



Sun OpenSSO Enterprise 8.0 Release Notes



Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Part No: 820-3745
October 3, 2008

Copyright 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. All rights reserved.

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.

Copyright 2008 Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 U.S.A. Tous droits réservés.

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 dérivées 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
What's New in OpenSSO Enterprise 8.0	6
New Features in OpenSSO Enterprise 8.0	6
New Features in Version 3.0 Policy Agents	8
OpenSSO Enterprise 8.0 Hardware and Software Requirements	10
Operating System (OS) Support	10
Supported Web Containers	11
JDK Requirements	22
Data Store Requirements	23
Hardware Requirements	23
OpenSSO Enterprise Supported Browsers	24
OpenSSO Enterprise 8.0 Issues	24
830: ID-FF schema metadata is not backward compatible	25
1781: amadmin login fails for non data store authentication	25
1977: SAMLv2 sample configure.jsp files fail on WebSphere Application Server 6.1	25
2222: Password reset and account lockout services report notification errors	26
2348: Document Distributed Authentication UI server support	27
2381: Access Manager Roles policy subject is supported only with AMSDK data store	27
2661: logout.jsp did not compile on WebSphere Application Server 6.1	27
2827: Configuring a site does not add the second server to the site	27
2905: jss4.jar entry is missing in the ssoadm classpath	28
3065: Same context ID is used for all users in ID-FF log records	28
3350, 2867: LDAP Follows Referral should be disabled for Active Directory Data Store	28
Upgrading to OpenSSO Enterprise 8.0	28
Redistributable Files	29
Deprecation Notifications and Announcements	29
How to Report Problems and Provide Feedback	30

Sun Welcomes Your Comments 30

Additional Sun Resources 30

 Accessibility Features for People With Disabilities 31

 Related Third-Party Web Sites 31

Revision History 31

Sun OpenSSO Enterprise 8.0 Release Notes

Last revised October 3, 2008

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 are essentially the same product, but they 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>.

Contents

- “Getting Started With OpenSSO Enterprise 8.0” on page 6
- “What’s New in OpenSSO Enterprise 8.0” on page 6
- “OpenSSO Enterprise 8.0 Hardware and Software Requirements” on page 10
- “OpenSSO Enterprise 8.0 Issues” on page 24
- “Upgrading to OpenSSO Enterprise 8.0” on page 28
- “Redistributable Files” on page 29
- “Deprecation Notifications and Announcements” on page 29
- “How to Report Problems and Provide Feedback” on page 30
- “Additional Sun Resources” on page 30
- “Revision History” on page 31

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 “Supported Web Containers” on [page 11](#).
2. Download and unzip the `opensso.zip` file from the OpenSSO project site:
<https://opensso.dev.java.net/public/use/index.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`

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
<https://opensso.dev.java.net/public/use/index.html>.

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 up-to-date documentation.

What's New in OpenSSO Enterprise 8.0

OpenSSO Enterprise 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 following new features:

- “New Features in OpenSSO Enterprise 8.0” on [page 6](#)
- “New Features in Version 3.0 Policy Agents” on [page 8](#)

New Features in OpenSSO Enterprise 8.0

- 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.
- 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 [“Supported Web Containers” on page 11](#).
- 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 [“Supported Web Containers” on page 11](#).
- 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 Java System Identity Manager, SiteMinder, and Oracle Access Manager is added.
- Service Tags are supported.

OpenSSO Enterprise 8.0 is Service Tag enabled. To use Service Tags, you must first register your product. On the OpenSSO Enterprise Admin Console, under Common Tasks, click Register This 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.

For more information about Service Tags and Sun Connection, see http://lv.sun.com/practice/services/sun_connect/index.jsp.

To check your inventory, use the Sun Inventory site:
<https://inventory.sun.com/inventory/>

- 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 6.3, 7.0, or 7.1 and Federation Manager 7.0
 - Policy agent upgrade to version 3.0 from version 2.2 agents

New Features in Version 3.0 Policy Agents

Sun is developing version 3.0 policy agents in conjunction with OpenSSO Enterprise 8.0. The version 3.0 agents have the following new features and improvements:

- Centralized agent configuration

The centralized agent configuration feature moves most of the agent configuration properties from the `AMAgent.properties` file to the OpenSSO Enterprise central data repository. An agent administrator can then manage the multiple agent configurations from a central server location, using either the OpenSSO Enterprise Administration Console or the `ssoadm` command-line utility. The agent administrator no longer needs to edit an agent's `AMAgent.properties` file.

