



Sun OpenSSO Enterprise 8.0 Upgrade Guide



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

Part No: 820-5019
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 SunTM 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 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.

OpenSSO Enterprise 8.0 Upgrade Guide

Last revised October 3, 2008

The *Sun OpenSSO Enterprise 8.0 Upgrade Guide* describes how to upgrade Sun Java System Access Manager and Sun Java System Federation Manager to OpenSSO Enterprise 8.0.

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.

Contents

- [“OpenSSO Enterprise 8.0 Upgrade Overview” on page 3](#)
- [“OpenSSO Enterprise 8.0 Pre-Upgrade Steps” on page 5](#)
- [“Collecting Configuration Data Required for the OpenSSO Enterprise Open SSO Enterprise 8.0 Upgrade” on page 7](#)
- [“Upgrading to OpenSSO Enterprise 8.0” on page 8](#)
- [“Optional OpenSSO Enterprise Open SSO Enterprise 8.0 Post-Upgrade Steps” on page 15](#)
- [“Additional Sun Resources” on page 15](#)
- [“Accessing Sun Resources Online” on page 16](#)
- [“Revision History” on page 17](#)

OpenSSO Enterprise 8.0 Upgrade Overview

- [“Previous Releases and Platforms Supported for the OpenSSO Enterprise 8.0 Upgrade” on page 4](#)
- [“OpenSSO Enterprise 8.0 Upgrade Considerations” on page 4](#)
- [“OpenSSO Enterprise 8.0 Coexistence and Backward Compatibility” on page 5](#)

Previous Releases and Platforms Supported for the OpenSSO Enterprise 8.0 Upgrade

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

Previous Release, Including Configuration Data in Sun Java System Directory Server	Upgrade Supported From This Platform
Sun Java System Access Manager 7.1 server Upgrade is supported for: <ul style="list-style-type: none">▪ Sun Java Enterprise System installer deployment▪ WAR file deployment only if the configuration data is in Sun Java System Directory Server. If the configuration data is in the File System (flat file), the upgrade is not supported.	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

OpenSSO Enterprise 8.0 Upgrade Considerations

- Upgrade of the configuration data is supported only from and to Sun Java System Directory Server. If the configuration data for an Access Manager 7.1 WAR file deployment is in the File System (flat file), the upgrade is not supported.
- The following Legacy and Realm mode upgrades are supported:
 - Legacy to Legacy mode
 - Legacy to Realm mode
 - Realm to Realm mode
- Upgrade is **not** supported for the following:
 - Access Manager or Federation Manager AMSDK
 - Access Manager or Federation Manager client SDK
 - Distributed Authentication UI server
 - IDP Discovery
 - Remote console

OpenSSO Enterprise 8.0 Coexistence and Backward Compatibility

- [“OpenSSO Enterprise 8.0 Coexistence” on page 5](#)
- [“OpenSSO Enterprise 8.0 Backward Compatibility” on page 5](#)

OpenSSO Enterprise 8.0 Coexistence

OpenSSO Enterprise 8.0 server can coexistence only with the Access Manager 7.1 Directory Server schema (DIT or Access Manager services configuration).

Coexistence is **not** supported between OpenSSO Enterprise 8.0 server and these releases:

- Access Manager 7 2005Q4
- Access Manager 6 2005Q1 (6.3) and earlier 6.x releases
- Federation Manager 7.0

Coexistence occurs when OpenSSO Enterprise and Access Manager 7.1 server instances are accessing the same Directory Server schema (DIT). This scenario usually occurs when multiple instances of Access Manager 7.1 that access the same Directory Server schema are being upgraded sequentially, one instance at a time. OpenSSO Enterprise 8.0 will continue to work with the Access Manager 7.1 schema and support all of the Access Manager 7.1 features (except for ID-FF metadata as described in the next section) until the schema is upgraded.

OpenSSO Enterprise 8.0 Backward Compatibility

Backward compatibility is supported for all Access Manager 7.1 and Access Manager 7 2005Q4 existing features including the full SDK and the client SDK APIs.

