OpenAM Release Notes

Version 12.0.2

Gene Hirayama

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

Abstract

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

Table of Contents

Chapter 1

What's New in OpenAM 12.0.2

OpenAM 12.0.2 is a maintenance release that resolves a number of issues, including security issues in OpenAM. It is strongly recommended that you update to this release to make your deployment more secure and to take advantage of important functional fixes. ForgeRock customers can contact support for help and further information.

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

- If you have already installed OpenAM, see *To Update OpenAM From 12.0*.

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 Importing an outdated configuration can result in a corrupted installation.

- If you are installing OpenAM for the first time, see *To Install OpenAM*.

1.1 Security Advisories

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/

The following security advisories have been included in this release:

- OpenAM Security Advisory #201506-01
- OpenAM Security Advisory #201506-02

1.2 Product Enhancements

This release does not include any new product enhancements.

Chapter 2

Before You Install OpenAM 12.0.2 Software

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

ForgeRock supports customers using the versions specified here. Other versions and alternative environments might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on a combination covered here.

2.1 OpenAM Operating System Requirements

ForgeRock supports customers using OpenAM server software on the following operating system versions.

- CentOS 6, 7
- Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2
- Oracle Linux 6, 7
- Oracle Solaris x64 10, 11
- Oracle Solaris SPARC 10, 11
- Red Hat Enterprise Linux 6, 7

- SuSE Linux 11
- Ubuntu Linux 12.04 LTS, 14.04 LTS

2.2 Java Requirements

OpenAM server software runs in a Java EE Web container, and requires a Java Development Kit.

ForgeRock supports customers using the following Java versions. ForgeRock recommends the most recent Java update, with the latest security fixes.

- Oracle Java Development Kit 6, 7, or 8
- IBM Java Development Kit 6 or 7 (when deploying in WebSphere only)

2.3 OpenAM Web Application Container Requirements

ForgeRock supports customers using OpenAM server software in the following web application container versions.

- Apache Tomcat 6, 7, 8 (ForgeRock's preferred web container for OpenAM)
- IBM WebSphere Application Server 8, 8.5
- JBoss Enterprise Application Platform 6
- JBoss Application Server 7
- Oracle WebLogic Server 11g, 12c

The web application container must be able to write to its own home directory, where OpenAM stores configuration files.

2.4 Data Store Requirements

The following table summarizes OpenAM data store support.

Table 2.1. Supported Data Stores

Data Store	Versions	Core Token Service (CTS) Data Store	Configuration Data Store	User Data Store
Embedded OpenDJ (included in OpenAM)	2.6.2	Supported	Supported	Supported
External OpenDJ	2.6, 2.6.2	Supported	Supported	Supported
IBM Tivoli Directory Server	6.3			Supported
Microsoft Active Directory	2008, 2008 R2, 2012, 2012 R2			Supported
Oracle Directory Server Enterprise Edition	11g	**NOT SUPPORTED**	Supported When using DSEE as a configuration store, you must set up an external OpenDJ directory service as a Core Token Service data store as well, and you must configure OpenAM to use the external OpenDJ directory service as the CTS data store.	Supported
Oracle Unified Directory	11g		Supported	Supported

2.5 Browser Requirements

The following table summarizes browser support.

Table 2.2. Supported Platforms & Browsers

Client Platform	Chrome 16 or later	Internet Explorer 9 or later	Firefox 3.6 or later	Safari 5 or later
Apple iOS 7 or later	Supported			Supported
Apple Mac OS X 10.8 or later	Supported		Supported	Supported
Google Android 4.3 or later	Supported			
Microsoft Windows 7 or later	Supported	Supported	Supported	Supported
Ubuntu Linux 12.04 LTS or later	Supported		Supported	

2.6 Native Application Platform Requirements

ForgeRock supports customers' use of OpenAM REST and other client APIs in native applications on the following platforms.

- Apple iOS 7 or later
- Apple Mac OS X 10.8 or later
- Google Android 4.3 or later
- Microsoft Windows 7 or later
- Ubuntu Linux 12.04 LTS or later

Other combinations might work as well. When opening a support ticket for an issue, however, make sure you can also reproduce the problem on one of these platforms.