The centralized agent configuration feature separates the version 3.0 agent configuration data into two sets:

- The properties required for the agent to start up and initialize itself are stored in the `OpenSSOAgentBootstrap.properties` file locally on the server where the agent is installed. For example, the agent profile name and password used to access the OpenSSO Enterprise server are stored in the bootstrap file.
- The rest of the agent properties are stored either centrally in the OpenSSO Enterprise data repository (centralized configuration option) or locally in the `OpenSSOAgentConfiguration.properties` file (local configuration option).

- Agent types

Version 3.0 agents are classified according to type: `J2EEAgent` or `WebAgent`.

- Agent groups

You can assign version 3.0 agents of the same type (`J2EEAgent` or `WebAgent`) to an agent group. All agents in a group then selectively share a common set of configuration properties. Thus, the agent configuration and management is simplified, because an administrator can manage all of the agents within a group as a single entity.

Although all agents in the same group can share the same properties, you might need to define some individual properties for an agent (for example, the notification URL or agent URI properties).

- More hot-swappable agent configuration properties

Version 3.0 agents have more hot-swappable configuration properties. An administrator can change a hot-swappable configuration property value for an agent without having to restart the agent's deployment container for the new value to take effect. Properties in `OpenSSOAgentBootstrap.properties` are not hot-swappable.

- One-level wildcard support in URL policy

While the regular wildcard support applies to multiple levels in a resource, the one-level wildcard applies to only the level where it appears in a resource.

- Default J2EE agent installation option with minimal questions asked during the installation

Default or custom installation:

- **Default** (`agentadmin --install`): The `agentadmin` program displays a minimal number of prompts and uses default values for the other options. Use the default install option when the default option meet your deployment requirements.

- **Custom** (`agentadmin - - custom-install`): The `agentadmin` program displays a full set of prompts, similar to the version 2.2 program. Use the custom install option when you want to specify values other than the default options.
- Option to create the agent profile for J2EE agents in the server during installation
The 3.0 agent installer supports an option to create the agent profile in the OpenSSO Enterprise server during the agent installation so you don't have to create the profile manually using the OpenSSO Enterprise Console or `ssoadm` utility.
- Automated migration support
You can migrate a version 2.2 agent to a version 3.0 agent using the `agentadmin` program with the `- -migrate` option.
Note: OpenSSO Enterprise does not support version 2.1 policy agents.

OpenSSO Enterprise 8.0 Hardware and Software Requirements

- [“Operating System \(OS\) Support” on page 10](#)
- [“Supported Web Containers” on page 11](#)
- [“JDK Requirements” on page 22](#)
- [“Data Store Requirements” on page 23](#)
- [“Hardware Requirements” on page 23](#)
- [“OpenSSO Enterprise Supported Browsers” on page 24](#)

Operating System (OS) Support

TABLE 1 Operating System (OS) Support

Operating System	Supported Web Containers
Solaris 10 OS on SPARC, x86, and x64 based systems	All “Supported Web Containers” on page 11
Solaris 9 OS on SPARC and x86 based systems	
Red Hat Enterprise Linux 4 server (Base and Advanced Platform)	All “Supported Web Containers” on page 11 except Geronimo
Red Hat Enterprise Linux 5 (Base and Advanced Platform)	
Ubuntu 8.0.4	“Glassfish Application Server V2 UR1 and UR2” on page 13 only

TABLE 1 Operating System (OS) Support *(Continued)*

Operating System	Supported Web Containers
Windows Server 2003 Standard Edition	All “Supported Web Containers” on page 11 except Geronimo
Windows Server 2003 Enterprise Edition	
Windows 2003 Server Datacenter Edition	
Windows Vista	
IBM AIX 5.3	“IBM WebSphere Application Server 6.1” on page 18 only

Supported Web Containers

OpenSSO Enterprise supports the following web containers:

- “Sun Java System Application Server 9.1 Update 1 and Update 2” on page 11
- “Glassfish Application Server V2 UR1 and UR2” on page 13
- “Sun Java System Web Server 7.0 Update 3” on page 14
- “Apache Tomcat 5.5.x and 6.x” on page 14
- “BEA WebLogic Server 9.2 MP2” on page 14
- “BEA WebLogic Server 10” on page 16
- “Oracle Application Server 10g” on page 17
- “IBM WebSphere Application Server 6.1” on page 18
- “Apache Geronimo Application Server 2.1.1” on page 20
- “JBoss Application Server 4.x” on page 22

Sun Java System Application Server 9.1 Update 1 and Update 2

Pre-Deployment Tasks

In the Application Server 9.1 domain where you plan to deploy OpenSSO Enterpriseserver, change the following JVM options either using the Application Server administration console or CLI utility:

- Change `-Xmx512m` to `-Xmx1024m`.
- If necessary, change `-client` to `-server`.

