OpenAM Snapshot 9 Release Notes

OpenAM Snapshot 9 is the ForgeRock release of OpenSSO Build 9.

The **OpenSSO Snapshot 9 Release Notes** provide the following information, as well as links to articles about the new OpenAM snapshot 9 features.

- OpenAM Snapshot 9 Hardware and Software Requirements
- Getting Started With OpenAM Snapshot 9
- What's in OpenAM Snapshot 9
- Using Policy Agents with OpenAM Snapshot 9
- Known Issues in This Release
- OpenSSO Enterprise 8.0 Sun Documentation
- Deprecation Notifications and Announcements
- How to Report Problems and Provide Feedback
- Additional Sun Resources

OpenAM Snapshot 9 Hardware and Software Requirements

OpenAM Snapshot 9 supports most hardware and software requirements supported by OpenSSO Enterprise 8.0. For information, see the "Sun OpenSSO Enterprise 8 Release Notes."

> ⊘ **Java 6 Required**
>
> This release of OpenAM requires Java 6 to run. This is due to the product taking advantage of new features in Java 6.

Getting Started With OpenAM Snapshot 9

If you have not previously installed OpenAM or OpenSSO, here are the basic steps to follow:

1. If necessary, install, configure, and start one of the supported web containers.
2. Download and unzip the openam_release9_20100207.zip file from the following site: http://www.forgerock.org/downloads/openam_release9_20100207.zip
3. Deploy the `openam.war` file to the web container, using the web container administration console or deployment command. Or, if supported by the web container, simply copy the WAR file to the container's autodeploy directory.
4. Configure OpenAM snapshot 9 using either the GUI Configurator or the command-line Configurator.
   To launch the GUI Configurator, enter the following URL in your browser: `protocol://host.domain:port/deploy_uri`.
   For example: https://openam.example.com:8080/openam
5. Perform any additional configuration using either the OpenAM Administration Console or the `ssoadm` command-line utility.
6. To download a version 3.0 policy agent, see ....

What's New in OpenAM Snapshot 9

- OpenSSO Express 9 Beta Administration Console
- OpenSSO Express 9 Fedlet Changes
- OpenSSO Express 9 Entitlements Service
- Microsoft Active Directory 2008 as the OpenSSO Express 9 User Data Store
- OAuth Token Service (Early Release)
- Additional Enhancements

OpenAM Snapshot 9 Beta Administration Console

OpenAM Snapshot 9 includes an alternate Administration Console that allows you to access the new OpenAM Entitlements Service and to use new work flows (common tasks) for Federation and Web Service Security (WSS). For more information, see:

- "New Properties in the OpenAM Snapshot 9 Administration Console"
- "Using the legacy OpenSSO Express 8 Beta Administration Console"

OpenAM Snapshot 9 Fedlet Changes

You can enable XML signing and decryption. For more information, see "New Functionality for the OpenAM Snapshot 9 Java Fedlet."

You can enable ASP.NET Fedlet Single Logout. For more information, see:"Implementing ASP.NET Fedlet Single Logout with OpenAM Snapshot 9."

OpenAM Snapshot 9 Entitlements Service

The OpenAM Entitlements Service provides fine-grained access control. OpenAM Snapshot 9 includes RESTful interfaces (in the form of URLs) which have been developed for the Entitlements Service. For more information, see:

- "Introducing the OpenAM Snapshot 9 Entitlements Service REST Interfaces"
- "Using the OpenAM Snapshot 9 REST Listener Management Interfaces"
- "Using the OpenAM Snapshot 9 REST Policy Evaluation Interfaces"
- "Using the OpenAM Snapshot 9 REST Privilege Management Interfaces"

Microsoft Active Directory 2008 as the OpenAM Snapshot 9 User Data Store

OpenAM Snapshot 9 supports Microsoft Active Directory as the user data store. For more information, see
"Using Microsoft Active Directory 2008 as the OpenAM Snapshot 9 User Data Store"

OAuth Token Service (Early Release)

The Early Access version of the OpenAM OAuth Token Service supports the the following OAuth Core 1.0 Specifications: consumer site registration, Request Token requests, Request Token authorizations, and Access Token requests. These features allow OpenAM to be deployed as a service provider site. For more information, see "Introducing the OpenAM OAuth Token Service (Snapshot 9 Early Access)"