Backward compatibility is **not** supported for:

- Releases earlier than Access Manager 6 2005Q1 (6.3)
- ID-FF schema metadata: ID-FF profiles do not work unless you upgrade the Access Manager or Federation Manager schema in Directory Server.

OpenSSO Enterprise 8.0 Pre-Upgrade Steps

Before you upgrade Access Manager or Federation Manager to OpenSSO Enterprise 8.0, perform these steps:

- [“Upgrade Related Components as Needed” on page 6](#)
- [“Backup the Access Manager or Federation Manager Schema” on page 6](#)
- [“Back Up Customized Configuration Files” on page 6](#)
- [“Set Your JAVA_HOME Environment Variable” on page 6](#)

Upgrade Related Components as Needed

The following components must be supported by Open SSO Enterprise 8.0:

- Sun Java System Directory Server
- Web container
- Operating system
- Shared components such as the JDK: Open SSO Enterprise 8.0 requires JDK 1.5 or later.

For a list of the supported versions of these components, see “[OpenSSO Enterprise Hardware and Software Requirements](#)” in *Sun OpenSSO Enterprise 8.0 Release Notes*.

If necessary, upgrade these components to a version supported by OpenSSO Enterprise 8.0.

Backup the Access Manager or Federation Manager Schema

Backup the Access Manager or Federation Manager schema (DIT) by exporting the schema to an LDIF file.

Back Up Customized Configuration Files

Back up any customized files in your Access Manager or Federation Manager deployment. For example, back up any JSP files that are customized for the Access Manager Console.

Set Your JAVA_HOME Environment Variable

The upgrade scripts and jar command require JDK 1.5 or later. Therefore, set your JAVA_HOME environment variable to point to a version 1.5 or later JDK installation.

Collecting Configuration Data Required for the OpenSSO Enterprise Open SSO Enterprise 8.0 Upgrade

During the upgrade process, you will need to know the following configuration data:

- “Access Manager or Federation Manager Server Settings” on page 7
- “Directory Server Settings for the Configuration Data Store” on page 7
- “Directory Server Settings for the User Data Store” on page 7

Access Manager or Federation Manager Server Settings

- Administrator (amadmin) password
- Server host name
- Server port
- Cookie domain
- Platform locale
- Default Policy Agent user (UrlAccessAgent) password
- Deploy URI of the existing Access Manager or Federation Manager instance

Directory Server Settings for the Configuration Data Store

- SSL enabled (yes or no)
- Host name
- Port
- Encryption key: Use the value of the `am.encryption.pwd` property from `AMConfig.properties` from the previous release.
- Root suffix
- Directory Server administrator
- Directory Server administrator password
- `amldapuser` password

Directory Server Settings for the User Data Store

- SSL enabled
Note. Before you upgrade, SSL should be disabled for the user data store.
- Directory name

- Port
- Root suffix. Use the value of the `com.ipplanet.am.rootsuffix` property from `AMConfig.properties` from the previous release.
- Directory Server Administrator. For example: "cn=Directory Manager"
- Directory Server Administrator password

Upgrading to OpenSSO Enterprise 8.0

- “Downloading and Unzipping the `opensso.zip` File” on page 8
- “Applying Customizations From Your Previous Deployment” on page 9
- “Running the Pre-Upgrade (`ssopre80upgrade`) Script” on page 9
- “Deploying the OpenSSO Enterprise Open SSO Enterprise 8.0 WAR File” on page 11
- “Configuring OpenSSO Enterprise Open SSO Enterprise 8.0 Against the Existing Access Manager or Federation Manager Schema” on page 12
- “Upgrading the Access Manager or Federation Manager Schema” on page 14

Downloading and Unzipping the `opensso.zip` File

OpenSSO Enterprise 8.0 is distributed as a downloadable ZIP file named `opensso.zip`. This ZIP file contains both Access Manager and Federation Manager functionality, plus the new OpenSSO Enterprise 8.0 features.