If the Java Security Manager is enabled, add the following permissions to the `server.policy` file. After you edit the file, restart the web container.

```
grant {
permission java.net.SocketPermission "*", "listen,connect,accept,resolve";
permission java.util.PropertyPermission "*", "read, write";
permission java.lang.RuntimePermission "modifyThreadGroup";
```

```
permission java.lang.RuntimePermission "setFactory";
permission java.lang.RuntimePermission "accessClassInPackage.*";
permission java.util.logging.LoggingPermission "control";
permission java.lang.RuntimePermission "shutdownHooks";
permission javax.security.auth.AuthPermission "getLoginConfiguration";
permission javax.security.auth.AuthPermission "setLoginConfiguration";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext.*";
permission java.io.FilePermission "<<ALL FILES>>", "read,write,execute,delete";
permission java.util.PropertyPermission "java.util.logging.config.class", "write";
permission java.security.SecurityPermission "removeProvider.SUN";
permission java.security.SecurityPermission "insertProvider.SUN";
permission javax.security.auth.AuthPermission "doAs";
permission java.util.PropertyPermission "java.security.krb5.realm", "write";
permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
permission java.util.PropertyPermission "java.security.auth.login.config", "write";
permission java.util.PropertyPermission "user.language", "write";
permission javax.security.auth.kerberos.ServicePermission "*", "accept";
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission java.security.SecurityPermission "putProviderProperty.IAIC";
permission java.security.SecurityPermission "removeProvider.IAIC";
permission java.security.SecurityPermission "insertProvider.IAIC";
permission java.lang.RuntimePermission "setDefaultUncaughtExceptionHandler";
permission javax.management.MBeanServerPermission "newMBeanServer";
permission javax.management.MBeanPermission "*", "registerMBean";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
permission javax.security.auth.AuthPermission "getSubject";
permission javax.management.MBeanTrustPermission "register";
permission java.lang.management.ManagementPermission "monitor";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission java.util.PropertyPermission "javax.xml.soap.MetaFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.MessageFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPConnectionFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPFactory", "write";
permission java.net.NetPermission "getProxySelector";
permission java.security.SecurityPermission "getProperty.authconfigprovider.factory";
permission java.security.SecurityPermission "setProperty.authconfigprovider.factory";
permission javax.security.auth.AuthPermission "doAsPrivileged";
permission javax.security.auth.AuthPermission "modifyPublicCredentials";
permission java.security.SecurityPermission "insertProvider.XMLDSig";
permission java.security.SecurityPermission "putProviderProperty.WSS_TRANSFORM";
permission java.security.SecurityPermission "insertProvider.WSS_TRANSFORM";
};
```

Glassfish Application Server V2 UR1 and UR2

Glassfish download locations are:

- Glassfish V2 UR1: <https://glassfish.dev.java.net/downloads/v2ur1-b09d.html>
- Glassfish V2 UR2: <https://glassfish.dev.java.net/downloads/v2ur2-b04.html>

Pre-Deployment Tasks

In the Glassfish domain where you plan to deploy OpenSSO Enterprise server, change the following JVM options either using the Glassfish administration console or by editing the `domain.xml` file:

- Change `-client` to `-server`.
- Change `-Xmx512m` to `-Xmx1024m`.

If the Java Security Manager is enabled, add the following permissions to the `server.policy` file. After you edit the file, restart the web container.

```
grant {
permission java.net.SocketPermission "*", "listen,connect,accept,resolve";
permission java.util.PropertyPermission "*", "read, write";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "setFactory";
permission java.lang.RuntimePermission "accessClassInPackage.*";
permission java.util.logging.LoggingPermission "control";
permission java.lang.RuntimePermission "shutdownHooks";
permission javax.security.auth.AuthPermission "getLoginConfiguration";
permission javax.security.auth.AuthPermission "setLoginConfiguration";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext.*";
permission java.io.FilePermission "<<ALL FILES>>", "read,write,execute,delete";
permission java.util.PropertyPermission "java.util.logging.config.class", "write";
permission java.security.SecurityPermission "removeProvider.SUN";
permission java.security.SecurityPermission "insertProvider.SUN";
permission javax.security.auth.AuthPermission "doAs";
permission java.util.PropertyPermission "java.security.krb5.realm", "write";
permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
permission java.util.PropertyPermission "java.security.auth.login.config", "write";
permission java.util.PropertyPermission "user.language", "write";
permission javax.security.auth.kerberos.ServicePermission "*", "accept";
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission java.security.SecurityPermission "putProviderProperty.IAIC";
permission java.security.SecurityPermission "removeProvider.IAIC";
permission java.security.SecurityPermission "insertProvider.IAIC";
permission java.lang.RuntimePermission "setDefaultUncaughtExceptionHandler";
permission javax.management.MBeanServerPermission "newMBeanServer";
permission javax.management.MBeanPermission "*", "registerMBean";
permission java.lang.RuntimePermission "createClassLoader";
```

```
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
permission javax.security.auth.AuthPermission "getSubject";
permission javax.management.MBeanTrustPermission "register";
permission java.lang.management.ManagementPermission "monitor";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission java.util.PropertyPermission "javax.xml.soap.MetaFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.MessageFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPConnectionFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPFactory", "write";
permission java.net.NetPermission "getProxySelector";
permission java.security.SecurityPermission "getProperty.authconfigprovider.factory";
permission java.security.SecurityPermission "setProperty.authconfigprovider.factory";
permission javax.security.auth.AuthPermission "doAsPrivileged";
permission javax.security.auth.AuthPermission "modifyPublicCredentials";
permission java.security.SecurityPermission "insertProvider.XMLDSig";
permission java.security.SecurityPermission "putProviderProperty.WSS_TRANSFORM";
permission java.security.SecurityPermission "insertProvider.WSS_TRANSFORM";
};
```