Additional Enhancements

- Session failover on the IBM AIX platform is now supported.
- OpenDS 2.2 is now supported as an OpenAM Snapshot 9 User Data Store.
- The Password Reset service is now supported on OpenDS 2.0 and later versions, Sun Directory Server Enterprise Edition 7.0, and Sun Directory Server Enterprise Edition 6.x.
- Symmetric keys for STS-issued tokens are now supported. See "New Functionality in the OpenAM Snapshot 9 Standard and Beta Administration Consoles."

Using Policy Agents with OpenAM Snapshot 9

OpenAM Snapshot 9 supports both version 3.0 and version 2.2 policy agents.

- ForgeRock is developing version 3.0 policy agents to function with OpenAM Releases and OpenAM Snapshots. However, version 3.0 agents are released on a separate schedule than OpenAM or OpenAM Snapshot releases. For the new features in version 3.0 policy agents, see one of these guides:
  - Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for J2EE Agents
  or
  - Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents

For information about version 3.0 agents, see http://docs.sun.com/coll/1767.1.

- Version 2.2 policy agents are compatible with OpenAM and OpenAM Snapshot releases. However, a version 2.2 agent must continue to store its configuration data locally in its `AMAgent.properties` file. And because the version 2.2 agent configuration data is local to the agent, OpenAM centralized agent configuration is not supported for version 2.2 agents. To configure a version 2.2 agent, you must continue to edit the agent's `AMAgent.properties` file.

For information about version 2.2 agents, see http://docs.sun.com/coll/1322.1.

Known Issues in This Release

- 4844: Fedlet single sign-on fails using IBM WebSphere Application Server 7.0
- 4859: Configurator buttons are not visible using Safari on a Mac
- 4862: OpenAM Snapshot 9 deployed on JBoss AS returns errors
- 4976: Cannot deploy OpenAM on Apache Geronimo 2.1.4
- 5168: OpenAM Snapshot 9 with new Console doesn't deploy on Oracle Application Server
- 5209:ssoadmcommands throw exception errors on IBM WebSphere Appplication Server 7.0
- 5324: Creating a group fails on IBM Tivoli Director Server as user data store
- 5326: Deleted group is not removed from group list with referential integrity enabled
- 5455: Configurator User Data Store settings password field is not rendered properly in Mozilla 1.7
- 5966: Cannot delete multiple identities using thedo-batchsub command
- 5970: Some Command-line commands fail when using JDK 1.6.0_18
- 6074: Configurator displays message "Cannot connect to Directory Server"
- 6079: Cannot deploy the OpenAM console-only WAR on GlassFish v2.1.1
- 6080: Cannot export multiple policies from the Beta Administration Console
- Configuring Session Failover when upgrading OpenAM from a Previous Version

4844: Fedlet single sign-on fails using IBM WebSphere Application Server 7.0

The OpenAM Fedlet fails if deployed on IBM WebSphere Application Server 7.0.

Workaround:

1. Download the OpenSSO External Library Bundle (`openam-fr-extlib.zip`) from [http://forgerock.org/openam.html|https://opensso.dev.java.net/public/use/index.html#source]
2. Unzip `openam-fr-extlib.zip` and add the following JAR files to the Fedlet `WEB-INF/lib` directory:

- `xalan.jar`
- `xercesImpl.jar`

4859: Configurator buttons are not visible using Safari on a Mac

When running the Configurator using Safari on a Mac, the Next and Cancel buttons are not visible, which gives the impression that the configuration cannot continue.

Workaround: Maximize the Safari browser to the fullest extent and scroll down to see the buttons.

4862: OpenAM Snapshot 9 deployed on JBoss AS returns errors

Attempting to deploy OpenAM Snapshot 9 on JBoss AS 5.0.0 or 5.1.0 returns class loader errors.