2.7 Special Requests

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

Chapter 3

OpenAM Changes and Deprecated Functionality

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

3.1 Important Changes to Existing Functionality

The following changes are listed in OpenAM 12.0.2:

- **OAuth2 Tokeninfo Endpoint is No Longer Realm-Specific**. Requests made to the `/oauth2/tokeninfo` endpoint no longer need to specify the realm the provided OAuth2 access token belongs to.

  For more information, see OPENAM-6534.

The following changes were listed in OpenAM 12.0.1:

- **Agent Group Membership Now Stored in Agent Profile**. Agent group membership information is now stored as part of the agent profile using the `agentgroup` attribute. You can assign an agent to a group by simply setting the `agentgroup` property upon creation. You can also use the **ssoadm show-agent** command to return the group membership detail in the `agentgroup` attribute. Note that the existing **ssoadm** commands (for example, `add-agent-to-grp` and `remove-agent-from-grp`) are still the preferred methods for managing group membership information.

During upgrade, agent profiles will be automatically upgraded to use the new `agentgroup` attribute to store the group's name.

For more information, see OPENAM-718.

- **Updated weblogic.xml for WebLogic**. When running OpenAM on WebLogic 11g, you must add a WebLogic-specific descriptor file, `WEB-INF/weblogic.xml` in the `.war` before deployment. The descriptor file maps resources defined for OpenAM in WebLogic deployments.

  An example `weblogic.xml` file is presented below.

```
<?xml version="1.0" encoding="UTF-8"?>
<weblogic-web-app xmlns="http://xmlns.oracle.com/weblogic/weblogic-web-app"
     xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
     xsi:schemaLocation="http://xmlns.oracle.com/weblogic/weblogic-web-app
     http://xmlns.oracle.com/weblogic/weblogic-web-app/1.3/weblogic-web-app.xsd">
      <context-root>/openam</context-root>
      <container-descriptor>
       <prefer-application-packages>

        <!-- Use bundled Jersey library -->
        <package-name>com.sun.jersey.*</package-name>
        <package-name>com.sun.research.ws.wadl.*</package-name>
        <package-name>com.sun.ws.rs.ext.*</package-name>

        <!-- Rhino -->
        <package-name>org.mozilla.javascript.*</package-name>

        <package-name>org.apache.commons.lang.*</package-name>
      </prefer-application-packages>
     </container-descriptor>
 </weblogic-web-app>
```

  For more information see, OPENAM-3333.

- **AD/LDAP/RADIUS Authentication Modules Allow More Than One Primary/Secondary Server**. The Active Directory, LDAP, and RADIUS authentication modules now allow one or more servers to be designated as primary or secondary servers.

  When authenticating users from a directory server that is remote to OpenAM, set the primary server values, and optionally, the secondary server values. Primary servers have priority over secondary servers.

  ssoadm attributes are: primary is `iplanet-am-auth-ldap-server`; secondary is `iplanet-am-auth-ldap-server2`.

  Both properties take more than one value; thus, allowing more than one primary or secondary remote server, respectively. Assuming a multi-data

center environment, OpenAM determines priority within the primary and secondary remote servers, respectively, as follows:

- Every LDAP server that is mapped to the current OpenAM instance has highest priority.

  For example, if you are connected to `openam1.example.com` and `ldap1.example.com` is mapped to that OpenAM instance, then OpenAM uses `ldap1.example.com`.

- Every LDAP server that was not specifically mapped to a given OpenAM instance has the next highest priority.

  For example, if you have another LDAP server, `ldap2.example.com`, that is not connected to a specific OpenAM server and if `ldap1.example.com` is unavailable, OpenAM connects to the next highest priority LDAP server, `ldap2.example.com`.

- LDAP servers that are mapped to different OpenAM instances have the lowest priority.

  For example, if `ldap3.example.com` is connected to `openam3.example.com` and `ldap1.example.com` and `ldap2.example.com` are unavailable, then `openam1.example.com` connects to `ldap3.example.com`.

For more information, see OPENAM-3575.

- **StartTLS Support for Directory Server-Based Data Stores**. You can now use StartTLS to initiate secure connections to directory server-based data stores. A new property, `sun-idrepo-ldapv3-config-connection-mode`, has been created and has possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature.