Sun Java System Web Server 7.0 Update 3

Note – OpenSSO Enterpriseserver supports Web Server 7.0 Update 3 only. Web Server 7.0 Update 1 and Web Server 7.0 Update 2 are **not** supported.

Pre-Deployment Tasks

Using the Web Server 7.0 administration console or CLI, set the JVM heap size option from the default -Xms128M -Xmx256M to -Xms256M -Xmx512M.

Apache Tomcat 5.5.x and 6.x

Pre-Deployment Tasks

For both Tomcat 5.5.x and Tomcat 6.x, set the -Xmx JVM option to -Xmx1024m.

BEA WebLogic Server 9.2 MP2

WebLogic Server 9.2 MP2 is supported on the operating systems shown on the following site:

[http://e-docs.bea.com/
platform/suppconfigs/configs92/92_over/overview.html#1122259](http://e-docs.bea.com/platform/suppconfigs/configs92/92_over/overview.html#1122259)

Pre-Deployment Tasks

In the `bea_home/user_projects/domains/domain_name/bin/setDomainEnv.sh` script, add the `click.mode=debug` system property using `JVM_OPTIONS`.

On Windows systems set the `JVM_OPTIONS` in `setDomainEnv.cmd`. For example:

```
set JVM_OPTIONS=-Dclick.mode=debug
```

If you are using the Security Token Service (STS), set the `MaxPermSize` JVM option to a minimum value of 128 MB. For example:

```
-XX:MaxPermSize=128M
```

If the Java Security Manager is enabled, add the following permissions to the `weblogic.policy` file:

```
grant {
permission java.net.SocketPermission "*", "listen,connect,accept,resolve";
permission java.util.PropertyPermission "*", "read, write";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "setFactory";
permission java.lang.RuntimePermission "accessClassInPackage.*";
permission java.util.logging.LoggingPermission "control";
permission java.lang.RuntimePermission "shutdownHooks";
permission javax.security.auth.AuthPermission "getLoginConfiguration";
permission javax.security.auth.AuthPermission "setLoginConfiguration";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext.*";
permission java.io.FilePermission "<<ALL FILES>>", "read,write,execute,delete";
permission java.util.PropertyPermission "java.util.logging.config.class", "write";
permission java.security.SecurityPermission "removeProvider.SUN";
permission java.security.SecurityPermission "insertProvider.SUN";
permission javax.security.auth.AuthPermission "doAs";
permission java.util.PropertyPermission "java.security.krb5.realm", "write";
permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
permission java.util.PropertyPermission "java.security.auth.login.config", "write";
permission java.util.PropertyPermission "user.language", "write";
permission javax.security.auth.kerberos.ServicePermission "*", "accept";
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission java.security.SecurityPermission "putProviderProperty.IAIC";
permission java.security.SecurityPermission "removeProvider.IAIC";
permission java.security.SecurityPermission "insertProvider.IAIC";
permission java.lang.RuntimePermission "setDefaultUncaughtExceptionHandler";
permission javax.management.MBeanServerPermission "newMBeanServer";
permission javax.management.MBeanPermission "*", "registerMBean";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
```

```
permission javax.security.auth.AuthPermission "getSubject";
permission javax.management.MBeanTrustPermission "register";
permission java.lang.management.ManagementPermission "monitor";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission java.util.PropertyPermission "javax.xml.soap.MetaFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.MessageFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPConnectionFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPFactory", "write";
permission java.net.NetPermission "getProxySelector";
permission java.security.SecurityPermission "getProperty.authconfigprovider.factory";
permission java.security.SecurityPermission "setProperty.authconfigprovider.factory";
permission javax.security.auth.AuthPermission "doAsPrivileged";
permission javax.security.auth.AuthPermission "modifyPublicCredentials";
permission java.security.SecurityPermission "insertProvider.XMLDSig";
permission java.security.SecurityPermission "putProviderProperty.WSS_TRANSFORM";
permission java.security.SecurityPermission "insertProvider.WSS_TRANSFORM";
};
```

