Sun OpenSSO Enterprise 8.0 Release Notes

Part No: 820–3745–20
August 18, 2010

ORACLE

100818@24661

Contents

Sun OpenSSO Enterprise 8.0 Release Notes

Last revised August 18, 2010

OpenSSO Enterprise 8.0 is the commercial version of OpenSSO server.

Note – If you are using WebLogic Server as the web container to deploy OpenSSO Enterprise server, see "4077: OpenSSO Enterprise configuration on WebLogic Server requires new `ldapjdk.jar`" on page 30.

Contents

Getting Started With OpenSSO Enterprise 8.0

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

1. If necessary, install, configure, and start one of the "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23.
2. Download and unzip the `opensso_enterprise_80.zip` file. See the Sun Software Product Map page for more information:

   `http://www.oracle.com/us/sun/sun-products-map-075562.html`
3. Deploy the `opensso.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 OpenSSO Enterprise 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: `http://openssohost.example.com:8080/opensso`

   If OpenSSO Enterprise is accessing an Access Manager 7.1 schema (DIT) in coexistence mode, see "3961: `amadmin` cannot log in to OpenSSO Console in coexistence mode" on page 44.
5. Perform any additional configuration using the either Administration Console or the new `ssoadm` command-line utility.
6. To download a version 3.0 policy agent, see the following site:

   `http://www.oracle.com/technetwork/indexes/downloads/index.html`.

OpenSSO Enterprise 8.0 Documentation

The OpenSSO Enterprise 8.0 documentation is available on the following site:

`http://docs.sun.com/coll/1767.1`

Check this site periodically to view the most recent documentation.

Oracle OpenSSO 8.0 Update 2

Oracle OpenSSO 8.0 Update 2 is available to patch an existing deployment or install as a deployment. For information, see the *Oracle OpenSSO 8.0 Update 2 Release Notes*.

OpenSSO Enterprise 8.0 Update 1

OpenSSO Enterprise 8.0 Update 1 is available as patch 141655-01 on `http://sunsolve.sun.com/`. Update 1 includes a WAR file (`opensso.war`) that you can use to patch OpenSSO Enterprise 8.0 or install as a new OpenSSO Enterprise 8.0 Update 1 deployment.

For information about Update 1, including new features, hardware and software requirements, installation, and known issues with workarounds, see the *Sun OpenSSO Enterprise 8.0 Update 1 Release Notes*.

Patches to Update 1

Oracle periodically releases patches to OpenSSO Enterprise 8.0 Update 1 on `http://sunsolve.sun.com/`. To find the latest patch for Update 1, search for patch ID 141655. To determine if you should install a patch, check the README file available with the patch.

Each patch release includes an `opensso.war` file that you can deploy as follows:

- Patch an existing OpenSSO Enterprise 8.0 deployment
- Install a new OpenSSO Enterprise 8.0 deployment
- Create or patch one of the following specialized WAR files:
  - OpenSSO Enterprise Administration console only
  - OpenSSO Enterprise server only without the Administration console
  - OpenSSO Enterprise Distributed Authentication UI server
  - OpenSSO Enterprise IDP Discovery Service

For more information see Chapter 2, "Installing OpenSSO Enterprise 8.0 Update 1," in *Sun OpenSSO Enterprise 8.0 Update 1 Release Notes*.

What's New in OpenSSO Enterprise 8.0

OpenSSO Enterprise 8.0 includes features such as access management, federation management, and web services security that are found in earlier releases of Sun Java System Access Manager and Sun Java System Federation Manager. OpenSSO Enterprise also includes the new features described in this section.

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*
- Simplified installation and configuration:
  - To install OpenSSO Enterprise, you simply deploy the `opensso.war` file using the respective web container administration console or command-line utility. When you first access the server using the deployment URI (`/opensso`), you are directed to the Configurator, which allows you to perform initial configuration tasks such as specifying administrator passwords and the configuration and user data stores.
  - You can also create and deploy specialized WAR files for a distributed authentication UI server, console only, server only, and Identity Provider (IDP) Discovery Service deployments using the `opensso.war` file.
- Centralized server and agent configuration data:
  - OpenSSO Enterprise and version 3.0 policy agent configuration data is stored in a centralized configuration data repository. You specify configuration values using either the OpenSSO Enterprise Administration Console or the new `ssoadm` command-line utility. You no longer need to set properties in the `AMConfig.properties` or `AMAgent.properties` files.
  - Many of the configuration properties are "hot swappable," which means you do not have to restart the web container after you modify a property.
  - The Embedded data store option allows you to store OpenSSO Enterprise and version 3.0 policy agent configuration data transparently without having to install Sun Java System Directory Server.
- Command-line Configurator (in addition to the GUI Configurator) to perform the initial configuration of OpenSSO Enterprise server.
- OpenSSO Enterprise Administration Console Common Tasks:
  - Create SAMLv2 Providers. You can easily create a SAMLv2 hosted or remote Identity Provider (IDP) or Service Provider (SP).
  - Create a Fedlet. A Fedlet is a lightweight Service Provider (SP) implementation of SAMLv2 SSO protocols. A Fedlet allows an Identity Provider (IP) to enable an SP that does not have federation implemented. The SP simply adds the Fedlet to a Java web application and then deploys the application.
  - Test Federation Connectivity. You can test or troubleshoot new or existing federated deployments to determine if connections are being made successfully and to identify the source of any problems.
- New web containers are added, as described in "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23.
- Simplified Web Services Security agents can be deployed on GlassFish and Sun Java System Application Server 9.1 using providers based on the JSR 196 SPI.

- WS-Federation supports the Identity Federation specification. OpenSSO Enterprise specifically supports the WS-Federation Passive Requestor Profile.
- Support for XACML version 2.0 support is added, specifically for `XACMLAuthzDecisionQuery` and `XACMLAuthzDecisionStatement`, as specified in the SAML 2.0 profile of XACML v2.0.
- Secure Authentication and Attribute Exchange allows an application to provide user authentication and attribute information with secure transfers between IDP and SP applications.
- Multiple federation protocol hub allows an OpenSSO Enterprise IDP to act as federation hub to perform single logout among different federation protocols (such as SAMLv2, ID-FF, and WS-Federation).
- SAMLv2 profile support includes IDP proxying, Affiliation, NameID mapping, ECP, Authentication Query, and Attribute Query.
- Security Token Service (STS) is available on "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23.
- SAMLv2 assertion failover is supported.
- New command-line utility (`ssoadm`) can configure both OpenSSO Enterprise server and version 3.0 policy agents.
- Integration with Sun Identity Manager, SiteMinder, and Oracle Access Manager is added.
- Service Tags are supported. See "Using Service Tags With Sun Inventory" on page 21.
- The Distributed Authentication UI server includes a configurator that allows you to perform initial configuration tasks such as specifying the OpenSSO Enterprise server and providing the Distributed Authentication UI server user and password.

  A Distributed Authentication UI server also provides support for cross domain single sign-on (CDSSO).
- Internationalization and localization changes include:
  - In addition to English, OpenSSO Enterprise includes support for French, Spanish, German, Japanese, Korean, Simplified Chinese, and Traditional Chinese.
  - Localized files are bundled in the `opensso.war` file by default (unlike Access Manager 7 2005Q4 and Access Manager 7.1, where localized files reside in separate localized packages).
- Unix, SecurID, and SafeWord authentication modules are available in OpenSSO Enterprise releases. SecurID is now a Java-based authentication module.
- Upgrade support includes:
  - Upgrade to OpenSSO Enterprise 8.0 from Access Manager 7.0 or 7.1 and Federation Manager 7.0
  - Policy agent upgrade to version 3.0 from version 2.2 agents

Policy Agent 3.0-01 Release

The Policy Agent 3.0-01 release includes both Java EE (formerly called J2EE) agents and web agents:

Java EE Agents in the Policy Agent 3.0-01 Release

Patch IDs for Java EE Agents in the Policy Agent 3.0-01 Release

The following version 3.0–01 Java EE agents are available on `http://sunsolve.sun.com/`.

TABLE 1 Patch IDs for Java EE Agents in the Policy Agent 3.0-01 Release

Version 3.0-01 Policy Agent For	Patch ID
Oracle WebLogic Server 11g Release 1 (10.3.3)	145385-01
Oracle WebLogic Server 10g Release 3 (10.3)	
Oracle WebLogic Server 9.2 and 10.0	
Oracle WebLogic Portal 9.2, 10.0, and 10.2	
Sun GlassFish 2.1, V2 UR1, V2 UR2, and v3	145383-01
Sun Java System Application Server 8.1, 8.2, 9.0, and 9.1	
Apache Tomcat 6.0.x	145384-01
JBoss Application Server 4.x and 5.x	145382-01
IBM WebSphere Application Server 6.1 and 7.0	145386-01
IBM WebSphere Portal Server 6.1	

Enhancements and Changes for Java EE Agents in the Policy Agent 3.0-01 Release

Note – Version 3.0 and later Java EE agents require JDK 1.5 or later on the server where you plan to install the agent. Although some web containers such as JBoss Application Server 4.x and Application Server 8.x can run using JDK 1.4, JDK 1.5 or later is required for both the agent web container and the `agentadmin` program.

Support is added for GlassFish v3

The version 3.0–01 Java EE agent for Sun Java System Application Server and GlassFish v2 also supports GlassFish v3. See also "Patch IDs for Java EE Agents in the Policy Agent 3.0-01 Release" on page 10.