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

  OpenAM automatically updates the `sun-idrepo-ldapv3-config-ssl-enabled` property to the `sun-idrepo-ldapv3-config-connection-mode` property when you upgrade. To enable StartTLS, set the `sun-idrepo-ldapv3-config-connection-mode` property to `StartTLS`. You will also need to update existing **ssoadm** scripts to use the new `sun-idrepo-ldapv3-config-connection-mode` property.

  For more information, see OPENAM-3714.

- **Move of OAuth 2.0 Well-Known Endpoints**. The well-known endpoints have been moved from `/openam/.well-known` to `/openam/oauth2/.well-known`.

  For more information, see OPENAM-4333.

- **StartTLS Support for AD/LDAP Authentication Modules**. You can now use StartTLS with the Active Directory and LDAP authentication modules to secure OpenAM's connection to the data stores. A new property, `openam-auth-ldap-connection-mode`, has been created with the possible values of `LDAP`, `LDAPS`, and `StartTLS` to enable this feature.

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

  OpenAM automatically updates the `iplanet-am-auth-ldap-ssl-enabled` property to the `openam-auth-ldap-connection-mode` property when you upgrade. You must manually set the value of the `openam-auth-ldap-connection-mode` to `StartTLS` to initiate a StartTLS connection to the data store. You will also need to update existing **ssoadm** scripts to use the new `openam-auth-ldap-connection-mode` property.

  For more information, see OPENAM-5097.

- **AD Authentication Module Now Provides iplanet-am-auth-ldap-ssl-trust-all**. The `iplanet-am-auth-ldap-ssl-trust-all` property in the Active Directory authentication module enables the `X509TrustManager` to trust all certificates when the Active Directory authentication module connects to AD servers protected by self-signed or invalid (for example, invalid hostnames) certificates.

  Caution: Use this property with care as it bypasses the normal certificate verification process.

  For more information, see OPENAM-5460.

- **Addional JVM Properties for WebSphere Installs**. OpenAM 12.0.1 requires an updated step when running OpenAM on WebSphere. The JVM settings require additional properties to be set.

```
-DamCryptoDescriptor.provider=IBMJCE
-DamKeyGenDescriptor.provider=IBMJCE
-Djavax.xml.parsers.DocumentBuilderFactory=org.apache.xerces.jaxp.DocumentBuilderFactoryImpl
-Djavax.xml.parsers.SAXParserFactory=org.apache.xerces.jaxp.SAXParserFactoryImpl
```

  Run the following procedures to set up the JVM properties on WebSphere. Note that these steps were run on WebSphere 8.5 on a Windows platform:

  1. Log in to the WebSphere console.

  2. In the left pane, expand Servers.

  3. Expand Server Types.

4. Click WebSphere application servers.
5. In the right pane, click on the server name.
6. In the Server infrastructure section, expand Java and Process Management.
7. Click Process definition.
8. In the Advanced properties section, click Java Virtual Machine.
9. In the Generic JVM arguments text field, add the JVM properties.
10. Save the configuration.

For more information, see OPENAM-6109.

- **OAuth2 Scopes Behavior Affected By Upgrade**. After an upgrade, OAuth 2.0 scope behavior uses a deprecated implementation class, `org.forgerock.openam.oauth2.provider.impl.ScopeImpl`.

  The workaround is to manually update the OAuth 2.0 providers to use the `org.forgerock.openam.oauth2.OpenAMScopeValidator`.

  For background information, see OPENAM-6319.

The following changes were listed for OpenAM 12.0.0:

- All OpenAM core server, tools, and agent installers now display a software license acceptance screen prior to configuration. You must agree to the license to continue the configuration.

  For users implementing scripted or silent installs, the installers and upgrader tools provide a `--acceptLicense` command-line option, indicating that you have read and accepted the terms of the license. If the option is not present on the command-line invocation, the installer or upgrader will interactively present a license agreement screen to the user.

- When you visit the Policies tab for a realm in OpenAM console, OpenAM now directs you to the new policy editor. For instructions on using the new policy editor, see the *Administration Guide* chapter, *Defining Authorization Policies*. Notice that policies now belong to applications as described in that chapter.