BEA WebLogic Server 10

WebLogic Server 10 is supported on the operating systems shown on the following site:

[http://e-docs.bea.com/
platform/suppconfigs/configs100/100_over/overview.html#1122259](http://e-docs.bea.com/platform/suppconfigs/configs100/100_over/overview.html#1122259)

Pre-Deployment Tasks

In the *bea_home/user_projects/domains/domain_name/bin/setDomainEnv.sh* script, add the *click.mode=debug* system property using *JVM_OPTIONS*.

On Windows systems set the *JVM_OPTIONS* in *setDomainEnv.cmd*. For example:

```
set JVM_OPTIONS=-Dclick.mode=debug
```

If you are using the Security Token Service (STS), set the *MaxPermSize* JVM option to a minimum value of 128 MB. For example:

```
-XX:MaxPermSize=128M
```

If the Java Security Manager is enabled, add the following permissions to the *weblogic.policy* file:

```
grant {
permission java.net.SocketPermission "*", "listen,connect,accept,resolve";
permission java.util.PropertyPermission "*", "read, write";
permission java.lang.RuntimePermission "modifyThreadGroup";
permission java.lang.RuntimePermission "setFactory";
permission java.lang.RuntimePermission "accessClassInPackage.*";
```



```

permission java.util.logging.LoggingPermission "control";
permission java.lang.RuntimePermission "shutdownHooks";
permission javax.security.auth.AuthPermission "getLoginConfiguration";
permission javax.security.auth.AuthPermission "setLoginConfiguration";
permission javax.security.auth.AuthPermission "modifyPrincipals";
permission javax.security.auth.AuthPermission "createLoginContext.*";
permission java.io.FilePermission "<<ALL FILES>>", "read,write,execute,delete";
permission java.util.PropertyPermission "java.util.logging.config.class", "write";
permission java.security.SecurityPermission "removeProvider.SUN";
permission java.security.SecurityPermission "insertProvider.SUN";
permission javax.security.auth.AuthPermission "doAs";
permission java.util.PropertyPermission "java.security.krb5.realm", "write";
permission java.util.PropertyPermission "java.security.krb5.kdc", "write";
permission java.util.PropertyPermission "java.security.auth.login.config", "write";
permission java.util.PropertyPermission "user.language", "write";
permission javax.security.auth.kerberos.ServicePermission "*", "accept";
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission java.security.SecurityPermission "putProviderProperty.IAIC";
permission java.security.SecurityPermission "removeProvider.IAIC";
permission java.security.SecurityPermission "insertProvider.IAIC";
permission java.lang.RuntimePermission "setDefaultUncaughtExceptionHandler";
permission javax.management.MBeanServerPermission "newMBeanServer";
permission javax.management.MBeanPermission "*", "registerMBean";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
permission javax.security.auth.AuthPermission "getSubject";
permission javax.management.MBeanTrustPermission "register";
permission java.lang.management.ManagementPermission "monitor";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission java.util.PropertyPermission "javax.xml.soap.MetaFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.MessageFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPConnectionFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPFactory", "write";
permission java.net.NetPermission "getProxySelector";
permission java.security.SecurityPermission "getProperty.authconfigprovider.factory";
permission java.security.SecurityPermission "setProperty.authconfigprovider.factory";
permission javax.security.auth.AuthPermission "doAsPrivileged";
permission javax.security.auth.AuthPermission "modifyPublicCredentials";
permission java.security.SecurityPermission "insertProvider.XMLDSig";
permission java.security.SecurityPermission "putProviderProperty.WSS_TRANSFORM";
permission java.security.SecurityPermission "insertProvider.WSS_TRANSFORM";
};

```

Oracle Application Server 10g

No pre-installation tasks are required.