Workaround:

1. In a staging directory, extract the files from the `openam.war` file.
2. In the extracted files, create a text-file named `jboss-web.xml` in the `WEB-INF` directory.
3. In the jboss-web.xml file, enter the following:

```
<!DOCTYPE jboss-web PUBLIC "-//JBoss//DTD Web Application 5.0//EN"
"http://www.jboss.org/j2ee/dtd/jboss-web_5_0.dtd">
<jboss-web>
<class-loading java2ClassLoadingCompliance='true'>
        <loader-repository>
            jbia.loader:loader=openam
            <loader-repository-config>
                java2ParentDelegaton=true
            </loader-repository-config>
        </loader-repository>
    </class-loading>
    <resource-ref>
        <res-ref-name>jdbc/openamusersdb</res-ref-name>
        <jndi-name>java:jdbc/openamusersdb</jndi-name>
    </resource-ref>
</jboss-web>
```

4. Delete the following directory:
5. *jboss-release*/server/*server-name*/work/jboss.web/localhost/openam
   where *jboss-release* is the specific release such as jboss-5.1.0.GA and *server-name* is the JBoss AS server
   instance name.
6. Restart the JBoss AS container.
7. Deploy the `openam.war` file.

4976: Cannot deploy OpenAM on Apache Geronimo 2.1.4

When attempting to deploy OpenAM on Apache Germonimo 2.1.4, deployment fails and the following message is displayed: "Unable to deploy: WSDL
generation failed."

Workaround: Use Apache Geronimo 2.1.1.

5168: OpenAM Snapshot 9 with new Console doesn't deploy on Oracle Application Server

The OpenAM Snapshot 9 openam.war with the new console doesn't deploy on Oracle Application Server.

Workaround:

1. Download the following JAR files from http://www.forgerock.com/downloads/openam-fr-extlib.zip:
   - el-api-1.0.jar
   - el-ri-1.0.jar
2. Recreate the openam{{.war}} to include the JAR files from Step 1. For example:

   ```
   jar -xvf openam.war WEB-INF/lib
   cp <el-jar-location>/el-api-1.0.jar WEB-INF/lib
   cp <el-jar-location>/el-ri-1.0.jar WEB-INF/lib
   jar -uf openam.war WEB-INF/lib*
   ```

3. Before deployment, in the deployment plan, remove `oracle.toplink`, `oracle.xml`,and `oracle.xml.security` under the `classloader`
   settings.
4. In the Oracle Application Server OC4J's `java2.policy` file, add the following OpenAM permissions to the `grant` statement (in addition to the
   existing OpenAM permissions):

   ```
   permission java.lang.RuntimePermission "getClassLoader";
   permission java.lang.RuntimePermission "modifyThread";
   permission javax.security.auth.PrivateCredentialPermission
     "com.sun.identity.authentication.internal.AuthSSOToken * \"*\"","read";
   ```

5209: `ssoadm` commands throw exception errors on IBM WebSphere Appplication Server 7.0

When OpenAM is deployed on IBM WebSphere Application Server 7.0 on the IBM AIX 5.3 platform using JDK 1.6.0, exception messages are displayed on the
command-line when executing ssoadm commands. The ssoadm commands are successfully executed despite the messages being displayed. You can ignore
the exception messages. The ssoadm logs are written to the OpenAM server log directory.

5324: Creating a group fails on IBM Tivoli Directory Server as user data store

If you are using IBM Tivoli Directory Server as the OpenAM user data store, the configuration is successful, but an attempt to add a group fails.

Workaround:

1. Log in to the OpenAM Console as `amadmin`.
2. Click Access Control, *realm-name*, Data Stores, and then the name of the data store for Tivoli Directory Server.
3. On the Generic LDAPv3 page:
   - If the **Attribute Name for Group Membership** field has a value (such as `memberOf`), remove the value.
   - In **Default Group Member's User DN**, specify a user. For example: `cn=user,dc=example,dc=com`Tivoli Directory Server requires at
     least one user in a group before you can create the group.
4. Click Save.

5326: Deleted group is not removed from group list with referential integrity enabled

In this scenario, OpenAM Snapshot 9 is configured to use Sun Java System Directory Server as the remote user data store and referential integrity is enabled for the Directory Server entries. However, if a group is deleted in Directory Server, the group is not removed from the user's group list, even though referential integrity is enabled.

