

Sun OpenSSO Enterprise 8.0 Release Notes



Part No: 820-3745-18
February 18, 2010

Sun Microsystems, Inc. has intellectual property rights relating to technology embodied in the product that is described in this document. In particular, and without limitation, these intellectual property rights may include one or more U.S. patents or pending patent applications in the U.S. and in other countries.

U.S. Government Rights – Commercial software. Government users are subject to the Sun Microsystems, Inc. standard license agreement and applicable provisions of the FAR and its supplements.

This distribution may include materials developed by third parties.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California. UNIX is a registered trademark in the U.S. and other countries, exclusively licensed through X/Open Company, Ltd.

Sun, Sun Microsystems, the Sun logo, the Solaris logo, the Java Coffee Cup logo, docs.sun.com, Java, and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

Products covered by and information contained in this publication are controlled by U.S. Export Control laws and may be subject to the export or import laws in other countries. Nuclear, missile, chemical or biological weapons or nuclear maritime end uses or end users, whether direct or indirect, are strictly prohibited. Export or reexport to countries subject to U.S. embargo or to entities identified on U.S. export exclusion lists, including, but not limited to, the denied persons and specially designated nationals lists is strictly prohibited.

DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Sun Microsystems, Inc. détient les droits de propriété intellectuelle relatifs à la technologie incorporée dans le produit qui est décrit dans ce document. En particulier, et ce sans limitation, ces droits de propriété intellectuelle peuvent inclure un ou plusieurs brevets américains ou des applications de brevet en attente aux Etats-Unis et dans d'autres pays.

Cette distribution peut comprendre des composants développés par des tierces personnes.

Certains composants de ce produit peuvent être dérivés du logiciel Berkeley BSD, licenciés par l'Université de Californie. UNIX est une marque déposée aux Etats-Unis et dans d'autres pays; elle est licenciée exclusivement par X/Open Company, Ltd.

Sun, Sun Microsystems, le logo Sun, le logo Solaris, le logo Java Coffee Cup, docs.sun.com, Java et Solaris sont des marques de fabrique ou des marques déposées de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pays. Toutes les marques SPARC sont utilisées sous licence et sont des marques de fabrique ou des marques déposées de SPARC International, Inc. aux Etats-Unis et dans d'autres pays. Les produits portant les marques SPARC sont basés sur une architecture développée par Sun Microsystems, Inc.

L'interface d'utilisation graphique OPEN LOOK et Sun a été développée par Sun Microsystems, Inc. pour ses utilisateurs et licenciés. Sun reconnaît les efforts de pionniers de Xerox pour la recherche et le développement du concept des interfaces d'utilisation visuelle ou graphique pour l'industrie de l'informatique. Sun détient une licence non exclusive de Xerox sur l'interface d'utilisation graphique Xerox, cette licence couvrant également les licenciés de Sun qui mettent en place l'interface d'utilisation graphique OPEN LOOK et qui, en outre, se conforment aux licences écrites de Sun.

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la législation américaine en matière de contrôle des exportations et peuvent être soumis au droit d'autres pays dans le domaine des exportations et importations. Les utilisations finales, ou utilisateurs finaux, pour des armes nucléaires, des missiles, des armes chimiques ou biologiques ou pour le nucléaire maritime, directement ou indirectement, sont strictement interdites. Les exportations ou réexportations vers des pays sous embargo des Etats-Unis, ou vers des entités figurant sur les listes d'exclusion d'exportation américaines, y compris, mais de manière non exclusive, la liste de personnes qui font objet d'un ordre de ne pas participer, d'une façon directe ou indirecte, aux exportations des produits ou des services qui sont régis par la législation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement désignés, sont rigoureusement interdites.

LA DOCUMENTATION EST FOURNIE "EN L'ETAT" ET TOUTES AUTRES CONDITIONS, DECLARATIONS ET GARANTIES EXPRESSES OU TACITES SONT FORMELLEMENT EXCLUES, DANS LA MESURE AUTORISEE PAR LA LOI APPLICABLE, Y COMPRIS NOTAMMENT TOUTE GARANTIE IMPLICITE RELATIVE A LA QUALITE MARCHANDE, A L'APTITUDE A UNE UTILISATION PARTICULIERE OU A L'ABSENCE DE CONTREFACON.