IBM WebSphere Application Server 6.1

Pre-Deployment Tasks

Adding genericJvmArguments

Add the genericJvmArguments using the WebSphere Admin Console or by editing the `server.xml` file:

1. Open the following file:

```
install_root/IBM/WebSphere/AppServer/profiles/AppSrv01/  
config/cells/cell/nodes/node/servers/server/server.xml
```

2. Find the `jvmEntries` element.
3. Add the following genericJvmArguments and save the file:

```
genericJvmArguments="-DamCryptoDescriptor.provider=IBMJCE  
-DamKeyGenDescriptor.provider=IBMJCE"
```

4. Restart WebSphere 6.1 Application Server.

Adding Permissions to the server.policy File

In the

install_root/IBM/WebSphere/AppServer/profiles/AppSrv01/properties/server.policy file, add the following permissions. After you edit the file, restart the web container.

```
grant {  
  permission java.net.SocketPermission "*", "listen,connect,accept,resolve";  
  permission java.util.PropertyPermission "*", "read, write";  
  permission java.lang.RuntimePermission "modifyThreadGroup";  
  permission java.lang.RuntimePermission "setFactory";  
  permission java.lang.RuntimePermission "accessClassInPackage.*";  
  permission java.util.logging.LoggingPermission "control";  
  permission java.lang.RuntimePermission "shutdownHooks";  
  permission javax.security.auth.AuthPermission "getLoginConfiguration";  
  permission javax.security.auth.AuthPermission "setLoginConfiguration";  
  permission javax.security.auth.AuthPermission "modifyPrincipals";  
  permission javax.security.auth.AuthPermission "createLoginContext.*";  
  permission java.io.FilePermission "<<ALL FILES>>", "read,write,execute,delete";  
  permission java.util.PropertyPermission "java.util.logging.config.class", "write";  
  permission java.security.SecurityPermission "removeProvider.SUN";  
  permission java.security.SecurityPermission "insertProvider.SUN";  
  permission javax.security.auth.AuthPermission "doAs";  
  permission java.util.PropertyPermission "java.security.krb5.realm", "write";  
  permission java.util.PropertyPermission "java.security.krb5.kdc", "write";  
  permission java.util.PropertyPermission "java.security.auth.login.config", "write";  
  permission java.util.PropertyPermission "user.language", "write";  
}
```

```

permission javax.security.auth.kerberos.ServicePermission "*", "accept";
permission javax.net.ssl.SSLPermission "setHostnameVerifier";
permission java.security.SecurityPermission "putProviderProperty.IAIC";
permission java.security.SecurityPermission "removeProvider.IAIC";
permission java.security.SecurityPermission "insertProvider.IAIC";
permission java.lang.RuntimePermission "setDefaultUncaughtExceptionHandler";
permission javax.management.MBeanServerPermission "newMBeanServer";
permission javax.management.MBeanPermission "*", "registerMBean";
permission java.lang.RuntimePermission "createClassLoader";
permission java.lang.RuntimePermission "accessDeclaredMembers";
permission java.lang.reflect.ReflectPermission "suppressAccessChecks";
permission javax.security.auth.AuthPermission "getSubject";
permission javax.management.MBeanTrustPermission "register";
permission java.lang.management.ManagementPermission "monitor";
permission javax.management.MBeanServerPermission "createMBeanServer";
permission java.util.PropertyPermission "javax.xml.soap.MetaFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.MessageFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPConnectionFactory", "write";
permission java.util.PropertyPermission "javax.xml.soap.SOAPFactory", "write";
permission java.net.NetPermission "getProxySelector";
permission java.security.SecurityPermission "getProperty.authconfigprovider.factory";
permission java.security.SecurityPermission "setProperty.authconfigprovider.factory";
permission javax.security.auth.AuthPermission "doAsPrivileged";
permission javax.security.auth.AuthPermission "modifyPublicCredentials";
permission java.security.SecurityPermission "insertProvider.XMLDSig";
permission java.security.SecurityPermission "putProviderProperty.WSS_TRANSFORM";
permission java.security.SecurityPermission "insertProvider.WSS_TRANSFORM";
};

```

Running the JSP Compiler With WebSphere Application Server 6.1

WebSphere Application Server 6.1 has an Eclipse-based JSP compiler that uses JDT (Java Development Tooling) and the AST (Abstract Syntax Tree) parser. For information about parsing and generating the Java code, see:

<http://www-128.ibm.com/developerworks/opensource/library/os-ast/>

If you plan to deploy OpenSSO Enterprise in the WebSphere Application Server 6.1 Admin Console, the source level for the JSPs must be set to 15 (JVM 1.5). The default is 13 (JVM 1.3), which causes compilation problems. See issue “[1977: SAMLv2 sample configure.jsp files fail on WebSphere Application Server 6.1](#)” on page 25.

This compiler depends on some of the user env settings, and if they are not propagated during the compiler initialization, the compiler can fail to initialize properly. There are two workarounds to this issue:

- Install WebSphere Application Server 6.1 as a non-root user, and the installation process should work as expected.

or

- Modify your web archive descriptor for the JDK compiler. Edit your `ibm-web-ext.xml` file under the web module deployment directory and add a line similar to:

```
<jspAttributes xmi:id="JSPAttribute_#####" name="useJDKCompiler"
value="true"/>
```

where `#####` is any unique number.