Workaround: For referential integrity to work properly, after you finish running the OpenAM Snapshot 9 Configurator, restart the remote Sun Directory Server.

5455: Configurator User Data Store settings password field is not rendered properly in Mozilla 1.7

If you are configuring OpenAM Snapshot 9 using the GUI Configurator with Mozilla 1.7, the Password field in the "Step 4: User Data Store Settings" screen is not rendered properly.

Workaround. To view the user data store settings correctly, reduce the font size in the browser.
Under View, reduce the text size to 75%, and the password field will display correctly.

5966: Cannot delete multiple identities using the `do-batch` sub command.

When attempting to delete multiple identities using the following do-bach sub command as in this example:

```
/ssoadm do-batch -u amadmin -f /tmp/.OpenAM_pass -D /tmp/del
```

the request is not processed as expected.

Workaround. In the `do-batch sub command`, use -Z instead of -D as the short option name for --batchfile.

5970: Some Command-line commands fail when using JDK 1.6.0_18

When OpenAM is deployed using JDK 1.6.0_18, some OpenAM command-line commands may fail.

Workaround. Use JDK 1.6_017 in this environment.

6074: Configurator displays message "Cannot connect to Directory Server"

This can occur when you don't provide a password when setting Configuration Data Store settings. In "Step 3: Configuration Data Store Settings" of the Configurator, if you don't enter a password, the Next button should be disabled. Instead, the Next button is enabled and you are inadvertenty allowed to proceed to the next step. The error message is displayed after you click Finish at the end of the program.

Workaround. Click "Return to Configurator," return to Step 3, and provide a password.

6079: Cannot deploy the OpenAM console-only WAR on GlassFish v2.1.1

After deploying the OpenAM `console.war` on GlassFish v2.1.1, when you click the URL to access the OpenAM login page, an ERROR 500 exception is thrown.

This occurs because This is because `esapiport.jar` is not present in the created console WAR.

Workaround. Obtain `esapiport.jar` from `openam.war`, and bundle it into the `console.war`.
After bundling this JAR, the exception is no longer displayed, and you should be able to access the OpenAM console.

6080: Cannot export multiple policies from the Beta Administration Console

On the Manage Policies of the page of the Beta Administration Console, when you select multiple policies and then click Export, the following message is displayed:

XML Parsing Error: junk after document element...

There is no workaround for this issue at this time.

Configuring Session Failover when upgrading OpenAM from a Previous Version

When you configure Session Failover after upgrading OpenAM from a previous version, you must manually unzip `ssoSessionTools.zip` and re-install its files. The new .zip file contains Message Queue 4.4. For detailed instructions, see "Installing and Configuring the OpenAM Enterprise Session Failover Components". Message Queue 4.4 is automatically installed on the OpenAM server when you unpack the openam.war file.

OpenAM Documentation

ForgeRock is working on providing an up to date documentation for the current release of OpenAM. in the meantime you can check the OpenSSO Enterprise 8.0 documentation, available at:

OpenSSO Enterprise 8.0 Documentation Center

Deprecation Notifications and Announcements

- The LDAP JDK file `ldapjdk.jar` was not included in OpenAM, beginning with OpenSSO Express 7 (predecessor of OpenAM).
- The Service Management Service (SMS) APIs (`com.sun.identity.sm` package) and SMS model will not be included in a future OpenAM release.
- The Unix authentication module and the Unix authentication helper (`amunixd`) will not be included in a future OpenAM release.
- The Sun Java System Access Manager 7.1 Release Notes stated that the Access Manager `com.iplanet.am.sdk` package, commonly known as the Access Manager SDK (AMSDK), and all related APIs and
  XML templates will not be included in future releases of OpenSSO (OpenAM predecessor), therefore it is not included in the OpenAM. Migration options are not available now and are not expected to be available in the future. OpenIDM provides user provisioning solutions that you can use instead of the AMSDK. For more information about Identity Manager, see http://www.forgerock.com/openidm.html.

How to Report Problems and Provide Feedback

If you have questions or issues with OpenAM Snapshot, report them in https://bugster.forgerock.org

If you are requesting help for a problem, please include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Machine type, operating system version, web container and version, JDK version, and OpenAM release version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any error logs or core dumps