▼ To Download and Unzip the `opensso.zip` File

- 1 **Log on as super user (root).**
- 2 **Create an upgrade base directory to download and unzip `opensso.zip`.**
You must have both read and write access to this directory.
This guide uses *zip-root* as the name of the upgrade base directory.
- 3 **Download `opensso.zip` from the OpenSSO project site to the directory you created in Step 1:**
<http://opensso.dev.java.net/public/use/index.html>
- 4 **Unzip the `opensso.zip` file.**
The upgrade scripts and related files are in the *zip-root/opensso/upgrade* directory.

Applying Customizations From Your Previous Deployment

If you customized any files in your previous Access Manager or Federation Manager deployment, you will need to apply your customizations to the `opensso.war` file. After you unzip `opensso.zip`, `opensso.war` is in the following directory:

`zip-root/opensso/deployable-war`

▼ To Apply Customizations to `opensso.war`

- 1 **Create a staging directory to extract the files in `opensso.war`. For example:** `openssocust`
- 2 **Extract the files in `opensso.war` into the staging directory. For example:**

```
# cd openssocust
# jar xvf zip-root/opensso/deployable-war/opensso.war
```
- 3 **Apply any customizations from the previous Access Manager or Federation Manager deployment. For example, apply any customized JSP files for the Administration Console.**
- 4 **Create a new WAR file from the staging directory with the customized files. For example:**

```
# cd openssocust
# jar cvf zip-root/opensso/deployable-war/amserver.war *
```

Important: The name of the new WAR file must be same as the deploy URI of the previous Access Manager or Federation Manager instance. For example, if the previous instance is deployed with the `/amserver` URI, the new WAR file must be named `amserver.war`.

Running the Pre-Upgrade (`ssopre80upgrade`) Script

The `ssopre80upgrade` script prepares the system for the upgrade by performing these tasks:

- Backs up essential Access Manager or Federation Manager files (such as logs and configuration files) on the existing system
- Removes the Access Manager 7.1, Access Manager 7 2005Q4, or Access Manager 6 2005Q1 (6.3) packages
- Removes the Federation Manager 7.0 packages
- Removes the SAMLv2 Plug-in package
- Updates the `/var/sadm/install/productregistry` file to reflect the package removal for the Java Enterprise System Access Manager packages

▼ To Run the Pre-Upgrade Script

- 1 **Login as super user (root).**
- 2 **Change to the *zip-root/opensso/upgrade/scripts* directory.**
- 3 **Run the *ssopre80upgrade* script:**
 - Solaris and Linux systems: `./ssopre80upgrade`
 - Windows: `ssopre80upgrade.bat`
- 4 **When prompted by the script, provide the following information:**
 - Federation Manager 7.0 staging directory, if you are upgrading a Federation Manager instance
 - Directory Server fully qualified host name
 - Directory Server port
 - Access Manager or Federation Manager top-level administrator DN (`amAdmin`)
 - Top-level administrator (`amAdmin`) password
 - Directory to store the Access Manager or Federation Manager backup files
 - OpenSSO Enterprise 8.0 configuration directory: Directory you specified when you ran the Configurator. Default is `/opensso`
 - OpenSSO 8.0 Enterprise upgrade directory. *zip-root/opensso/upgrade*
 - OpenSSO 8.0 Enterprise staging directory: Directory where you customized the WAR file. For example: `openssocust`
- 5 **Set the following properties in the *zip-root/opensso/upgrade/config/ssUpgradeConfig.properties* file:**
 - `XML_ENCODING`: For example: `XML_ENCODING=UTF-8`
 - `BASEDIR`: Upgrade base directory. For example: `BASEDIR=zip-root/opensso`
 - `ORG_NAMING_ATTR`: Organization naming attribute. Default is `o`. For example: `ORG_NAMING_ATTR=o`
 - `USER_NAMING_ATTR`: User naming attribute. Default is `uid`. For example: `USER_NAMING_ATTR=uid`
 - `DEPLOY_URI`: OpenSSO Deploy URI. For example: `DEPLOY_URI=amserver`
 - `PAM_SERVICE_NAME`:
 - Solaris systems: `PAM_SERVICE_NAME=other`
 - Linux systems: `PAM_SERVICE_NAME=password`
 - `DB_NAME`: OpenSSO Enterprise backend database. Default: `DB_NAME=userRoot`