Using the `ssoadm` and `ampassword` Utilities

Before you run the setup script to install the tools and scripts, modify the setup script. Before `-cp ...` in the last line, insert:

```
-D"amCryptoDescriptor.provider=IBMJCE" -D"amKeyGenDescriptor.provider=IBMJCE"
```

After you run the setup script to install the tools and before you run `ssoadm`, add the following items to the `ssoadm` script:

- Add `xalan.jar` to the classpath after `openfedlib.jar`. For example:
`${TOOLS_HOME}/lib/xalan.jar`
- Add the following items before `com.sun.identity.cli.CommandManager` and `com.sun.identity.tools.bundles.Main`:
`-D"amKeyGenDescriptor.provider=IBMJCE"`
`-D"amCryptoDescriptor.provider=IBMJCE"`

After you run the setup script and before you run `ampassword`, add the following items to the `ampassword` script before `com.ipplanet.services.ldap.ServerConfigMgr` and `com.sun.identity.tools.bundles.Main`:

```
-D"amCryptoDescriptor.provider=IBMJCE" -D"amKeyGenDescriptor.provider=IBMJCE"
```

Apache Geronimo Application Server 2.1.1

Note – OpenSSO Enterprise server supports Geronimo Application Server 2.1.1 with Tomcat on Solaris systems only.

Pre-Deployment Task

Modify the `/geronimo-tomcat6-jee5-2.0.2/bin/geronimo.sh` file by adding `-X:MaxPermSize=512M`, as shown in the following start block:

```
elif [ "$1" = "start" ] ; then
shift
touch "$GERONIMO_OUT"
```

```

$START_OS_CMD "$_RUNJAVA" $JAVA_OPTS $GERONIMO_OPTS \
$JAVA_AGENT_OPTS \
-Dorg.apache.geronimo.base.dir="$GERONIMO_BASE" \
-Djava.endorsed.dirs="$ENDORSED_DIRS" \
-Djava.io.tmpdir="$GERONIMO_TMPDIR" \
-XX:MaxPermSize=512M \
-jar "$GERONIMO_HOME"/bin/server.jar $LONG_OPT "$@" \
>> $GERONIMO_OUT 2>&1 &
echo "" echo "Geronimo started in background. PID: $!"
if [ ! -z "$GERONIMO_PID" ]; then echo $! > $GERONIMO_PID
fi

```

To deploy the OpenSSO Enterprise WAR file on Geronimo, you must provide a deployment plan file either inside or outside of the WAR file. If placed inside the WAR file, name the plan `geronimo-web.xml` and place the file in `WEB-INF` directory. If placed outside of the WAR file, the plan file can be named otherwise. Here is a sample plan file:

```

<?xml version="1.0" encoding="UTF-8"?>
<web-app xmlns="http://geronimo.apache.org/xml/ns/j2ee/web-1.2">
  <environment>
    <moduleId>
      <groupId>sun</groupId>
      <artifactId>FAM</artifactId>
      <version>8.0</version>
      <type>war</type>
    </moduleId>
  </environment>
  <context-root>/fam1</context-root>
</web-app>

```

In the above example, the WAR file is deployed at:

```
geronimo-tomcat6-jee5-2.0.2/repository/sun/FAM/8.0/FAM-8.0.war
```

The web application is deployed at *protocol://server:port/fam1*. You can change the deployment plan depending on your deployment scenario.

Notes:

- Geronimo console URL: *protocol://server:8080/console/portal/welcome*
- Default user name and password: `system/manager`
- To start the Geronimo server: `/geronimo-tomcat6-jee5-2.0.2/bin/geronimo.sh start`
- To stop the Geronimo server: `/geronimo-tomcat6-jee5-2.0.2/bin/geronimo.sh stop`

JBoss Application Server 4.x

OpenSSO Enterprise server supports only the Exploded Deployment on JBoss Application Server 4.x. For more information see:

<http://wiki.jboss.org/wiki/Wiki.jsp?page=ExplodedDeployment>

If you are using the Security Token Service (STS), set the MaxPermSize JVM option to a minimum value of 128 MB. For example:

```
-XX:MaxPermSize=128M
```

To deploy OpenSSO Enterprise server on JBoss Application Server 4.x:

1. Create a subdirectory under *JBOSS_HOME/server/instance/deploy/name_of_war_file*.
For example:

```
# mkdir /opt/jboss-4.2.2.GA/server/fam/deploy/fam.war
```
2. Explode the opensso.war file in this new directory. For example: You don't need to restart the container, because JBoss will automatically hot-deploy it.

```
# cd /opt/jboss-4.2.2.GA/server/fam/deploy/opensso.war  
# jar xvf /tmp/opensso.war
```
3. Point your browser to `http://host.domain:port/opensso` or `http://host:port/opensso` and start configuring OpenSSO Enterpriseserver.
4. The OpenSSO Enterprise Configurator will write a bootstrap file in your home directory.
For example:
`/AccessManager/AMConfig_opt_jboss-4.2.2.GA_server_fam_.deploy_opensso.war_`

