO generates "Failed to create SSO token." error
- OPENAM-5674: Upgrade report for goto migration can be empty

6.3.2. Known Issues in OpenAM 11.0.2

The following important known issues remained open at the time release 11.0.2 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-4430: Upgrade wizard is not actual and not the same for the others languages than EN
- OPENAM-4320: NotificationServlet does not check for null before closing writer in finally block
- OPENAM-4262: IDP Proxy should set destination depending on the Binding
- OPENAM-4252: StatusCode SAML response missing space
- 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-4218: JAVA_HOME is not set correctly when installing admin tools (ssoadm, ampassword, amverifyarchive)
- OPENAM-4215: ScopingImpl#makeImmutable should perform null checks
- OPENAM-4213: Root cause of MetaData import is lost when debug level is set to 'error'
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3783: Device print check of installed plugins and fonts does not work
- OPENAM-3780: Max number and percentage of tolerated difference between installed fonts is replaced by each other
- OPENAM-3548: Items on the device print authn page are disordered
- OPENAM-3547: Typos and errors of 11.0 additional fields
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3390: Japanese translation for OpenAM 11.0
- OPENAM-3243: The Core Auth Module persistent cookie options are different from the Persistent Cookie Module
- OPENAM-3223: Policy Wildcard Matches doesn't work after OpenAM upgrade with an ODSEE
- OPENAM-3205: Missing labels in OAuth2 "Register a Client" page
- OPENAM-3159: Difference in case between results of identity/json/attributes REST API between first and subsequent calls
- OPENAM-3152: CTS -- External Store Passwords configured in default server settings shown in clear text elsewhere

- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- 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-2874: The OpenID Connect client registration endpoint does not set idTokenSignedResponseAlg to its default
- OPENAM-2777: Default user profile name field in device print page is unused
- OPENAM-2715: Mandatory OAuth2 Provider settings not enforced in the UI
- OPENAM-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- 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-2453: HTTP GET /ws/1/entitlement/privilege? HTTP 400 with message "Unable to search privileges."
- 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-2090: OPENAM_HOME/.version file is not updated
- 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-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-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1659: Default Authentication Locale is not used as fallback
- 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-1456: Change of the agent group in the J2EE policy agent profile causes profile corruption
- 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-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-1105: Init properties sometimes don't honor final settings
- OPENAM-774: Invalid characters check not performed.
- OPENAM-291: SelfWrite permissions are denied to sub realms
- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings

6.3.3. Known Issues in OpenAM 11.0.1

The following important known issues remained open at the time release 11.0.1 became available. For details and information on other issues, see the OpenAM issue tracker.

- OPENAM-3864: Policy evaluation results differs between clean and upgraded OpenAM instances
- OPENAM-3841: Export metadata produces XML Parsing Error after upgrade to AM11.0.1
- OPENAM-3827: json/session endpoint not listing sessions
- OPENAM-3811: Possible CME while serializing InternalSessions
- OPENAM-3809: The final SLO response should be sent using appropriate binding
- OPENAM-3790: Spurious authentication cookie can prevent logout to work
- OPENAM-3739: configurator tool fails when AuthClientUtil is initialized before the tool
- OPENAM-3660: RedirectCallbackHander uses HttpServletRequest.getRequestURL to construct AM_REDIRECT_BACK_SERVER_URL
- OPENAM-3659: OAuth2 auth module uses HttpServletRequest.getRequestURL() to construct ORIG_URL cookie
- OPENAM-3651: LoA based SAML2IDPFinder fails with NPE if the AuthnRequest did not contain RequestedAuthnContext
- OPENAM-3646: REST endpoint frrest/oauth2/token reports tokenName access_token when given a refresh_token
- OPENAM-3633: SystemConfigurationUtil returning wrong information while config is reloaded in rare condition
- OPENAM-3466: LDAP authentication module does not apply the change of the password for the bind DN user until restart
- OPENAM-3447: CTS update fails due to attribute conflict
- OPENAM-3333: WebLogic 11(10.3.6.0) doesn't create an OAuth2 token
- 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-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-3207: PLLRequestServlet should log an error if the configured maximum request size is exceeded

- OPENAM-3205: Missing labels in OAuth2 "Register a Client" page
- OPENAM-3184: Insufficient error logging when 'agent profile' can not be found by CDCServlet
- OPENAM-3112: REST authenticate resource should cope with charset provided with Content-Type header
- OPENAM-3109: Token conflicts can occur if OpenDJ servers are replicated
- OPENAM-3105: CachedSubEntries.getSubEntries() shouldn't sort LDAPSearchResults
- 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-2948: RESTful read performance: identityExists() is called twice before searching user entry
- 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-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-2656: PrefixResourceName#compare() strips off trailing '/' in PathInfo
- 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-2453: HTTP GET /ws/1/entitlement/privilege? HTTP 400 with message "Unable to search privileges."
- 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-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1659: Default Authentication Locale is not used as fallback
- OPENAM-1655: AttributeQueryUtil ignores configured SPAttributeMapper
- 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-1456: Change of the agent group in the J2EE policy agent profile causes profile corruption
- 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-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-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

6.3.4. Known Issues in OpenAM 11.0.0

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 7
Documentation Updates

The following table tracks changes to the documentation set following the release of OpenAM 11:

Table 7.1. Documentation Change Log

Date	Description
2016-08-25	Clarified which web containers are supported for deploying the Distributed Authentication `.war` file in Chapter 4, "*Installing OpenAM Distributed Authentication*" in the *Installation Guide*.
2016-07-15	Corrected the description of the Auto Federation Attribute property in Section 12.4.2, "Hints for Assertion Processing" in the *Administration Guide*.
2016-07-15	The procedure to turn off user data caching has a new step to disable persistent search. See Procedure 18.1, "To Turn Off Global User Data Caching" in the *Administration Guide*.
2016-04-20	The descriptions of the Relay State URL List property in Section 12.3, "Configuring Identity Providers" in the *Administration Guide* and Section 12.4, "Configuring Service Providers" in the *Administration Guide* have been corrected.
2016-04-05	Section 2.2.1, "Hints For the Active Directory Authentication Module" in the *Administration Guide* and Section 2.2.12, "Hints For the LDAP Authentication Module" in the *Administration Guide* has been updated with the property `openam-auth-ldap-operation-timeout`.
2016-03-15	Reorganization of 11.0.x docs, combining 11.0.0, 11.0.1, 11.0.2, and 11.0.3 release notes
2013-11-08	Initial release of OpenAM 11.0.0.

Chapter 8
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/.

Chapter 9

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