  OpenAM has changed its internal representation for policies to better fit the underlying implementation, which is based on a new engine designed for higher performance and fine-grained policies. When you upgrade to this version, OpenAM migrates your policies to the new representation.

  Depending on your existing policies before upgrade, you can see the following differences:

- Existing policies with multiple resource rules map to multiple new policies.

  When a single policy maps to multiple policies during migration, OpenAM appends a number to the existing name for each new policy. This allows you to recognize the set of policies when you must manage them together, for example, to change them all in the same way.

  This behavior is to optimize policy evaluation performance. The newer policy engine matches resources to policies during evaluation with indexing that proves very efficient as long as each policy specifies one resource pattern. OpenAM processes the list of resources in policies in linear fashion, so long lists of resources can slow policy evaluation.

- Conditions in existing policies map to newer representations.

  New representations exist for all existing conditions provided in OpenAM out of the box. Custom conditions developed for your deployment do not map to any of the newer conditions provided. In this case, you must write your custom conditions by implementing the newer service provider interfaces, and then replace your existing policies to use them.

  To see how to implement a custom policy plugin, see the *Developer's Guide* chapter, *Customizing Policy Evaluation*.

- When OpenAM encounters issues migrating policies during upgrade, it writes messages about the problems in the upgrade log. When you open a policy in the policy editor that caused problems during the upgrade process, the policy editor shows the issues, but does not let you fix them directly. Instead, you must create equivalent, corrected policies in order to use them in OpenAM.

- It is strongly recommended *not* to use the forward slash character in policy names. Users running OpenAM servers on Tomcat and JBoss web containers will not be able to manipulate policies with the forward slash character in their names without setting the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` argument in the `CATALINA_OPTS` environment variable before starting the OpenAM web container.

  It is also strongly recommended not to enable the `ALLOW_ENCODED_SLASH=true` setting while running OpenAM in production. Using this option introduces a security risk. See Apache Tomcat 6.x Vulnerabilities and the related CVE for more information.

  If you have policy names with forward slashes after migration to OpenAM 12, rename the policies so that they do not have forward slashes. Perform the following steps if you use Tomcat or JBoss as your OpenAM web container:

  1. Stop the OpenAM web container.

2. Add the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting to the `CATALINA_OPTS` environment variable.
3. Restart the OpenAM web container.
4. Rename any policies with forward slashes in their names.
5. Stop the OpenAM web container.
6. Remove the `-Dorg.apache.tomcat.util.buf.UDecoder.ALLOW_ENCODED_SLASH=true` setting from the `CATALINA_OPTS` environment variable.
7. Restart the OpenAM web container.

OpenAM configuration has changed in several ways to accommodate the changes to the way policies are managed:

- The Policy Configuration Service is simplified. For details see the *Reference* section, *Policy Configuration*.
- OpenAM now requires policy referrals only when an application is administered across multiple realms, as can be the case when one policy agent protects multiple applications. Otherwise, OpenAM can use new settings in policy agent profiles to direct policy agent requests to the appropriate realm and application.

Note

Referrals are not shown by default in the policy editor. To enable them, in the OpenAM console, select Configuration > Global > Policy Configuration, set Activate Referrals to Enabled, and then click Save.

  The web and Java EE policy agent profiles includes the new settings under OpenAM Services > Policy Client Service in OpenAM console. These new settings allow you to set the realm and application for a policy agent. The settings are compatible with existing policy agents, as they are not used by the policy agents themselves, but instead by OpenAM when handling policy agent requests.

The fix for OPENAM-3509 ensures that OpenAM considers a trailing slash as part of the resource name to match. This improves compatibility between self and subtree modes, and compatibility with older policy agents.

- The Device ID (Match), HMAC One-Time Password (HOTP), and Device ID (Save) modules, configured together in an authentication chain, provide the same functionality as the Device Print Authentication module that is present in OpenAM 11.x versions.

  The Device Print authentication module is only available for OpenAM 11.x versions and their upgrades. If you have upgraded from OpenAM 11.x to OpenAM 12.0, you can still use the Device Print module, customize it, and create new instances of the module or use the Device ID (Match) and Device ID (Save) modules.