JDK Requirements

TABLE 2 JDK Requirements

OpenSSO Enterprise	Supported JDK Version
Server	JDK 1.5.x or 1.6.x
	64-bit JVM on supported web containers
Client (OpenSSO SDK)	JDK 1.4.x, 1.5.x. or JDK 1.6.x

Data Store Requirements

TABLE 3 Data Store Requirements

Data Store Type	Supported Data Stores
Configuration data store (also referred to as the Service Management data store)	<ul style="list-style-type: none"> ■ Sun Java System Directory Server 5.2, 6.0, 6.2, and 6.3 ■ OpenSSO Enterprise (embedded store)
User data store	<ul style="list-style-type: none"> ■ Sun Java System Directory Server 5.2, 6.0, 6.2, and 6.3 ■ OpenSSO Enterprise (embedded store) Note: The OpenSSO Enterprise user data store is supported only for prototype, proof of concept (POC), or developer deployments that have a small set of users. It is not supported for production deployments. ■ Microsoft Active Directory 2003 on Windows Server 2003 R2 ■ IBM Tivoli Directory Server 6.1

Hardware Requirements

TABLE 4 OpenSSO Enterprise Hardware Requirements

Component	Requirement
RAM	Prototype or developer deployment: 1 GB Production deployment: 4 GB recommended
Disk space	For server with console, server only, or console only deployment: <ul style="list-style-type: none"> ■ 512 MB for OpenSSO Enterprise binary files and configuration data ■ 2 GB for log files, including container log files For client SDK deployment: <ul style="list-style-type: none"> ■ 100 MB minimum ■ 1 GB recommended for debug logs, if debug level (<code>com.ipplanet.services.debug.level</code>) is set to Message

OpenSSO Enterprise Supported Browsers

TABLE 5 OpenSSO Enterprise Supported Browsers

Browser	Platform
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 XP and Windows 2003
Microsoft Internet Explorer 6.0 SP2	Windows XP
Microsoft Internet Explorer 6.0 SP1	Windows 2000
Mozilla 1.7.12	Solaris OS, versions 9 and 10
	Windows XP
	Windows 2000
	Red Hat Linux 4 and 5
Netscape Communicator 8.0.4	Windows XP
	Windows 2000
Netscape Communicator 7.1	Solaris OS, versions 9 and 10

OpenSSO Enterprise 8.0 Issues

- “830: ID-FF schema metadata is not backward compatible” on page 25
- “1781: amadmin login fails for non data store authentication” on page 25
- “1977: SAMLv2 sample configure.jsp files fail on WebSphere Application Server 6.1” on page 25
- “2222: Password reset and account lockout services report notification errors” on page 26
- “2348: Document Distributed Authentication UI server support” on page 27
- “2381: Access Manager Roles policy subject is supported only with AMSDK data store” on page 27
- “2661: logout.jsp did not compile on WebSphere Application Server 6.1” on page 27
- “2827: Configuring a site does not add the second server to the site” on page 27
- “2905: jss4.jar entry is missing in the ssoadm classpath” on page 28
- “3065: Same context ID is used for all users in ID-FF log records” on page 28
- “3350, 2867: LDAP Follows Referral should be disabled for Active Directory Data Store” on page 28

For more information about OpenSSO Enterprise issues, see:

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

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](#) (<http://infobot.sfbay.sun.com/~js125477/ReviewDrafts/UPG/>).

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`.

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/webmodule/name/
```

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

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`.

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

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

The Access Manager Roles policy subject is supported only with the 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.

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 25.

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.

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.)

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.

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.

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 Access Manager 6 2005Q1 (6.3) 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.

For the detailed upgrade steps, see the [Sun OpenSSO Enterprise 8.0 Upgrade Guide](http://infobot.sfbay.sun.com/~js125477/ReviewDrafts/UPG/) (<http://infobot.sfbay.sun.com/~js125477/ReviewDrafts/UPG/>).

Redistributable Files

Sun OpenSSO Enterprise 8.0 does not contain any files that you can redistribute to non-licensed users of the product.

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. Sun Java System 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 as follows:

- Sun Support Resources (SunSolve) services at <http://sunsolve.sun.com/>.
This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract

So that we can best assist you in resolving problems, please have the following information available when you contact support:

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 6 Revision History

Date	Description of Changes
October 3, 2008	In progress RR review draft
August 26, 2008	Early Access (EA) release