Issue 5633: New property is added to reset session idle time for not-enforced URLs

Version 3.0–01 Java EE agents include the following new property to specify whether the session idle timeout should be reset after a user with a valid session accesses a URL in the not-enforced list:

```
com.sun.identity.agents.config.notenforced.refresh.session.idletime
```

Values for this property can be:

- `true`: The session idle time is reset after a user with a valid session accesses a URL in the not-enforced list.
- `false` (default): The session idle time is not reset.

Set this property depending on the location of the agent's configuration repository. If the repository is local to the agent's host server, add the property to the agent's `OpenSSOAgentConfiguration.properties` file and restart the OpenSSO server instance.

If the agent's configuration repository is centralized, use the OpenSSO Administration Console as follows:

1. Log in to the OpenSSO Administration Console.
2. Click Access Control, *realm-name*, Agents, J2EE, *j2ee-agent-name*, and then Advanced.

3. Under Custom Properties, add the new property with its corresponding value.
4. Click Save.

Issue 6107: JBoss Application Server agent supports custom principal feature

JBoss Application Server 4.x and 5.x login modules support the custom principal feature, which allows users to specify a custom principal in the JBoss AS configuration. The version 3.0–01 agent for JBoss AS 4.x and 5.x also supports the custom principal feature.

To use this feature, add the following line to the `<login-module>` element in the *JBOSS_HOME*`/server/default/conf/am-login-config.xml` file:

```
<module-option name = "principalClass">com.sample.CustomPrincipal</module-option>
```

For example, the `<login-module>` element should then be as follows:

```
<login-module code = "com.sun.identity.agents.jboss.v40.AmJBossLoginModule"
                  flag = "required">
    <module-option name = "unauthenticatedIdentity">anonymous</module-option>
    <module-option name = "principalClass">com.sample.CustomPrincipal</module-option>
</login-module>
```

In this example, `com.sample.CustomPrincipal` is the custom principal implementation class name. This class must be in the JBoss AS `classpath`.

Issue 6108: JBoss Application Server agent redirects to the client's requested URI

If the requested URI is using `J2EE_POLICY` or `ALL` filter mode and a user accesses a resource protected with J2EE policies by the version 3.0–01 JBoss AS 4.x and 5.x agent, the user is redirected to the client's requested resource after authentication by OpenSSO 8.0 server. Previously, the user was redirected to the client's home page.

Issues and Workarounds for Java EE Agents in the Policy Agent 3.0-01 Release

CR 6976312: Install fails for WebSphere Application Server agent using IBM JDK on all systems except AIX

If you run the `agentadmin` or `agentadmin.bat` script to install the version 3.0-01 policy agent for IBM WebSphere Application Server 6.1/7.0 or IBM WebSphere Portal Server 6.1 using the IBM JDK on systems other than IBM AIX, the installation fails because the script cannot find the IBM JCE provider.

Workaround: Add following JAVA options to the `agentadmin` or `agentadmin.bat` script and then rerun the installation:

```
AGENT_OPTS="-DamKeyGenDescriptor.provider=IBMJCE
-DamCryptoDescriptor.provider=IBMJCE
-DamRandomGenProvider=IBMJCE"
```

CR 6976304: WebSphere Application Server administrative console cannot be accessed

After you install the version 3.0-01 policy agent for WebSphere Application Server 6.1/7.0 or IBM WebSphere Portal Server 6.1, you cannot access the WebSphere administrative console.

Workaround. In the WebSphere Application Server agent profile, add the WebSphere administrative console URL in the Agent Root URL for CDSSO list, as follows:

1. Log in to the OpenSSO Administration Console.
2. Click Access Control, *realm-name*, Agents, J2EE, and then the *j2ee-agent-name*.
3. In Agent Root URL for CDSSO, add the WebSphere administrative console URL.
4. Click Save.

CR 6976308: WebSphere Application Server administrative console redirects to an incorrect URL in CDSSO mode

After you install the version 3.0-01 policy agent for WebSphere Application Server 6.1/7.0 or IBM WebSphere Portal Server 6.1 in cross-domain single sign-on (CDSSO) mode and try to access the administrative console, you are redirected to an incorrect `agentapp` URL. The URL port is pointing to the admin port instead of the `agentapp` instance port.

Workaround. In the URL in the browser address bar, manually specify the correct port number for the `agentapp` instance.

Problems Fixed for Java EE Agents in the Policy Agent 3.0-01 Release

TABLE 2 Problems Fixed for Java EE Agents in the Policy Agent 3.0-01 Release

CR or Issue	Description
6121	401 error is returned instead of a 302 error when the client presents an invalid SSO Token
4461	Security context exception occurred with JBoss AS agent
6107	Custom principal in JBoss AS 4.3 is not working with J2EE agent
6108	J2EE Agent 3.0 for JBoss AS does not redirect to client request
4969	Tomcat agent J2EE tests are denied when debug level set to error mode
2779	J2EE agents should have the `agentadmin` script executable permission set by default
5008	GlassFish v3 server fails to start with invalid format error
5012	Tomcat 6.0 version 3.0 agent returns error with not-enforced IP list
5764	`agentadmin` script does not set up `classpath` correctly on GlassFish V3
4677	Tomcat 6.0 agent membership removal causes HTTP 403 access denied error
5197	Application logout does not clean up sessions
5744	Issue with URL pattern matching for port number in J2EE agents
4959	HTTPS session binding should be enabled by default in agent profile
5024	When not-enforced IP is used, accessing application of declarative security returns configuration error
5071	J2EE agent with CDSSO, cookie hijacking, and composite advice has second login issue
5633	J2EE agent does not reset session idle time for not-enforced URLs
5627	IP Resource condition fails if login URL in agent profile has `resource=true` included
6933534	Tomcat 6.0 version 3.0 agent classes are not added to `classpath` resulting in Tomcat startup failure

Web Agents in the Policy Agent 3.0-01 Release

Patch IDs for Web Agents in the Policy Agent 3.0-01 Release

The following version 3.0–01 web agents are available on `http://sunsolve.sun.com/`.

TABLE 3 Patch IDs for Web Agents in the Policy Agent 3.0-01 Release

Version 3.0-01 Policy Agent For	Patch ID
Apache HTTP Server 2.0.x	144698–01
Apache HTTP Server 2.2.x	144699–01
Microsoft Internet Information Services (IIS) 6.0 Supported on Microsoft Windows Server 2003, with separate agents for 32–bit and 64–bit systems.	144700–01
Microsoft Internet Information Services (IIS) 7.0 and 7.5 Supported on Microsoft Windows Server 2008 R2, with separate agents for 32–bit and 64–bit systems.	144701–01
Sun Java System Web Proxy Server 4.0.x	144702–01
Sun Java System Web Server 7.0	144703–01

Enhancements and Changes for Web Agents in the Policy Agent 3.0-01 Release

For more information about web agent properties, see the *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents*.

CR 6891373: New Properties Support POST Data Preservation With Sticky Sessions

In the 3.0–01 release, new properties support POST data preservation with sticky sessions configured. If you are using POST data preservation with a load balancer deployed in front of the agent, set the following properties for sticky sessions:

- `com.sun.am.policy.agents.config.postdata.preserve.stickysession.mode` specifies the sticky session mode. The values can be `COOKIE` if the load balancer uses a cookie to get the sticky session or `URL` if the load balancer uses a query parameter in the URL to get the sticky session. For example:

  ```
  com.sun.am.policy.agents.config.postdata.preserve.stickysession.mode = URL
  ```

- `com.sun.am.policy.agents.config.postdata.preserve.stickysession.value` specifies the name and value of the cookie or query parameter used for the sticky session. For example:

  ```
  com.sun.am.policy.agents.config.postdata.preserve.stickysession.value = AgentID=01
  ```

Important: For a sticky session to be set, you must set both of these properties correctly (and not to null).

These new properties are in the `OpenSSOAgentConfiguration.properties` file. Set these properties depending on the location of your agent's configuration repository. If the repository is local to the agent's host server, edit the agent's `OpenSSOAgentConfiguration.properties` file.

If the agent's configuration repository is centralized, use the OpenSSO Console:

1. Log in to the OpenSSO Administration Console.
2. Click Access Control, *realm-name*, Agents, Web, *web-agent-name*, and then Advanced.
3. Under Custom Properties, add both new properties with their corresponding values.
4. Click Save.

CR 6903850: Wildcard (*) Support Added for Not-Enforced Client IP List

The policy agent `com.sun.identity.agents.config.notenforced.ip` property in the `OpenSSOAgentConfiguration.properties` file now allows the wildcard character (*) to define an IP address. For example:

```
com.sun.identity.agents.config.notenforced.ip[2] = 192.168.11.*
com.sun.identity.agents.config.notenforced.ip[3] = *.10.10.*
```

Set this agent property depending on the location of your agent configuration repository. If the repository is centralized on the OpenSSO server, use the OpenSSO Console. If the repository is local to the agent's host server, edit the agent's `OpenSSOAgentConfiguration.properties` file.

CR 6947499: NSS_STRICT_NOFORK Must be Disabled for Version 3.0–01 Apache Agents

The NSS and NSPR libraries used in the policy agent 3.0–01 release have changed since the version 3.0 agents were released. Therefore, to use the version 3.0–01 Apache HTTP Server 2.0.x or Apache HTTP Server 2.2.x policy agent on any platform, the `NSS_STRICT_NOFORK` environment variable must be set to `DISABLED`.