  

  Important

  The Device ID (Match) profiles (that is, device fingerprints) are incompatible with profiles created from the Device Print authentication module. If the user has existing device print profiles, created from the Device Print authentication module, these old profiles will always fail to match the client's new device profiles using the scripted Device ID (Match) module even when using the same device.

  With the Device ID (Match) and Device ID (Save) modules, the user must resave each device profile, which deletes the old 11.x profiles stored for the user.

- Following a change to the SAML 2.0 pages in OpenAM, you no longer customize `saml2login.template` and `saml2loginwithrelay.template` to add a progress bar for SSO. Instead, customize `saml2/jsp/autosubmitaccessrights.jsp` as described in the procedure in the OpenAM Administration Guide, *To Indicate Progress During SSO* .

- Changing passwords by using a PUT REST API call is no longer supported.

  Use a POST request to `/json/`*`subrealm`*`/users/`*`username`*`?_action=changePassword` to change a password.

- The response returned when submitting incorrect credentials to `/json/authenticate` has changed.

Table 3.1. Failed Authentication Message

OpenAM 11.0.1	OpenAM 12.0.0

<pre>{
 "errorMessage": "Authentication Failed!!",
 "failureUrl": "https://openam.example.com:8443"
}</pre>
	<pre>{
	 "code": 401,
	 "reason": "Unauthorized",
	 "message": "Authentication Failed!!",
	 "detail": {
	  "failureUrl": "https://openam.example.com:8443"
	 }
	}</pre>

- When running OpenAM on WebLogic 11g, you must add a WebLogic-specific descriptor file, `WEB-INF/weblogic.xml` to the .war before deployment.
- In the OpenID Connect 1.0 module you can map local user profile attributes to OpenID Connect Token claims, allowing the module to retrieve the user profile based on the ID Token. The key is the ID Token field name and value is the local user profile attribute name. The default has been changed as follows: mail=email, uid=sub. (OPENAM-5263)
- The class hierarchy for the `ResourceName` interfaces has changed. Previous implementations should be source-compatible, but will not be binary-compatible, and will need recompiling.
- The OAuth2 provider uses RSA as its default encryption algorithm. The default OAuth2 client agent configuration has been changed to RS256 to match the OAuth2 provider algorithm. The client agent continues to support HMAC algorithms; only the default encryption algorithm has been changed to support out of the box functionality. (OPENAM-5279)
- 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`.
- Updates to OAuth 2.0 and OpenID Connect authentication modules mean that any custom implementations of `org.forgerock.openam.authentication.modules.oauth2.AccountMapper` or `org.forgerock.openam.authentication.modules.oauth2.AttributeMapper` no longer work, and need to be reimplemented against `org.forgerock.openam.authentication.modules.common.mapping.AttributeMapper` and/or `org.forgerock.openam.authentication.modules.common.mapping.AccountProvider` as appropriate.
- The XUI, now the default for end-user pages, handles DNS/realm alias differently from the classic UI, which was the default in previous OpenAM versions. With the classic UI, the realm alias is specified both in the host name

and the URI path. With the XUI, the host name alone specifies the realm. The XUI evaluates a realm specified in the path of the URL as a subrealm of the realm specified by the host name alias.

For example, with the classic UI, you could authenticate to a realm, `realm1` using the DNS alias `realm1.example.com:8080` and the realm query parameter, `realm=realm1`, as follows:

```
http://realm1.example.com:8080/openam/UI/Login?realm=realm1
```

With XUI, you do not include a realm in the URI if it has already been mapped, as now any URI realm is additive and specifies a subrealm of the DNS alias realm. For example, using the following URL indicates that you are attempting to authenticate to `/realm1/realm1` (that is, the sub-realm, `realm1` under the realm, `realm1`).

```
http://realm1.example.com:8080/openam/XUI/#Login/realm1
```

As another example, if you have a sub-realm called `test` under `/realm1` and make a request to:

```
http://realm1.example.com:8080/openam/XUI/#Login/test
```

The request authenticates to `/realm1/test`. Note also that the use of URI realm is preferred over realm as a query parameter.

3.2 Deprecated Functionality

The following functionality is deprecated in OpenAM 12.0.1, and is likely to be removed in a future release.