Contents

Sun OpenSSO Enterprise 8.0 Release Notes	5
Getting Started With OpenSSO Enterprise 8.0	6
OpenSSO Enterprise 8.0 Documentation	6
OpenSSO Enterprise 8.0 Update 1	7
Patches to Update 1	7
What's New in OpenSSO Enterprise 8.0	7
Using Service Tags With Sun Inventory	10
Hardware and Software Requirements For OpenSSO Enterprise 8.0	11
Platforms Supported For OpenSSO Enterprise 8.0	11
Web Containers Supported For OpenSSO Enterprise 8.0	12
JDK Requirements For OpenSSO Enterprise 8.0	14
Data Store Requirements For OpenSSO Enterprise 8.0	14
Session Failover Requirements for OpenSSO Enterprise 8.0	15
Policy Agents Supported for OpenSSO Enterprise 8.0	16
Database Logging Requirements For OpenSSO Enterprise 8.0	16
Hardware Requirements For OpenSSO Enterprise 8.0	16
Web Browsers Supported For OpenSSO Enterprise 8.0	17
OpenSSO Enterprise 8.0 Issues	18
Web Container and Server Issues	18
Data Store Issues	23
Authentication Issues	24
Policy Issues	25
Session Issues	26
Command-Line Utilities Issues	26
Client SDK Issues	28
Federation and SAML Issues	29
Web Services Security (WSS) Issues	30
Access Manager SDK (AMSDK) Issues	31

Upgrade, Compatibility, and Coexistence Issues	31
Policy Agents Issues	33
Internationalization Issues	34
Localization Issues	36
Upgrading to OpenSSO Enterprise 8.0	37
Deprecation Notifications and Announcements	38
How to Report Problems and Provide Feedback	38
Sun Welcomes Your Comments	38
Additional Sun Resources	39
Accessibility Features for People With Disabilities	39
Related Third-Party Web Sites	39
Revision History	39

Sun OpenSSO Enterprise 8.0 Release Notes

Last revised February 18, 2010

Sun™ OpenSSO Enterprise 8.0 is part of the OpenSSO project (<http://opensso.org/>) and is the Sun commercial version of OpenSSO server.

These Release Notes also apply to Sun OpenSSO Express. OpenSSO Enterprise and OpenSSO Express have these differences:

- OpenSSO Enterprise will be released approximately every 12 months, will receive extensive automated and manual testing by Sun QA Engineering, and will have periodic patches and hot fixes.
- OpenSSO Express will be released approximately every three months, will receive extensive automated testing and moderate manual testing by Sun QA Engineering, but will **not** have patches and hot fixes. For more information, see the OpenSSO Express FAQs: <https://opensso.dev.java.net/public/about/faqcenter/SupportFAQ.html>.

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 19.

Contents

- “Getting Started With OpenSSO Enterprise 8.0” on page 6
- “OpenSSO Enterprise 8.0 Update 1” on page 7
- “What’s New in OpenSSO Enterprise 8.0” on page 7
- “Using Service Tags With Sun Inventory” on page 10
- “Hardware and Software Requirements For OpenSSO Enterprise 8.0” on page 11
- “OpenSSO Enterprise 8.0 Issues” on page 18
- “Upgrading to OpenSSO Enterprise 8.0” on page 37
- “Deprecation Notifications and Announcements” on page 38
- “How to Report Problems and Provide Feedback” on page 38

- “Additional Sun Resources” on page 39
- “Revision History” on page 39

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 12.
2. Download and unzip the `opensso_enterprise_80.zip` file from one of the following sites:
 - OpenSSO project: <https://opensso.dev.java.net/public/use/index.html>
 - Sun: http://www.sun.com/software/products/opensso_enterprise
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 33.

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, go to View by Category, Identity Management, and Policy Agents on the Sun Downloads site: <http://www.sun.com/download/>.

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.

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 OpenSSO Enterprise 8.0 Update 1 Release Notes at <http://wikis.sun.com/x/SAP7BQ>.

Patches to Update 1

Sun 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, “Installing OpenSSO Enterprise 8.0 Update 1” at <http://wikis.sun.com/x/RgQCBg>.

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 12](#).
- 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 12.](#)
- 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 10.](#)
- 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 and Express 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

Using Service Tags With Sun Inventory

OpenSSO 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. You can register OpenSSO Enterprise, OpenSSO Express, or even a nightly build.

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.