Problems Fixed for Web Agents in the Policy Agent 3.0-01 Release

Problems Fixed For All Web Agents

TABLE 4 Problems Fixed For All Web Agents

CR or Issue	Description
1776	Not-enforced list does not work in special circumstances
3755	Non-IP Based Token Restrictions not working with Access Manager 7 and version 3.0 agents
4755	Log message sent by Web Server 7.0 2.2 agent has an empty `recMsg`
4836	Policy agent should encode special characters in cookies by URL encoding
4917	Log a "no policy or action decision found" message at warning level
5060	3.0 Apache agents have issue with agent logout feature
5155	Support for x-forwarded-for headers in web agents
5229	Expired `AppSSOToken` during agent configuration fetch
5259	Cannot use wildcard characters in the path info part of URL in not enforced list
5266	In CDSSO mode, corrupted headers are included in the response
5323	Web agents remove CDSSO parameters from URL incorrectly
5413	Application parameters getting corrupted when CDSSO parameters are removed from the query
5425	Composite advice getting duplicated whenever access manager is restarted
5434	Apache agent doesn't work properly with `mod_python` handler
5453	Requests with existing `iPlanetDirectoryPro` cookies can cause Assertion to be ignored during session upgrade in CDSSO mode
5538	Agent crashes web server when setting long value for `amlbcookie`
5552	Policy evaluation fails when the request URL contains query parameters
5637	Agent doesn't work due to variable initialization issue

TABLE 4 Problems Fixed For All Web Agents *(Continued)*

CR or Issue	Description
5666	Problems when path info is "/"
6086	Agent enforce URL case sensitivity during policy evaluation
6903850	Provide wildcard (*) support for Not Enforced Client IP List
6953714	Agent hangs while fetching policy decision if user session is validated from cache and policy has expired
6954327	In CDSSO, double POST issue problem during session upgrade
6774751	Access Manager 7.1 protected page is jumbled when session is upgraded
6959619	Host name is not set correctly when there is a load balancer in front of the agent

Problems Fixed for the Apache HTTP Server 2.0.x and 2.2.x Agents

TABLE 5 Problems Fixed for the Apache HTTP Server 2.0.x and 2.2.x Agents

CR or Issue	Description
4501	Additional HTTP methods support for version 3.0 Apache agent
4799	Some extra information gets printed on protected pages intermittently
5640	Attributes headers issue with 3.0 agent on IBM AIX systems
6947499	Apache 2.2 agent does not work when SSL enabled

Problems Fixed for the Sun Java System Web Server 7.0 Agent

TABLE 6 Problems Fixed for the Sun Java System Web Server 7.0 Agent

CR or Issue	Description
4688	Web Server agent notifications not working with protocol and port rewriting
4815	Memory corruption with POST data preservation
4911	Cookie reset for CDSSO set on incorrect domain
4934	Problem with POST data preservation feature in Web Server 7.0 agent
5207	Need a sticky cookie for load balancing with POST data preservation
5218	POST preservation data feature doesn't work with virtual hosts
5526	POST data preservation is not used when PA redirects as a result of composite advice
5532	Agent crashes web server when root policy is not found

TABLE 6 Problems Fixed for the Sun Java System Web Server 7.0 Agent *(Continued)*

CR or Issue	Description
5706	Need sticky session for POST data preservation to use URL
6937576	IIS 6.0 and web server agents do no handle overridden URL properly
6958056	POST data preservation feature doesn't work with normal FQDN and virtual hosts

Problems Fixed for the Sun Java System Web Proxy Server 4.0.x Agent

TABLE 7 Problems Fixed for the Sun Java System Web Proxy Server 4.0.x Agent

CR or Issue	Description
4911	Cookie reset for CDSSO set on incorrect domain
5680	Policy agent 2.2-02 on Web Proxy Server 4.0.4 has memory leak
6937576	IIS 6.0 and Web Server agents do no handle overridden URL properly
6953702	Cannot access CGIs through Web Proxy Server 3.0 agent in CDSSO mode

Problems Fixed for the Microsoft Internet Information Services (IIS) 6.0 Agent

TABLE 8 Problems Fixed for the Microsoft Internet Information Services (IIS) 6.0 Agent

CR or Issue	Description
4815	Memory corruption with POST data preservation
4816	Random crashes with IIS 6.0 agent
5207	Need a sticky cookie for load balancing with POST data preservation
5218	POST preservation data feature doesn't work with virtual hosts
5526	POST data preservation is not used when PA redirects as a result of composite advice
5532	Agent crashes Web Server when root policy is not found
5621	IIS 6.0 agent is not responding with OK message to notifications from server
5706	Need sticky session for POST data preservation to use URL
6929312	IIS agent: Existing header as `reutersuuid` will be replaced by a new header that contains its key
6937576	IIS 6.0 and web server agents do not handle overridden URL properly
6958056	POST data preservation feature doesn't work with normal FQDN and virtual hosts

Problems Fixed for the Microsoft Internet Information Services (IIS) 7.0 Agent

TABLE 9 Problems Fixed for the Microsoft Internet Information Services (IIS) 7.0 Agent

CR or Issue	Description
5621	IIS 6.0 Agent is not responding with OK message to notifications from server
6929312	For IIS 7.0 agent, existing header as `reutersuuid` will be replaced by a new header that contains its key
6937576	IIS 6.0 and Web Server agents do no handle overriden URL properly
6956162	"Object Moved error" with redirects in Policy Agent 3.0 for IIS 7.0
6956232	Policy Agent 3.0 for IIS 7.0 changes ASP.NET session ID
6955905	Server problems when cookie reset is enabled in IIS 7.5
6934736	IIS 7.0 agent is not responding with OK message to notifications from server

Installation of Version 3.0-01 Policy Agents

A version 3.0-01 policy agent requires a full installation. If you have a version 3.0 agent already installed, you must uninstall the existing version 3.0 agent and then reinstall the new version 3.0-01 agent. To install a version 3.01–01 agent, follow these steps:

1. If you have a version 3.0 agent installed, uninstall the agent by following the instructions in the respective Policy Agent 3.0 guide in the OpenSSO Enterprise 8.0 documentation collection: `http://docs.sun.com/coll/1767.1`.

   Important: Before you uninstall the agent, back up your existing agent deployment. For example, for the Apache HTTP Server 2.2.x agent, back up the files under *AgentHome*`/web_agents/apache22_agent`, where *AgentHome* is where you installed the agent.
2. Create a directory to download the version 3.0–01 patch file.
3. Download the patch for the agent you want to install from `http://sunsolve.sun.com/`.
4. In the download directory, unzip the version 3.0–01 patch file. A patch for a web agent contain a README file and separate ZIP files for each platform supported by the specific agent you downloaded. A patch for a Java EE agent contains one ZIP file for all supported platforms.
5. Unzip the file for your specific platform.

   The files and directories required by the specific agent are then available in the *zip-root*`/web_agents/`*agent-name* directory, where *zip-root* is where you unzipped the file and *agent-name* identifies the specific agent.

Check the README available with the agent for more information about the agent for your specific platform.

6. Install and configure the version 3.0–01 agent by following the instructions in the respective Policy Agent 3.0 guide in the OpenSSO Enterprise 8.0 documentation collection: `http://docs.sun.com/coll/1767.1`.

   Note: Version 3.0 and later agents require JDK 1.5 or later on the server where you plan to install the agent. Before you run the `agentadmin` program to install the agent, set your `JAVA_HOME` environment variable to point to the JDK installation directory.

Using Service Tags With Sun Inventory

OpenSSO Enterprise 8.0 is Service Tag enabled, which allows you to use Sun Inventory to track and organize your OpenSSO product (as well as other hardware and software products). To use Service Tags, you must first register your product.

To register, you need a Sun Online Account (SOA) or Sun Developer Network (SDN) account. If you do not have one of these accounts, you can get an account during the product registration process.

To register your OpenSSO product and start using Service Tags, follow these steps:

1. Log in to the OpenSSO Admin Console as `amadmin`.
2. On the Console, under `Common Tasks`, click `Register This Product`.
3. If you do not have an SOA or SDN account, provide the information for a new account.
4. Click `Register`.

Service Tag registration files are stored in the *config-directory*/*deployuri*`/lib/registration` directory. For example: `opensso-config/opensso/lib/registration`.

For more information, see:

- Sun Inventory: `https://inventory.sun.com/inventory/`
- Service Tags FAQs: `http://servicetags.central/faq.html`

Check these sites to see if Service Tags are supported on your specific platform, or if you need to determine if a specific OpenSSO server is already registered.

Hardware and Software Requirements For OpenSSO Enterprise 8.0

Note – The hardware and software requirements for OpenSSO Enterprise 8.0 described in this section represent the only environments in which it can be deployed with full support from Sun Microsystems. No support is provided for environments that do not meet the stated requirements.

Sun Microsystems assumes no responsibility or liability for any environments that don't adhere to supported hardware and software requirements for OpenSSO Enterprise 8.0 as documented. Sun strongly recommends that you involve the Sun Professional Services organization before you begin the installation and deployment process. This may require additional expense on your part.

Caution – If you plan to use the OpenSSO configuration data store, you must deploy OpenSSO Enterprise on a local file system and not on an NFS-mounted file system. The OpenSSO configuration data store, which is deployed with OpenSSO Enterprise, is not supported on an NFS-mounted file system.