- Classic (JATO-based) UI is deprecated for end user pages. OpenAM offers the JavaScript-based XUI as a replacement. Classic UI for end user pages is likely to be removed in a future release.
- Older REST services relying on the following endpoints are deprecated:

  /identity/attributes
  /identity/authenticate
  /identity/authorize
  /identity/create
  /identity/delete
  /identity/read
  /identity/search
  /identity/update
  /ws/1/entitlement/decision
  /ws/1/entitlement/decisions

/identity/isTokenValid
/identity/logout
/ws/1/entitlement/entitlement
/ws/1/entitlement/entitlements

The following table shows how legacy and newer endpoints correspond.

Table 3.2. REST Endpoints

Deprecated URIs	Newer Evolving URIs
/identity/attributes	/json/users
/identity/authenticate	/json/authenticate
/identity/authorize	/json/policies?_action=evaluate, /json/policies?_evaluateTree
/identity/create, /identity/delete, /identity/read, /identity/search, /identity/update	/json/agents, /json/groups, /json/realms, /json/users
/identity/isTokenValid	/json/sessions/*tokenId*?_action=validate
/identity/logout	/json/sessions/?_action=logout
/ws/1/entitlement/decision, /ws/1/entitlement/decisions, /ws/1/entitlement/entitlement, /ws/1/entitlement/entitlements	/json/policies?_action=evaluate, /json/policies?_evaluateTree
N/A	/json/applications
N/A	/json/applicationtypes
N/A	/json/conditiontypes
N/A	/json/dashboard
N/A	/json/decisionscombiners
N/A	/json/policies
N/A	/json/referrals
N/A	/json/serverinfo
N/A	/json/subjectattributes
N/A	/json/subjecttypes
N/A	/xacml/policies

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

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.

- With the implementation of XACML 3.0 support when importing and exporting policies, the following `ssoadm` commands have been replaced:

Table 3.3. Policy Import and Export With ssoadm

Deprecated Command	Newer Evolving Command
`create-policies`	`create-xacml`
`delete-policies`	`delete-xacml`
`list-policies`	`list-xacml`
`update-policies`	`create-xacml`

For more information, see the *OpenAM Reference* section ssoadm — configure OpenAM core services.

- 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.
- The OAuth 2.0 plugin interface for custom scopes `Scope` is deprecated and likely to be removed in a future release.

  Custom OAuth 2.0 scopes plugins now implement the `ScopeValidator` interface instead. For an example, see the *Developer's Guide* chapter, *Customizing OAuth 2.0 Scope Handling*.
- The OAuth 2.0 plugin interface for custom response types, `ResponseType`, is deprecated and likely to be removed in a future release.

Custom OAuth 2.0 response type plugins now implement the `ResponseTypeHandler` interface instead.

3.3 Removed Functionality

- **Removal of Unused Install-Time LDAP Users**. Default LDAP users that were set up during initial installation have been removed, because they were not referenced anywhere in the configuration. Any associated access control instructions to the removed entries have also been removed.

  When targeting Oracle DSEE as the user store, OpenAM no longer creates the following entries and ACIs:

  - dn: ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=dsameuser, ou=DSAME users, CHOSEN_SUFFIX
  - dn: cn=amldapuser,ou=DSAME Users, CHOSEN_SUFFIX
  - allow (all) userdn = "ldap:///cn=dsameuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - allow (read,search) userdn = "ldap:///cn=amldapuser,ou=DSAME Users,CHOSEN_SUFFIX";
  - deny (write) userdn ="ldap:///self". The aci was updated to remove the `dsameuser` reference from the target filter.

  When targeting OpenDJ as the user store (internally or externally), OpenAM no longer creates the following entries and ACIs:

  - dn: ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX
  - dn: cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX
  - allow (read,search) userdn = "ldap:///cn=ldapuser,ou=opensso adminusers,CHOSEN_SUFFIX";
  - allow (all) userdn = "ldap:///cn=openssouser,ou=opensso adminusers,CHOSEN_SUFFIX";
  - deny (write) userdn ="ldap:///self". The aci was updated to remove the `openssouser` reference from the target filter.

New installations will not have these entries and ACIs. For upgraded deployments, you must manually remove the entries if they are not being used.

For details, see the explanation in (OPENAM-1036 and in OpenAM Security Advisory #201505-05).

- 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.