- [“Platforms Supported For OpenSSO Enterprise 8.0” on page 11](#)
- [“Web Containers Supported For OpenSSO Enterprise 8.0” on page 12](#)
- [“JDK Requirements For OpenSSO Enterprise 8.0” on page 14](#)
- [“Data Store Requirements For OpenSSO Enterprise 8.0” on page 14](#)
- [“Session Failover Requirements for OpenSSO Enterprise 8.0” on page 15](#)
- [“Policy Agents Supported for OpenSSO Enterprise 8.0” on page 16](#)
- [“Database Logging Requirements For OpenSSO Enterprise 8.0” on page 16](#)
- [“Hardware Requirements For OpenSSO Enterprise 8.0” on page 16](#)
- [“Web Browsers Supported For OpenSSO Enterprise 8.0” on page 17](#)



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 1 Platforms Supported For OpenSSO Enterprise 8.0

Platform	Supported Web Containers
Solaris 10 OS on SPARC, x86, and x64 based systems	All “Web Containers Supported For OpenSSO Enterprise 8.0” on page 12 except for Geronimo Application Server 2.1.1 with Tomcat only
Solaris 9 OS on SPARC, x86, and x64 based systems	
OpenSolaris	GlassFish Application Server V2 UR1 and UR2
	Apache Tomcat 6.0.18

TABLE 1 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	All “Web Containers Supported For OpenSSO Enterprise 8.0” on page 12 except Geronimo
Red Hat Enterprise Linux 4 server Base and Advanced Platform on Intel 32-bit (x86) servers and AMD 64-bit (x86_64) servers	
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 12 except Geronimo
Windows Server 2003 R2 on 64-bit servers	All “Web Containers Supported For OpenSSO Enterprise 8.0” on page 12
Windows XP Windows Vista	All “Web Containers Supported For OpenSSO Enterprise 8.0” on page 12 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 2 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.sun.com/download/index.jsp

TABLE 2 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.sun.com/download/index.jsp 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/technology/products/database/oracle10g Version 10.1.3.1 is supported.
IBM WebSphere Application Server 6.1	See http://www-01.ibm.com/software/webervers/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 3 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 4 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 4 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 5 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 6 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 <code>AMAgent.properties</code> 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 7 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 <code>STR_TO_DATE</code> 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 8 Hardware Requirements For OpenSSO Enterprise 8.0

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

TABLE 8 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 (<code>com.ipplanet.services.debug.level</code>) is set to <code>message</code> 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 <code>message</code>. ■ Check the <code>.access</code> and <code>.error</code> logs periodically in the <code>logs</code> 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 9 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 9 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

- “Web Container and Server Issues” on page 18
- “Data Store Issues” on page 23
- “Authentication Issues” on page 24
- “Policy Issues” on page 25
- “Session Issues” on page 26
- “Command-Line Utilities Issues” on page 26
- “Client SDK Issues” on page 28
- “Federation and SAML Issues” on page 29
- “Web Services Security (WSS) Issues” on page 30
- “Access Manager SDK (AMSDK) Issues” on page 31
- “Upgrade, Compatibility, and Coexistence Issues” on page 31
- “Policy Agents Issues” on page 33
- “Internationalization Issues” on page 34
- “Localization Issues” on page 36

For more information about OpenSSO Enterprise issues, see:

<https://opensso.dev.java.net/servlets/ProjectIssues>

Web Container and Server Issues

- “4077: OpenSSO Enterprise configuration on WebLogic Server requires new `ldapjdk.jar`” on page 19
- “WebLogic Server `StuckThreadMaxTime` value is exceeded during configuration” on page 20
- “4099: ID-WSF sample with JDK 1.4 WAR returned exception” on page 20
- “4094: Multi-server setup fails when `amadmin` password and directory manager password for configuration data store are not the same” on page 21
- “4055: Error occurred after adding an advanced property in console” on page 21
- “3858: Out of memory exceptions occur under heavy load with JDK 1.5 and 1.6 SunPKCS11 provider” on page 21
- “3837: Configuration fails on Oracle Application Server 10g” on page 22
- “2222: Password reset and account lockout services report notification errors” on page 23

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] ExecuteThread: '5' for queue: 'weblogic.kernel.Default (self-tuning)' has been busy for "681" seconds working on the request "Http Request: /opensso/setup/setSetupProgress", 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`

These JAR files are available in the following ZIP file:

http://download.java.net/general/opensso/stable/issues/issue_4099.zip

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 Express 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” on page 23](#)
- [“4085: OpenSSO Enterprise is unable to store the CRL in the LDAP directory” on page 23](#)
- [“3827: Replication configuration hangs on second GlassFish instance” on page 23](#)
- [“3350, 2867: LDAP Follows Referral should be disabled for Active Directory Data Store” on page 24](#)
- [“Failover does not occur for Access Manager SDK \(AMSDK\) plug-in” on page 24](#)

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” on page 24](#)
- [“4100: Certificate authentication with CRL checking fails” on page 24](#)
- [“4054: amadmin authentication fails with URL org parameter” on page 24](#)
- [“1781: amadmin login fails for non Data Store authentication” on page 25](#)

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 23](#).