Platforms Supported For OpenSSO Enterprise 8.0

TABLE 10 Platforms Supported For OpenSSO Enterprise 8.0

Platform	Supported Web Containers
Solaris 10 OS on SPARC, x86, and x64 based systems Solaris 9 OS on SPARC, x86, and x64 based systems	All "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23 except for Geronimo Application Server 2.1.1 with Tomcat only
OpenSolaris	GlassFish Application Server V2 UR1 and UR2 Apache Tomcat 6.0.18

TABLE 10 Platforms Supported For OpenSSO Enterprise 8.0 *(Continued)*

Platform	Supported Web Containers
Red Hat Enterprise Linux 5 Base and Advanced Platform on Intel 32–bit (x86) servers and AMD 64–bit (x86_64) servers Red Hat Enterprise Linux 4 server Base and Advanced Platform on Intel 32–bit (x86) servers and AMD 64–bit (x86_64) servers	All "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23 except Geronimo
Ubuntu 8.0.4	GlassFish Application Server V2 UR1 and UR2 Apache Tomcat 6.0.18
Windows Server 2003 Standard Edition Windows Server 2003 Enterprise Edition Windows Server 2003 Datacenter Edition	All "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23 except Geronimo
Windows Server 2003 R2 on 64–bit servers	All "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23
Windows XP Windows Vista	All "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23 except Oracle Server, JBoss Application Server, and Geronimo
Windows 2008 Server	GlassFish Application Server V2 UR1 and UR2 Apache Tomcat 6.0.18
IBM AIX 5.3	IBM WebSphere Application Server 6.1

Notes:

- OpenSSO Enterprise supports patches and updates to these base releases? For example, subsequent patches and updates to Red Hat Linux 4.7 or Red Hat Linux 5.2 are supported.
- If not specifically documented for a platform, OpenSSO Enterprise supports 32–bit and 64–bit versions of an operating system if the supported OpenSSO Enterprise web container is also supported in the 32–bit and 64–bit mode on the same system.

Web Containers Supported For OpenSSO Enterprise 8.0

TABLE 11 Web Containers Supported For OpenSSO Enterprise 8.0

Web Container	Considerations
Sun Java System Application Server 9.1 Update 1 and Update 2	Download: `http://www.oracle.com/technetwork/indexes/downloads/index.html`

TABLE 11 Web Containers Supported For OpenSSO Enterprise 8.0 *(Continued)*

Web Container	Considerations
GlassFish Application Server V2 UR1 and UR2	GlassFish site: `https://glassfish.dev.java.net/` GlassFish download locations: GlassFish V2 UR1: `https://glassfish.dev.java.net/downloads/v2ur1-b09d.html` GlassFish V2 UR2: `https://glassfish.dev.java.net/downloads/v2ur2-b04.html`
Sun Java System Web Server 7.0 Update 3 (32–bit and 64–bit)	Download: `http://www.oracle.com/technetwork/indexes/downloads/index.html` Update 3 only. Updates 1 and 2 are **not** supported.
Apache Tomcat 5.5.27 and 6.0.18 and later	See `http://tomcat.apache.org/`
Oracle WebLogic Server 9.2 MP2	See `http://www.oracle.com/us/products/middleware/application-server/index.htm`
Oracle WebLogic Server 10	See `http://www.oracle.com/us/products/middleware/application-server/index.htm` For the supported operating systems, see the following site: `http://download.oracle.com/docs/cd/E13196_01/platform/suppconfigs/index.html#1122259`
Oracle Application Server 10g	See `http://www.oracle.com/technetwork/indexes/products/index.html` Version 10.1.3.1 is supported.
IBM WebSphere Application Server 6.1	See `http://www-01.ibm.com/software/webservers/appserv/was/`
Apache Geronimo Application Server 2.1.1	See `http://geronimo.apache.org/` Supported **only** with Tomcat on Solaris systems.
JBoss Application Server 4.x	See `http://www.jboss.com/`

For more information, including considerations and pre-deployment tasks for each web container, see Chapter 2, "Deploying the OpenSSO Enterprise Web Container," in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

JDK Requirements For OpenSSO Enterprise 8.0

TABLE 12 JDK Requirements For OpenSSO Enterprise 8.0

OpenSSO Enterprise 8.0	Supported JDK Version
Server	JDK 1.5.x or 1.6.x 64-bit JVM on supported web containers **Solaris virtual memory requirements**. For Solaris systems, configure at least twice as much virtual memory as the JVM heap size, especially when the JVM is configured in 64–bit mode with over 4 GB for the heap size. Therefore, you might need to increase the operating system swap space.
Client (OpenSSO SDK)	JDK 1.4.x, 1.5.x. or JDK 1.6.x

Data Store Requirements For OpenSSO Enterprise 8.0

TABLE 13 Data Store Requirements For OpenSSO Enterprise 8.0

Data Store Type	Supported Data Stores
Configuration data store (also referred to as the Service Management data store)	■ OpenSSO configuration data store **Note**: If you specify the OpenSSO configuration data store, you must deploy OpenSSO Enterprise on a local file system, because the OpenSSO configuration data store is **not** supported on an NFS-mounted file system. ■ Sun Java System Directory Server 5.2, 6.0, 6.3, and 6.3.1
User data store	■ Sun Java System Directory Server 5.2, 6.0, 6.3, and 6.3.1 ■ Microsoft Active Directory 2003 on Windows Server 2003 R2 ■ IBM Tivoli Directory Server 6.1 ■ OpenSSO user data store **Note**: The OpenSSO user data store is **not** supported for production deployments. It is recommended only for prototype, proof of concept (POC), or developer deployments that have a small number of users.

TABLE 13 Data Store Requirements For OpenSSO Enterprise 8.0 *(Continued)*

Data Store Type	Supported Data Stores
Caution: Sun Java System Directory Server 6.2 is **not** recommended. For more information, see `http://sunsolve.sun.com/search/document.do?assetkey=1-66-235361-1`.	

For more information about data stores, see Chapter 2, "Building the Deployment Architecture," in *Sun OpenSSO Enterprise 8.0 Deployment Planning Guide*.

Session Failover Requirements for OpenSSO Enterprise 8.0

TABLE 14 Session Failover Requirements for OpenSSO Enterprise 8.0

Component	Requirement
OpenSSO Enterprise 8.0	Two or more OpenSSO Enterprise instances must be running on different host servers and configured as a site behind a load balancer. The load balancer does not have any specific requirements. However, a load balancer that supports cookie-based sticky configuration usually provides better performance.
Sun Java System Message Queue 4.1	Message Queue brokers must be running in cluster mode on different servers.
Oracle Berkeley DB 4.6.18	The Berkeley DB client and database must be deployed on the same servers as the Message Queue brokers. You can deploy the Message Queue brokers and Berkeley DB on the same servers that are running the OpenSSO Enterprise instances. However, for improved performance, consider installing the brokers on different servers.

For more information, see Chapter 8, "Implementing OpenSSO Enterprise Session Failover," in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

Policy Agents Supported for OpenSSO Enterprise 8.0

TABLE 15 Policy Agents Supported for OpenSSO Enterprise 8.0

Policy Agent Version	OpenSSO Enterprise Support
Version 3.0 policy agents	OpenSSO Enterprise supports new version 3.0 J2EE and web policy agents, including new version 3.0 features. For more information, including the available version 3.0 agents, see `http://docs.sun.com/coll/1767.1`.
Version 2.2 policy agents	OpenSSO Enterprise supports version 2.2 J2EE and web policy agents. However, when deployed with OpenSSO Enterprise, a version 2.2 policy agent must continue to use version 2.2 features. For example, the agent must store its configuration data locally in its `AMAgent.properties` file, and OpenSSO Enterprise centralized agent configuration is not supported. For more information, including the available version 2.2 agents, see `http://docs.sun.com/coll/1322.1`.
Version 2.1 policy agents	OpenSSO Enterprise does **not** support version 2.1 policy agents.

Database Logging Requirements For OpenSSO Enterprise 8.0

TABLE 16 Database Logging Requirements For OpenSSO Enterprise 8.0

Database	OpenSSO Enterprise Requirements
MySQL	MySQL version 4.1.1 or later, because the OpenSSO Enterprise logger uses the MySQL `STR_TO_DATE` function. **Note**: The Solaris 10 OS includes MySQL Server 4.0.37, so you must upgrade this MySQL version to use OpenSSO Enterprise database logging.
Oracle	Oracle Database 10g or later

Hardware Requirements For OpenSSO Enterprise 8.0

TABLE 17 Hardware Requirements For OpenSSO Enterprise 8.0

Component	Requirement
RAM	Prototype or developer deployment: 1 GB Production deployment: 4 GB recommended

TABLE 17 Hardware Requirements For OpenSSO Enterprise 8.0 *(Continued)*

Component	Requirement
Disk space	For OpenSSO Enterprise server with console, server only, or console only deployment: ■ Server: 512 MB for OpenSSO Enterprise binary files and configuration data ■ Log files: 7 GB for log files, including container log files For client SDK deployment: ■ Client SDK: 100 MB minimum ■ Log files: 5 GB recommended for debug logs, if debug level (`com.iplanet.services.debug.level`) is set to `message` **Considerations for log files**: The log file requirements depend on the actual production load and can be adjusted accordingly. The disk space requirements are based on the default 100 MB log file size, with one history file per log file type. Several considerations are: ■ Delete the debug log files periodically, especially if the debug level is set to `message`. ■ Check the `.access` and `.error` logs periodically in the `logs` directory for their size and contents. ■ Consider configuring the log rotation to delete the oldest log files.