Chapter 4

OpenAM Fixes, Limitations, and Known Issues

OpenAM issues are tracked at https://bugster.forgerock.org/jira/browse/OPENAM. This chapter covers the status of key issues and limitations at release 12.0.2.

4.1 Key Fixes

The following bugs were fixed in release 12.0.2. For details, see the OpenAM issue tracker.

- OPENAM-5804: Forgot password in XUI with a sub-realm when using RFC3986 specs not redirecting correctly
- OPENAM-5826: Zero Page Login disallowed after OPENAM-sec-201503-v1102-CAS is applied
- OPENAM-5841: Realm override query parameter on login not overriding realm
- OPENAM-6000: Accessing XUI through a FQDN that is resolvable but not mapped throws an internal server error
- OPENAM-6039: Asynchronous queue for OAuth2 Tokens can result in token validation failures
- OPENAM-6293: XUI freezes at startup when serverinfo service call fails

- OPENAM-6377: CTSOperations is currently performing setLatestAccessTime on a local token, rather than the remote one.
- OPENAM-6455: ConnectionCount logic does not produce a sensible ConnectionFactory max pool size for some scenarios
- OPENAM-6457: DirectoryContentUpgrader causes Entry Already Exists exception for CTS suffix when upgrading OpenAM
- OPENAM-6468: InvalidClassException with certauth after #201505-01 patch
- OPENAM-6499: Configuration store servers are not listed in Directory Configuration
- OPENAM-6501: RestSecurity is instantiated every time user makes serverinfo request
- OPENAM-6503: Unable to update policies in subrealm
- OPENAM-6534: OAuth2 tokeninfo endpoint should be realm-independent
- OPENAM-6545: ServerInfoResource should attempt to cache ServiceConfigs per realm rather than creating one on each request
- OPENAM-6613: Updating Hosted IDP Authentication Context Mapper does not save values
- OPENAM-6627: Self-registration fails in XUI when using realms

4.2 Limitations

The following items are limitations in 12.0.2:

- **Manually Update Required for Some Fixes**. The changes related to OPENAM-6468 and OPENAM-6499 are not handled automatically by upgrade, thus when upgrading OpenAM from 12.0.1 or from a version where the #201505-01 security patch has been applied, the Object Deserialisation Class Whitelist server setting needs to be updated manually with the following new entries:

```
com.sun.identity.common.configuration.ServerConfigXML
com.sun.identity.common.configuration.ServerConfigXML$DirUserObject
com.sun.identity.common.configuration.ServerConfigXML$ServerGroup
com.sun.identity.common.configuration.ServerConfigXML$ServerObject
java.security.cert.Certificate
java.security.cert.Certificate$CertificateRep
```

- **Different OpenAM Version Within a Site**. Do not run different versions of OpenAM together in the same OpenAM site.
- **Deleting Referral Policy**. 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.
- **Avoid Use of Special Characters in Policy or Application Creation**. Do not use special characters within policy, application or referral names (for example, "my+referral") using the Policy Editor or REST endpoints as OpenAM returns a 400 Bad Request error. The special characters are: double quotes ("), plus sign (+), command (,), less than (<), equals (=), greater than (>), backslash (\), and null (\u0000). (OPENAM-5262)
- **Avoid Using REST Endpoint Names for Realm Names**. Do not use the names of OpenAM REST endpoints as the name of a realm. The OpenAM REST endpoint names that should not be used includes: `users`, `groups`, `realms`, `policies`, and `applications`. (OPENAM-5314)
- **Deploying OpenAM on Windows in an IPv6 Network**. 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).
- **Database Repository Type is Experimental**. The Database Repository type of data store is experimental and not supported for production use.
- **Enforcing Session Quotas With Session Failover**. 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.
- **OpenAM with Embedded Directory Server in IPv6 Networks**. On hosts with pure IPv6 networks, OpenAM configuration has been seen to fail while starting the embedded OpenDJ directory server (OPENAM-3008).
- **JBoss 6.3 Support for Java 8**. As of this writing, JBoss 6.3/AS 7.4.0 does not support Java 8. Until JBoss 6.3 fully supports Java 8, you can use JDK 1.7.0_56 (OPENAM-4876).
- **Note about HttpServletResponse And HttpServletRequest**. The `HttpServletRequest` instance passed to `AMPostAuthProcessInterface#onLogout` will be null. The `HttpServletResponse` instance passed to

`AMPostAuthProcessInterface#onLogout` is not the actual `HttpServletResponse` corresponding to the request but a faux instance whose only purpose is to transfer headers back to the actual `HttpServletResponse` (OPENAM-4045).