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 Enterprise 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” on page 25
- “3949: OCSP checking needs permission added to `server.policy` file” on page 25
- “3796: Creation of Fedlet in console failed in a console only deployment” on page 25
- “2381: Access Manager Roles policy subject is supported only with Access Manager repository data store” on page 26

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”](#) on page 26
- [“2827: Configuring a site does not add the second server to the site”](#) on page 26

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”](#) on page 27
- [“3955: Unable to execute the ssoadm command”](#) on page 27

- [“2905: jss4.jar entry is missing in the ssoadm classpath” on page 28](#)

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.slis.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.ipplanet.am.service.password
```

```
Logging configuration class "com.sun.identity.log.slis.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.ipplanet.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.ipplanet.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” on page 28](#)
- [“4080: Client SDK Configurator puts the wrong shared secret in the `AMConfig.properties` file” on page 29](#)

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 SDKAMConfig.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” on page 29](#)
- [“3065: Same context ID is used for all users in ID-FF log records” on page 29](#)
- [“2661: logout.jsp did not compile on WebSphere Application Server 6.1” on page 29](#)
- [“1977: SAMLv2 sample configure.jsp files fail on WebSphere Application Server 6.1” on page 30](#)

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 30.

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.xml 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.xml 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.xml 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” on page 31

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” on page 31](#)

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” on page 32](#)
- [“4108: Incorrect encryption key used after configuring OpenSSO Enterprise against existing schema \(DIT\)” on page 32](#)
- [“3962: Incorrect Console URL returned after authentication for non-admin user” on page 32](#)
- [“3961: `amadmin` cannot log in to OpenSSO Console in coexistence mode” on page 33](#)
- [“2348: Document Distributed Authentication UI server support” on page 33](#)

- “830: ID-FF schema metadata is not backward compatible” on page 33

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.ipplanet.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 [Installing the OpenSSO Enterprise 8.0 Update 1 Admin Tools](http://wikis.sun.com/x/tYF1BQ) (<http://wikis.sun.com/x/tYF1BQ>).

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” on page 34

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” on page 34](#)
- [“4051: Multi-byte trusted partner name is garbled in Console” on page 35](#)
- [“3993: End user page shows question marks for CCK and JA locales” on page 35](#)
- [“3976: Online Help “Tips on Searching” shows 404 error in non-English locale” on page 35](#)
- [“3766: encode.jsp and ampasword -e differ with multi-byte \(non-ASCII\) characters” on page 35](#)
- [“3763: Some non-ASCII characters are garbled when the web container is in C locale” on page 35](#)
- [“3713: Password reset page is not localized for CCJK locales” on page 35](#)
- [“3590: Change location for dounix_msgs.po files” on page 36](#)
- [“1793: Authentication fails with multi-byte character for org or module in query parameter” on page 36](#)

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 38.

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”](#) on page 36
- [“3994: In Spanish locale, cannot access Certificate for Configuration > Authentication”](#) on page 36
- [“3971: In Chinese \(zh_CN\) locale, online help is in English”](#) on page 36
- [“3802: Problems in the French part of copyright notice”](#) on page 37

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 31.

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.ipplanet.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. Sun Identity Manager provides user provisioning solutions that you can use instead of the AMSDK. For more information about Identity Manager, see http://www.sun.com/software/products/identity_mgr/index.jsp.

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 Sun Resources

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

- Sun Services: <http://www.sun.com/service/consulting/>
- Sun Software Products: <http://www.sun.com/software/>
- Sun Support Resources <http://sunsolve.sun.com/>
- Sun Developer Network (SDN): <http://developers.sun.com/>
- Sun Developer Services: <http://www.sun.com/developers/support/>

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 Sun upon request to determine which versions are best suited for deploying accessible solutions.

For information about Sun's commitment to accessibility, visit <http://sun.com/access>.

Related Third-Party Web Sites

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

Note – Sun 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. Sun 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 10 Revision History

Date (Revision)	Description of Changes
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 12 section.

TABLE 10 Revision History (Continued)

Date (Revision)	Description of Changes
January 4, 2010 (17)	■ Updated “Platforms Supported For OpenSSO Enterprise 8.0” on page 11 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 17 for Mac OS X 10.4.
April 10, 2009 (13)	■ In “Data Store Requirements For OpenSSO Enterprise 8.0” on page 14, 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 11, added the “Database Logging Requirements For OpenSSO Enterprise 8.0” on page 16 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 18 : ■ 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 11 .
November 11, 2008 (10)	Initial release.
August 26, 2008 (05)	Early Access (EA) release draft.