Web Browsers Supported For OpenSSO Enterprise 8.0

TABLE 18 Web Browsers Supported For OpenSSO Enterprise 8.0

Browser	Platform
Firefox 2.0.0.x and 3.0.x	Windows Vista, Windows XP, and Windows Server 2003 Solaris OS, versions 9 and 10 Red Hat Linux 4 and 5 Mac OS X 10.4 and later
Firefox 1.0.7 and 1.5	Windows XP Windows 2000 Solaris OS, versions 9 and 10 Red Hat Linux 4 and 5
Microsoft Internet Explorer 7	Windows Vista, Windows XP, and Windows Server 2003
Microsoft Internet Explorer 6.0 SP1	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000

TABLE 18 Web Browsers Supported For OpenSSO Enterprise 8.0 *(Continued)*

Browser	Platform
Mozilla 1.7.12	Solaris OS, versions 9 and 10
	Windows XP
	Windows 2000
	Red Hat Linux 4 and 5

OpenSSO Enterprise 8.0 Issues

For more information about OpenSSO Enterprise issues, see:

`https://opensso.dev.java.net/servlets/ProjectIssues`

Web Container and Server Issues

- "3837: Configuration fails on Oracle Application Server 10g" on page 34
- "2222: Password reset and account lockout services report notification errors" on page 34

CR 6935896: Undeploying OpenSSO Enterprise on Sun GlassFish 2.1 using the CLI is unsuccessful

Trying to undeploy OpenSSO Enterprise 8.0 on Sun GlassFish 2.1 or Sun Java System Application Server 9.1 Update 2 is not successful and returns an "Invalid user or password" error (reported by CR 6808492). Subsequent attempts also fail with the same error message.

Workaround. This problem has been fixed in OpenSSO Enterprise 8.0 Update 1 Patch 3 (patch ID 141655-04). The following workaround applies to OpenSSO Enterprise 8.0 deployments before patch 3:

1. In the *appSrvr_install_directory*`/domains/domain1/config/domain.xml` file, add the following entry under the `java-config` attribute:

   ```
   <jvm-options>
   -Dorg.apache.catalina.loader.WebappClassLoader.ENABLE_CLEAR_REFERENCES=false
   </jvm-options>
   ```

2. Restart the GlassFish or Application Server instance.
3. Undeploy OpenSSO Enterprise 8.0 using the GlassFish or Application Server `asadmin undeploy` command.

4077: OpenSSO Enterprise configuration on WebLogic Server requires new `ldapjdk.jar`

OpenSSO Enterprise configuration fails on WebLogic Server because `weblogic.jar` bundles an older `ldapjdk.jar` file.

Sun provides a new `ldapjdk.jar` file that includes security and performance related fixes. You must provide the following workaround for both WebLogic Server 9.2 and WebLogic Server 10.

Workaround. Put the Sun `ldapjdk.jar` ahead of `weblogic.jar` in the `CLASSPATH`, as follows:

1. Extract `ldapjdk.jar` from `opensso.war` in a temporary directory using the following command:

   ```
   jar xvf opensso.war WEB-INF/lib/ldapjdk.jar
   ```

2. Copy the above extracted `ldapjdk.jar` to the WebLogic `lib` directory.

   For example, for WebLogic Server 10 on Solaris or Linux systems: *BEA_HOME*`/weblogic_10.0/server/lib`

   Or, for WebLogic Server 9.2 on Windows:*BEA_HOME*`\weblogic92\server\lib`

3. Prefix the path to this `ldapjdk.jar` to the existing `classpath`. by editing the startup script used to start WebLogic Server. In the following examples, *BEA_HOME* is where WebLogic Server is installed.

For WebLogic 9.2 on Windows, edit:

BEA_HOME\weblogic92\samples\domains\wl_server\bin\startWebLogic.cmd

Change `set CLASSPATH=%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%` to:

```
set CLASSPATH=BEA_HOME\weblogic92\server\lib\ldapjdk.jar;%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%
```

For WebLogic 10 on Windows, edit:

BEA_HOME\wlserver_10.0\samples\domains\wl_server\bin\startWebLogic.cmd

Change `set CLASSPATH=%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%` to:

```
set CLASSPATH=
BEA_HOME\wlserver_10.0\server\lib\ldapjdk.jar;%CLASSPATH%;%MEDREC_WEBLOGIC_CLASSPATH%
```

For WebLogic 9.2 MP2 on Solaris or Linux, edit:

/bea/weblogic92/samples/domains/wl_server/bin/ startWebLogic.sh

or

/usr/local/bea/user_projects/domains/base_domain/bin/startWebLogic.sh

Change `CLASSPATH="${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"` to:

```
CLASSPATH=
"BEA_HOME/weblogic92/server/lib/ldapjdk.jar${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"
```

For WebLogic 10 on Solaris or Linux, edit:

/bea/wlserver_10.0/samples/domains/wl_server/bin/startWebLogic.sh

or

/bea/user_projects/domains/wl10_domain/bin/startWebLogic.sh

Change `CLASSPATH="${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"` to

```
CLASSPATH=
"BEA_HOME/wlserver_10.0/server/lib/ldapjdk.jar${CLASSPATH}${CLASSPATHSEP}${MEDREC_WEBLOGIC_CLASSPATH}"
```

4. Restart the server.
5. Configure OpenSSO Enterprise.

WebLogic Server `StuckThreadMaxTime` value is exceeded during configuration

If you are configuring WebLogic Server 9.2 MP2 or 10 using the Configurator and you take longer than 600 seconds to finish the configuration, the following error is returned to the terminal and WebLogic Server domain and server logs:

```
<Error> <WebLogicServer> <BEA-000337> <[STUCK] Exe
cuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy
for "681" seconds working on the request "Http Request: /opensso/setup/setSetup
Progress", which is more than the configured time (StuckThreadMaxTime) of "600"
seconds. Stack trace: ...
```

This error occurs because the WebLogic Server has exceeded its "Stuck Thread Max Time:" default value of 600 seconds.

Workaround. If the Configurator does not respond, restart it. Also, consider setting the WebLogic Server "Stuck Thread Max Time" value from its default 600 seconds to a larger value such as 1200 seconds. Use the WebLogic Console to change this value (*base_domain* > `Environment > Servers > Admin Server > Configuration/Tuning`).

4099: ID-WSF sample with JDK 1.4 WAR returned exception

On WebLogic Server 8.1, `opensso-client-jdk14.war` configured for ID-WSF returned an error when looking for service.

Workaround. Add following JAR files under *weblogic-home*`/jdk142_08/jre/lib/endorsed`:

- `jax-qname.jar`
- `namespace.jar`
- `relaxngDatatype.jar`
- `xalan.jar`

To obtain these JAR files, contact your Sun representative.

4094: Multi-server setup fails when `amadmin` password and directory manager password for configuration data store are not the same

This issue occurs only if the following conditions are met:

- Your configuration data store is Sun Java System Directory Server.
- You are trying to perform a multi-server installation.
- Your `amadmin` password is different from the Directory Server bind `dn` password.

Workaround. There are two parts to this workaround:

1. Make sure your configuration Directory Server bind `dn` password is same as the `amadmin` password.
2. Configure the second and additional OpenSSO Enterprise servers. To perform the second server installation and point to the first OpenSSO Enterprise server's configuration directory, simply access the Configurator page of the second OpenSSO Enterprise server and enter the `amadmin` password, cookie domain, and other details for Step 1 and Step 2.

   For Step 3, do not select the Add to Existing Deployment. Instead, select the first instance option and provide the same Directory Server name, port, DN, password, and encryption key of your first server. Then, proceed with the configuration as usual.

4055: Error occurred after adding an advanced property in console

Adding an advanced property in the Console caused OpenSSO Enterprise server to return an error. This problem can occur after adding any advanced configuration property.

Workaround. If you change the default server configuration in the Console, you must restart the OpenSSO Enterprise server web container.

3858: Out of memory exceptions occur under heavy load with JDK 1.5 and 1.6 SunPKCS11 provider

JDK 1.5 and 1.6 contain a list of PKCS11 providers. The default is `sun.security.pkcs11.SunPKCS11` (see the provider list below). Under a heavy load, this provider will generate an Out of Memory Exception (OOME) for the web container and cause the container to crash. At minimum, the following scenarios are impacted:

- SSL on these web containers: GlassFish Application Server V2 UR2, WebLogic Server 9.2, and JBoss Application Server 4.2.2 (but not on Sun Java System Web Server 7.0, which uses a different JSS implementation for SSL)
- SAML2 signing on Sun Java System Web Server 7 U3

The issue is currently under investigation and might impact other web container platforms not listed above.