- **XACML Policy Import and Export**. OpenAM can only import XACML 3.0 files that were either created by an OpenAM instance, or that have had minor manual modifications, due to the reuse of some XACML 3.0 parameters for non-standard information.

4.3 Known Issues

The following important known issues remained open at the time release 12.0.2 became available. For details and information on other issues, see the OpenAM issue tracker.

- **Missing Policy Actions after Upgrading 11.0.0 > 11.02 > 12.0.1**. OpenAM's 11.0.0 has two Policy Editor actions: `GET` and `POST`. If you upgrade to OpenAM 11.0.2 or later, additional actions are available: `DELETE`, `HEAD`, `OPTIONS`, `PATCH`, and `PUT`. When upgrading from 11.0.2 (or later), the new actions will be missing from the Policy Editor.

  You can add the actions in OpenAM 12.0.1 by running the following **ssoadm** command:

  ```
  $ openam/bin/ssoadm set-appl -e -m iPlanetAMWebAgentService \
    -u amadmin -f .pass -D appl.text
  ```

  where `appl.txt` is a file containing the actions:

  ```
  actions=GET=true
  actions=POST=true
  actions=PUT=true
  actinos=DELETE=true
  actions=HEAD=true
  actions=OPTIONS=true
  actions=PATCH=true
  ```

  For information, see OPENAM-6424.

- **Do Not End Policy Names with a "/" Character**. Do not use a "/" character at the end of a policy name as it will cause OpenAM to not read, edit, or delete the policy.

  After upgrade, users who have policies with a trailing slash "/" character at the end of a policy name should remove the slash (OPENAM-5400).

To remove slashes in the policy names, remove them as recommended in OPENAM-5187.

- **Do Not Include a "?" Character in Policy Names**. Policy names with a "?" character leads to the policy editor not being able to edit it (OPENAM-5363).
- **Restart Container When Getting Exception**. After you deploy OpenAM 12.0.1, if you get an "Cannot initialize Authentication" exception on some containers (WebLogic 11 and 12, and JBoss), you must restart the container (OPENAM-6345).
- **Upgrade Incorrectly Sets the Default Value for the REST API Service**. The workaround is to manually set the Default Version setting in the REST API service to the preferred value:

```
$ openam/bin/ssoadm set-attr-defs -s RestApisService -t Global \
  -a openam-rest-apis-default-version=Latest -u amadmin -f .pass
```

For background information, see OPENAM-6302.

- OPENAM-71: SAML2 error handling in HTTP POST and Redirect bindings
- OPENAM-480: Adding a server to a site requires restart of OpenAM
- 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-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-1505: LogoutViewBean does not use request information for finding the correct template
- OPENAM-1659: Default Authentication Locale is not used as fallback

- OPENAM-1660: Read-access to SubjectEvaluationCache is not synchronized
- OPENAM-1831: OpenAM 10.0 subrealm DNS alias doesn't work as expected unless setting com.sun.identity.server.fqdnMap
- 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-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-2404: new_org.jsp is displayed from the original realm in case of session upgrade
- 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-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-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-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-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-4430: Upgrade wizard is out of date for other languages than EN
- OPENAM-4517: GUI installer crashes and restarts in Safari
- OPENAM-5234: AuthLevel policy condition does not work with pol. agents when result code 403 is expected
- 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-6056: LoginViewBean does not correctly handle empty ChoiceCallbacks
- OPENAM-6319: OAuth2 scopes behaviour affected by the upgrade
- OPENAM-6340: XUI needs to support DNS/Alias behaviour for subrealms as per OPENAM-5508
- OPENAM-6565: .well-known/openid-configuration is published with both DNS Realm alias AND realm in the path, resulting in failed authentication

Chapter 5

How to Report Problems and 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 12.0.2, report them in https://bugster.forgerock.org.

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

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

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

Chapter 6

Support

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