Workaround. Remove the `SunPKCS11` provider from the provider list in the `java.security` file for the JVM. For example, if the security provider section in your `java.security` file (found in *JDK_Path*`/jre/lib/security/`) looks like:

```
security.provider.1=sun.security.pkcs11.SunPKCS11 \
   ${java.home}/lib/security/sunpkcs11-solaris.cfg
security.provider.2=sun.security.provider.Sun
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
```

Change it to:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=sun.security.rsa.SunRsaSign
security.provider.3=com.sun.net.ssl.internal.ssl.Provider
security.provider.4=com.sun.crypto.provider.SunJCE
security.provider.5=sun.security.jgss.SunProvider
security.provider.6=com.sun.security.sasl.Provider
```

Note. This workaround can lower your performance because the provider used now is not as optimized as the `SunPKCS11` provider. It also prevents you from using hardware security tokens if the `SunPKCS11` provider is required.

3837: Configuration fails on Oracle Application Server 10g

With Oracle Application Server 10g version 10.1.3.1 as the web container, OpenSSO configuration failed with an exception error.

Workaround. Before you configure OpenSSO, add the following JVM option to the "Server Properties" for the target Oracle Application Server 10g server instance:

```
-Doc4j.jmx.security.proxy.off=true
```

2222: Password reset and account lockout services report notification errors

OpenSSO Enterprise submits email notifications using the unqualified sender name, `Identity-Server`, which returns error entries in the logs.

Workaround. Change the sender name from `Identity-Server` to `Identity-Server@hostname.domainname` in the following files:

- In `amPasswordResetModuleMsgs.properties`, change `fromAddress.label`.
- In `amAuth.properties`, change `lockOutEmailFrom`.

Data Store Issues

4102: TTL for service management configuration is not working

Time to live (TTL) for service management configuration is not working because the TTL property is not being initialized.

4085: OpenSSO Enterprise is unable to store the CRL in the LDAP directory

After getting the certificate revocation list (CRL) from the CRL distribution point extension, OpenSSO Enterprise does not store the CRL in the LDAP directory.

3827: Replication configuration hangs on second GlassFish instance

In this scenario, OpenSSO Enterprise is deployed on two GlassFish (or Application Server 9.1) instances on Windows Vista server. During the configuration of the second OpenSSO Enterprise instance, replication of the configuration using the "Add to Existing Deployment" option hangs.

Workaround. This issue still exists on Windows Vista systems. For Windows systems other than Vista, add the following GlassFish (or Application Server 9.1) JVM option:

```
-Dcom.sun.enterprise.server.ss.ASQuickStartup=false
```

3350, 2867: `LDAP Follows Referral` should be disabled for Active Directory Data Store

An Active Directory data store sometimes hangs the system. This problem can also occur when you are creating a new Active Directory data store.

Workaround. In the OpenSSO Enterprise Admin Console, disable `LDAP Follows Referral` for the Active Directory data store:

1. Click `Access Control`, *top-level-realm*, `Data Stores`, *ActiveDirectory-data-store-name*.
2. Uncheck `Enabled` for the `LDAP Follows Referral`.
3. Save your changes.

Failover does not occur for Access Manager SDK (AMSDK) plug-in

If OpenSSO Enterprise is configured with the AMSDK plug-in and the directory server is set up for MMR, failover does not occur if a directory server instance goes down.

Authentication Issues

4103: Windows Desktop SSO authentication module returns "No Configuration Found" error

If you configure a Windows Desktop SSO authentication module to perform a Kerberos authentication from Internet Explorer 6.0 on Windows Server 2003, the "No configuration found" error is returned.

4100: Certificate authentication with CRL checking fails

If you configure Certificate authentication and enable "Match Certificate to CRL" the authentication fails. See also the related issue "4085: OpenSSO Enterprise is unable to store the CRL in the LDAP directory" on page 34.

4054: `amadmin` authentication fails with URL `org` parameter

If the OpenSSO Enterprise Admin (`amadmin`) creates a new realm (such as `myorg`) and later tries to log in to the new realm as follows:

```
http://host:port/opensso/UI/Login?org=myorg
```

OpenSSO Enteprise returns an `Authentication Failed` error.

Workaround. As `amadmin`, you can log in only to the root realm (and only to Data Store or Application modules).

1781: `amadmin` login fails for non Data Store authentication

If you change the authentication module for the root realm to anything besides `DataStore`, `amadmin` will not be able to log into the Console.

Workaround. Log in using `http://host.domain/deployurl/UI/Login?module=DataStore`.

Policy Issues

3952: Server samples are missing the policy samples link

The `index.html` under *host*:*port*/*uri*/`samples` displays:

```
1. Authentication Samples
2. ID-FF Sample
3. SAMLv2 Sample
4. Multi-Federation Protocols Sample
```

However, the following link to the policy samples is missing in `index.html`:
host:*port*/*uri*/`samples/policy/policy-plugins.html`

Workaround: Open the *host*:*port*/*uri*/`samples/policy/policy-plugins.html` file in your browser.

3949: OCSP checking needs permission added to `server.policy` file

To enable OCSP checking for an OpenSSO web container that has enabled the Java Security Manager, add the following permission to the `server.policy` (or equivalent) file:

```
permission java.security.SecurityPermission "getProperty.ocsp.*";
```

3796: Creation of Fedlet in console failed in a console only deployment

If you generate a console only deployment, creating a Fedlet using the Console Common Tasks failed with an error message stating that there was no file or directory for `sp-extended.xml`. The `com.iplanet.services.configpath` property was not set by the console only Configurator.

Workaround. Edit the `AMConfig.properties` file and set the `com.iplanet.services.configpath` property to the configuration directory. For example:

```
com.iplanet.services.configpath=/consoleonly
```

2381: Access Manager Roles policy subject is supported only with Access Manager repository data store

The Access Manager Roles policy subject is supported only with the Access Manager Repository (AMSDK) data store. By default, this subject is disabled in the policy configuration. Therefore, enable the Access Manager Roles policy subject only if the data store type is configured to use the AMSDK plug-in.

For more information, see Chapter 15, "Enabling the Access Manager SDK (AMSDK) Identity Repository Plug-in," in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

Session Issues

3910: `setup.bat` of `ssoSessionTools.zip` fails to install tools

After you unzip `ssoSessionTools.zip`, running the `setup.bat` script fails to install the session scripts and returns the following error:

```
Unable to locate JRE meeting specification "1.4+"
```

Workaround. In the `setup.bat` script, remove `-version:"1.4+"` from the `java.exe` command and rerun the script.

2827: Configuring a site does not add the second server to the site

Session failover configuration does not add the second OpenSSO Enterprise instance to the assigned servers list.

Workaround. Use the OpenSSO Enterprise Console or `ssoadm` utility to manually add the second server instance to the servers list.

Command-Line Utilities Issues

4079: `ssoadm import-svc-cfg` command fails when using Directory Server as the configuration data store

Sometimes the `import-svc-cfg` subcommand fails because OpenSSO Enterprise cannot delete nodes in the Service Manager data store. The following scenarios can cause this problem:

1. Configure OpenSSO Enterprise using a remote Sun Java System Directory Server as the configuration data store.
2. Export the service XML file by using the `ssoadm export-svc-cfg` command.
3. Re-import the service XML data obtained in Step 2 using the `ssoadm import-svc-cfg` command.
4. When you are asked to delete the existing data, choose yes.

   The following error message is returned: `Unexpected LDAP exception occurred`.

Workaround. Re-execute the `ssoadm import-svc-cfg` command until it succeeds.

3955: Unable to execute the `ssoadm` command

You are unable to execute the `ssoadm` command with the `get-realm` due to this exception.

```
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader" failed
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
       com.iplanet.am.service.password
Logging configuration class "com.sun.identity.log.s1is.LogConfigReader" failed
com.sun.identity.security.AMSecurityPropertiesException: AdminTokenAction:
FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
```

```
       com.iplanet.am.service.password
AdminTokenAction:  FATAL ERROR: Cannot obtain Application SSO token.
Check AMConfig.properties for the following properties
       com.sun.identity.agents.app.username
       com.iplanet.am.service.password
```

Check if the `amadmin` password is different from the directory manager password for the service management data store. If yes, apply the following workaround.

Workaround. Modify the server configuration XML as follows:

1. Log in to the OpenSSO Console as `amadmin`.
2. Use the `ssoadm.jsp` `get-svrcfg-xml` to get the server configuration XML.
3. Use `encode.jsp` to encode the `amadmin` password.
4. Set the encoded password in the two places represented by *amadmin-password* in the XML. For example:

```
<User name="User1" type="proxy">
            <DirDN>
                cn=puser,ou=DSAME Users,dc=opensso,dc=java,dc=net
            </DirDN>
            <DirPassword>
               amadmin-password
            </DirPassword>
        </User>
        <User name="User2" type="admin">
            <DirDN>
                cn=dsameuser,ou=DSAME Users,dc=opensso,dc=java,dc=net
            </DirDN>
            <DirPassword>
               amadmin-password
            </DirPassword>
        </User>
        <BaseDN>
            dc=opensso,dc=java,dc=net
        </BaseDN>
    </ServerGroup>
```

5. Use the `ssoadm.jsp` `set-svrcfg-xml` to set the altered server configuration XML.

2905: `jss4.jar` entry is missing in the `ssoadm` `classpath`

After running the `setup` script for the `ssoadm` utility, trying to run `ssoadm` returns a `NoClassDefFoundError` error. This problem occurs for an upgraded OpenSSO Enterprise instance.

Workaround. To use JSS, add `jss4.jar` to the `classpath` and set the `LD_LIBRARY_PATH` environment variable. (If you are using the default JCE, `jss4.jar` is not required to be in the `classpath`.)

Client SDK Issues

4081: SMS cache is disabled by default on the Client SDK

For a Client SDK installation, the service management service (SMS) cache is disabled by default.

Workaround: For Web Services Security (WSS) applications, set `com.sun.identity.sm.cache.enabled=false` in the `AMConfig.properties` file; otherwise the fix for issue 3171 will not work.

For all other Client SDK applications, set `com.sun.identity.sm.cache.enabled=true` in the `AMConfig.properties` file to enable SMS caching, which can prevent performance problems.

4080: Client SDK Configurator puts the wrong shared secret in the `AMConfig.properties` file

The Client SDK WAR file Configurator puts the wrong shared secret in the `AMConfig.properties` file.

Workaround. Copy the shared secret value and the password encryption key from the OpenSSO Enterprise server to the Client SDK`AMConfig.properties` file under the *$HOME*`/OpenSSOClient` directory.

Federation and SAML Issues

3923: Creating an entity (IDP or SP) in Console Common Tasks page fails on Oracle Application Server

With OpenSSO Enterprise deployed on Oracle Application Server, creating an entity (IDP or SP) in the Console Common Tasks page causes an exception.

Workaround. When `opensso.war` is deployed on Oracle Application Server, disable the import option for the `oracle.xml` file in the deployment plan view (`Deploy: Deployment Settings > Configure Class Loading > oracle.xml`).

3065: Same context ID is used for all users in ID-FF log records

All ID-FF log records have same the context (or login) ID, even if they are for different users.

2661: `logout.jsp` did not compile on WebSphere Application Server 6.1

The `logout.jsp` file requires JDK 1.5, but the JDK source level for JSP files is set to JDK 1.3 on IBM WebSphere Application Server 6.1.

Workaround. See the workaround for "1977: SAMLv2 sample `configure.jsp` files fail on WebSphere Application Server 6.1" on page 41.

1977: SAMLv2 sample `configure.jsp` files fail on WebSphere Application Server 6.1

On a WebSphere Application Server 6.1 instance, the `/sample/saml2/sp/configure.jsp` and `/sample/saml2/idp/configure.jsp` files fail to compile. The `configure.jsp` files require JDK 1.5, but the JDK source level for JSP files is set to JDK 1.3 on WebSphere Application Server 6.1.

Workaround: Edit the JSP engine configuration parameters to set the JDK source level to 1.5:

1. Open the `WEB-INF/ibm-web-ext.xmi` file.

   JSP engine configuration parameters are stored either in a web module's configuration directory or in a web module's binaries directory in the `WEB-INF/ibm-web-ext.xmi` file:

   Configuration directory. For example:

   `{WAS_ROOT}/profiles/`*profilename*`/config/cells/`*cellname*`/applications/`*enterpriseappname*`/deployments/`*deployedname*`/webmodulename/`

   Binaries directory, if an application was deployed into WebSphere Application Server with the flag "Use Binary Configuration" flag set to `true`. For example:

   `{WAS_ROOT}/profiles/`*profilename*`/installedApps/`*nodename*`/`*enterpriseappname*`/webmodulename/`
2. Delete the `compileWithAssert` parameter by either deleting the statement from the file or enclosing the statement with comment tags (`<!–` and `–>`).
3. Add the `jdkSourceLevel` parameter with the value of 15. For example:

   ```
   <jspAttributes xmi:id="JSPAttribute_1" name="jdkSourceLevel" value="15"/>
   ```

   Note: The integer (`_1`) in `JSPAttribute_1` must be unique within the file.
4. Save the `ibm-web-ext.xmi` file.
5. Restart the application.

For more information about the `jdkSourceLevel` parameter as well as other JSP engine configuration parameters, see:

```
http://publib.boulder.ibm.com/
infocenter/wasinfo/v6r1/topic/com.ibm.websphere.nd.doc/info/ae/ae/
rweb_jspengine.html
```

Web Services Security (WSS) Issues

4057: Dynamic web service provider configuration with endpoint does not take effect

If you set up the proxy use case based on the loan sample for Web Services Security (WSS) and create two web service providers (WSP) with profile names other than `wsp`, an error occurs.

Workaround. For JAX-WS/web application based web services, use the static point end as the WSP name to support multiple web services. For EJB based web services, use the default WSP configuration.

Access Manager SDK (AMSDK) Issues

4139: With OpenSSO configured with AMSDK plug-in, session service assigned to a new role has conflict resolution level attribute issue

With OpenSSO Enterprise configured with the Access Manager SDK (AMSDK) plug-in, the session service assigned to a new role has a conflict resolution level attribute issue. Changing the conflict resolution level doesn't take effect on a user assigned with the role.

Workaround: Replace the `cospriority` attribute using a utility such as `ldapmodify`. For example:

```
ldapmodify -p 50389 -h dshost -D"cn=directory manager" -w dmpassword -c -f /tmp/mod
```

where `/tmp/mod` is:

```
dn:cn="cn=sfo1,dc=opensso,dc=java,dc=net",
cn=iPlanetAMSessionService,dc=opensso,dc=java,dc=net
changetype:modify
replace:cospriority
cospriority:4
```

Upgrade, Compatibility, and Coexistence Issues

5801: During upgrade, `updateschema.sh` fails while executing `ssoadm` in a site configuration

If you are upgrading from OpenSSO Enterprise 8.0 to an OpenSSO 8.0 Update 1 patch release and OpenSSO Enterprise 8.0 has been configured as a site with a load balancer, the `updateschema.sh` script fails while executing the `ssoadm` utility.

Workaround. Before you run the `updateschema.sh` or `updateschema.bat` script:

1. Install the `ssoadm` utility from the OpenSSO Enterprise Update 1 patch release.
2. After you install the `ssoadm` utility, edit the `ssoadm` or `ssoadm.bat` utility by adding the following property to the `java` command:

   ```
   -D"com.iplanet.am.naming.map.site.to.server=
   http://loadbalancer.example.com:8080/opensso=http://sso1.example.com:8080/opensso"
   ```

   where `loadbalancer` is the load balancer for the OpenSSO Enterprise site, and `sso1` is the OpenSSO Enterprise server where `ssoadm` or `ssoadm.bat` is installed.

For more information, see Chapter 3, "Installing the OpenSSO Enterprise 8.0 Update 1 Admin Tools," in *Sun OpenSSO Enterprise 8.0 Update 1 Release Notes*.

4108: Incorrect encryption key used after configuring OpenSSO Enterprise against existing schema (DIT)

After configuring OpenSSO Enterprise against an existing schema (DIT) , you cannot log in to the console, because the encryption key entered during the configuration (the one from the old Access Manager or Federation Manager instance) is not used. Instead, a new incorrect encryption key is generated, which creates an incorrect `serverconfig.xml` file.

Workaround.

1. Change to OpenSSO Enterprise config directory.
2. Change the encryption key in the `AMConfig.properties` file with the correct value.
3. Copy the backup copy of `serverconfig.xml` from the previous Access Manager or Federation Manager instance.

4. Restart OpenSSO Enterprise server.

3962: Incorrect Console URL returned after authentication for non-admin user

If OpenSSO is configured with an Access Manager 7.1 Directory Server schema (DIT) in coexistence mode and a non-admin user logs in to the OpenSSO Console, the user is taken to an invalid URL. For example:

```
http://ssohost.example.com:8080/amserver/..amserver/base/AMAdminFrame.
```

Workaround. Edit the URL as follows:

protocol`://`*host*`.`*domain*`:`*port*`/`*deploy_uri*`/idm/EndUser`

For example:

```
http://ssohost.example.com:8080/amserver/idm/EndUser
```

3961: `amadmin` cannot log in to OpenSSO Console in coexistence mode

If OpenSSO is configured with an Access Manager 7.1 Directory Server schema (DIT) in coexistence mode, an attempt to log in as `amadmin` to the Console using LDAP authentication fails.

Workaround. To log in as `amadmin` to the OpenSSO Console in coexistence mode, add the `module=DataStore` query parameter. For example:

protocol`://`*host*`.`*domain*`:`*port*`/`*deploy_uri*`/UI/Login/?module=DataStore`

For example:

```
http://ssohost.example.com:8080/amserver/UI/Login/?module=DataStore
```

2348: Document Distributed Authentication UI server support

The OpenSSO Enterprise Distributed Authentication UI server component works only with OpenSSO Enterprise. The following scenarios are not supported:

- Distributed Authentication UI server 7.0 or 7.1 with a OpenSSO Enterprise server
- OpenSSO Enterprise Distributed Authentication UI server with an Access Manager 7.0 or 7.1 server

830: ID-FF schema metadata is not backward compatible

If you are upgrading from a previous release of Access Manager or Federation Manager to OpenSSO Enterprise 8.0, ID-FF profiles do not work unless you also upgrade the Access Manager or Federation Manager schema.

Workaround. Before you try the ID-FF profiles, upgrade the Access Manager or Federation Manager schema. For more information about upgrading the schema, see the *Sun OpenSSO Enterprise 8.0 Upgrade Guide*.

Policy Agents Issues

3581: Policy evaluation with DNS condition fails for version 3.0 policy agents

For the version 3.0 policy agent for Sun Java System Application Server or GlassFish Application Server, policy evaluation with a DNS condition fails, because by default, the `ServletRequest.getRemoteHost` method returns an IP address instead of a host name.

Workaround. Change the default behavior by setting the following property in the Application Server or GlassFish `domain.xml` file:

```
dns-lookup-enabled="true"
```

Or, if you prefer, set this property in the Application Server or GlassFish Admin console.

Internationalization Issues

4090: Non-English entitlements are garbled

Workaround: To view the localized entitlements, which are provided in `.txt` format, use a browser with the encoding specified for each locale in the browser as follows:

- French (fr): ISO–8859-1
- Spanish (es): ISO–8859-1

- German (de): ISO–8859-1
- Simplified Chinese (zh_CN): UTF-8
- Traditional Chinese (zh_TW): UTF-8
- Korean (ko): UTF-8
- Japanese (ja): EUC-JP

4051: Multi-byte trusted partner name is garbled in Console

In the OpenSSO Console, if you go to Federation > SAML1.x Configuration, and then create a new Trusted Partner with a multi-byte Name in the Common Settings section, the trusted partner name is garbled.

3993: End user page shows question marks for CCK and JA locales

On the Geronimo web container in CCK and JA locales, if you log in as a user other than `amadmin`, the Access Control, *realm*, General, EndUser page (`http://`*host*`:`*port*`/`*deployuri*`/idm/EndUser`) shows question marks.

3976: Online Help "Tips on Searching" shows 404 error in non-English locale

If you log in to the OpenSSO Console in a non-English locale such as French, click Help, and then "Tips on Searching", the right Help panel shows a 404 error.

Workaround. To view "Tips on Searching" in English, set the browser language to English and then refresh the online Help window

3766: `encode.jsp` and `ampassword -e` differ with multi-byte (non-ASCII) characters

If a password file contain multi-byte (non-ASCII) characters, the `ampassword` utility does not return the correct encrypted value. However, `encode.jsp` does return the correct value.

Workaround. If you are using `ampassword`, use a password file that contain only ASCII characters. If the password contains multi-byte characters, use `encode.jsp` to encrypt the password:

1. Log in to the OpenSSO Admin Console as `amadmin`.
2. Specify the following URL: `http://host.example.com:58080/`*deploy-uri*`/encode.jsp`
3. When you are prompted, enter the password and click Encode.
4. Copy the encrypted password.

3763: Some non-ASCII characters are garbled when the web container is in C locale

If you start the web container in the C locale and set your browser to a language such as French, after you log in to the Admin Console, some characters are garbled.

3713: Password reset page is not localized for CCJK locales

For CCJK locales, the password reset page (`http://`*host*`:`*port*`/`*deployuri*`/password`) is not localized.

3590: Change location for `dounix_msgs.po` files

The `dounix_msgs.po` files for the Unix authentication module have not been translated because the Unix authentication module will not be included in a future OpenSSO Enterprise release. See "Deprecation Notifications and Announcements" on page 49.

1793: Authentication fails with multi-byte character for org or module in query parameter

If you try to log in to the OpenSSO Console using the `org` or `module` parameter with characters that are not UTF-8, the login fails. For example:
`http://`*host*`:`*port*`/`*deployuri*`/UI/Login?module=`*Japanese-string*`&gx_charset=UTF-8`

Workaround. Use UTF-8 URLencoding characters such as `%E3%81%A6` instead of native characters.

Localization Issues

4017: In Spanish locale, "2.2 Agents" is translated only as Agentes in Console

If the OpenSSO Console is in the Spanish locale, the 2.2 is missing from the translation of "2.2 Agents".

3994: In Spanish locale, cannot access Certificate for Configuration > Authentication

If the OpenSSO Console is in the Spanish locale, clicking Configuration, Authentication, and then Certificate returns an error.

3971: In Chinese (zh_CN) locale, online help is in English

In the Chinese (zh_CN) locale. the Console online help text is displayed in English rather than Chinese. If you set your browser preferred language to zh_CN, only the online help text in the left tree will be English. If you set your browser preferred language to zh, all online help text will be English.

Workaround. Copy the zh_CN online Help contents to a new zh directory in the web container's webapps directory and the restart the web container.

For example for Apache Tomcat, copy /Tomcat6.0.18/webapps/opensso/html/zh_CN/* to a new directory named /Tomcat6.0.18/webapps/opensso/html/zh/. And then restart the Tomcat container.

3802: Problems in the French part of copyright notice

In the French part of the English copyright notice, “Etats-unis” is missing an accent, a space is missing after the comma at “armes nucléaires,des missiles”, and spaces should not be in “Etats - Unis”.

Upgrading to OpenSSO Enterprise 8.0

Upgrading to OpenSSO Enterprise 8.0 is supported from the following releases:

Previous Release, Including Configuration Data in Sun Java System Directory Server	Upgrade Supported From This Platform
Sun Java System Access Manager 7.1 server Both Java Enterprise System installer and WAR file deployments	Solaris SPARC, Solaris x86, Linux, and Windows systems
Sun Java System Access Manager 7 2005Q4 server	Solaris SPARC, Solaris x86, and Linux systems
Sun Java System Federation Manager 7.0 server	Solaris SPARC, Solaris x86, Linux, and Windows systems

The upgrade process includes upgrading an existing Access Manager or Federation Manager server instance and the corresponding configuration data stored in Sun Java System Directory Server.

Realm Name Change: If you are upgrading to OpenSSO Enterprise 8.0, the syntax for specifying the realm name is changed from Access Manager 7.0 and 7.1. For example, if the realm name in Access Manager is specified as realm=users, after the upgrade to OpenSSO Enterprise 8.0, you must change the name to realm=/users. This name change affects all services trying to authenticate against realms; therefore, you should consider this configuration change during your upgrade planning.

For the detailed upgrade steps, see the *Sun OpenSSO Enterprise 8.0 Upgrade Guide*.

See also "Upgrade, Compatibility, and Coexistence Issues" on page 43.

Deprecation Notifications and Announcements

- The Service Management Service (SMS) APIs (`com.sun.identity.sm` package) and SMS model will not be included in a future OpenSSO Enterprise release.
- The Unix authentication module and the Unix authentication helper (`amunixd`) will not be included in a future OpenSSO Enterprise 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 a future OpenSSO Enterprise release. Migration options are not available now and are not expected to be available in the future. Oracle Identity Manager provides user provisioning solutions that you can use instead of the AMSDK. For more information about Oracle Identity Manager, see the following site:

  I`http://www.oracle.com/us/products/middleware/identity-management/oracle-identity-manager/index.html`

How to Report Problems and Provide Feedback

If you have questions or issues with OpenSSO Enterprise, contact Sun Support Resources (SunSolve) at `http://sunsolve.sun.com/`.

This site has links to the Knowledge Base, Online Support Center, and Product Tracker, as well as to maintenance programs and support contact numbers.

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 OpenSSO Enterprise version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. Go to `http://docs.sun.com/` and click `Feedback`.

Provide the full document title and part number in the appropriate fields. The part number is a seven-digit or nine-digit number that can be found on the title page of the book or at the top of the document. For example, the title is *Sun OpenSSO Enterprise Release Notes* and the part number is 820-3745.

Additional Resources

You can find additional useful information and resources at the following locations:

- Oracle Services: `http://www.oracle.com/us/support/systems/advanced-customer-services/index.html`
- Oracle Software Products: `http://www.oracle.com/us/sun/sun-products-map-075562.html`
- Support Resources `http://sunsolve.sun.com/`
- Oracle Technology Network: `http://www.oracle.com/technetwork/index.html`

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Oracle upon request to determine which versions are best suited for deploying accessible solutions.

For information about Oracle's commitment to accessibility, see `http://www.oracle.com/accessibility/index.html`.

Related Third-Party Web Sites

Third-party URLs are referenced in this document and provide additional, related information.

Note – Oracle is not responsible for the availability of third-party Web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Oracle will not be responsible or liable for any actual or alleged damage or loss caused by or in connection with the use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Revision History

TABLE 19 Revision History

Date (Revision)	Description of Changes
August 18, 2010 (20)	■ Added the "Java EE Agents in the Policy Agent 3.0-01 Release" on page 10 section. ■ Added the "Oracle OpenSSO 8.0 Update 2" on page 7 section. ■ Revised outdated URLs.
July 14, 2010 (19)	■ Added the new "Policy Agent 3.0-01 Release" on page 10 section. ■ Added "CR 6935896: Undeploying OpenSSO Enterprise on Sun GlassFish 2.1 using the CLI is unsuccessful" on page 30. ■ Revised outdated URLs.
February 18, 2010 (18)	Changed BEA to Oracle for the WebLogic Server web containers in the "Web Containers Supported For OpenSSO Enterprise 8.0" on page 23 section.
January 4, 2010 (17)	■ Updated "Platforms Supported For OpenSSO Enterprise 8.0" on page 22 for CR 6894607. ■ Added information for issues 5801, 5647, 5651, and 5091. ■ Removed references to upgrading Access Manager 6.3 because an upgrade from this version is not supported.
June 18, 2009 (16)	Added the "Patches to Update 1" on page 7 section.
May 15, 2009 (15)	Added the "OpenSSO Enterprise 8.0 Update 1" on page 7 section.
April 17, 2009 (14)	Updated "Web Browsers Supported For OpenSSO Enterprise 8.0" on page 28 for Mac OS X 10.4.
April 10, 2009 (13)	■ In "Data Store Requirements For OpenSSO Enterprise 8.0" on page 25, added a note stating that the OpenSSO configuration data store is not supported on an NFS-mounted file system. ■ In "Hardware and Software Requirements For OpenSSO Enterprise 8.0" on page 22, added the "Database Logging Requirements For OpenSSO Enterprise 8.0" on page 27 section and updated the versions of Sun Java System Directory Server supported for the user data store.
November 20, 2008 (12)	For "OpenSSO Enterprise 8.0 Issues" on page 29: ■ Added issues 3581, 3858, and 4139. ■ Updated workaround for issue 4099.
November 14, 2008 (11)	Added late changes including new issues and changes to "Hardware and Software Requirements For OpenSSO Enterprise 8.0" on page 22.

TABLE 19 Revision History *(Continued)*

Date (Revision)	Description of Changes
November 11, 2008 (10)	Initial release.
August 26, 2008 (05)	Early Access (EA) release draft.