- `INSTANCE_TYPE`: Set to the instance type you are upgrading:
 - Access Manager: `INSTANCE_TYPE=AM`
 - Federation Manager: `INSTANCE_TYPE=FM`
- `LDAP_USER_PASS`: `amldapuser password`
- `ORG_OBJECT_CLASS=sunismangedorganization` is the default.
- `USER_OBJECT_CLASS=inetorgperson` is the default.

Deploying the OpenSSO Enterprise Open SSO Enterprise 8.0 WAR File

▼ To Deploy the OpenSSO Enterprise Open SSO Enterprise 8.0 WAR File

- 1 log on as super user (`root`).
- 2 Undeploy the existing Access Manager or Federation Manager web applications:
 - For an Access Manager 7.1 WAR file deployment, undeploy the WAR file using the web container's CLI or administration console.
 - For a Java Enterprise System installer deployment of Access Manager 7.1, Access Manager 7 2005Q4, or Access Manager 2005Q1 (6.3), undeploy all web applications (`amserver`, `console`, `password`, `services`) by running the `amconfig` script with `DEPLOY_LEVEL=26` in the `amsamplesilent` file.
For more information, see [Chapter 2, “Running the Access Manager amconfig Script,” in *Sun Java System Access Manager 7.1 Postinstallation Guide*](#).
 -

- 3 Deploy the OpenSSO Enterprise WAR file using web container's deployment command or administration console.

The OpenSSO Enterprise WAR file is either:

- `zip-root/opensso/deployable-war/opensso.war`, if you did not apply any customizations or
- A customized OpenSSO WAR file you created in [“To Apply Customizations to `opensso.war`” on page 9](#)

Important: Deploy the new OpenSSO Enterprise WAR file on same host and port where the previous Access Manager or Federation Manager instance was deployed.

- 4 Restart the OpenSSO Enterprise web container.

Configuring OpenSSO Enterprise Open SSO Enterprise 8.0 Against the Existing Access Manager or Federation Manager Schema

After you deploy the OpenSSO WAR file, you must configure the new OpenSSO Enterprise deployment against the existing Access Manager or Federation Manager schema (or DIT) using the Configurator.

This guide describes the GUI Configurator. If you prefer, you can also use the command-line Configuration, as described in [Chapter 4, “Configuring OpenSSO Enterprise Using the Command-Line Configurator,”](#) in *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

▼ To Configure OpenSSO Enterprise Against the Existing Access Manager or Federation Manager Schema

- 1 **Launch the GUI Configurator by entering the OpenSSO Enterprise URL in your browser:**

protocol://serverhost:serverport/deployuri

For example: `http://serverhost.example.com:8080/amserver`

- 2 **On the Configuration Options page, click Create New Configuration.**

- 3 **Step 1: General: On the Default User Password page, enter and confirm the amAdmin password.**

Use the same amadmin password as the Access Manager or Federation Manager instance you are upgrading.

Click **Next** to continue.

- 4 **Step 2: Server Settings**

- **Server URL:** Use the same value as the Access Manager or Federation Manager instance you are upgrading
- **Cookie Domain:** Use the same value as the Access Manager or Federation Manager instance you are upgrading
- **Platform Locale:** Use the same value as the Access Manager or Federation Manager instance you are upgrading
- **Configuration Directory:** Use the default value (/opensso) or specify another value.

Click **Next** to continue.

- 5 **Step 3: Configuration Data Store Settings**

Check **First Instance**.

For **Configuration Data Store**, check Sun Java System Directory Server.

Specify the following Directory Server values from the existing Access Manager or Federation Manager instance:

- **SSL Enabled** (check box)
- **Host Name**
- **Port**
- **Encryption Key**
- **Root Suffix**
- **Login ID:** Directory Server Admin DN
- **Password:** Directory Server Admin password

Click **Next** to continue.

6 Step 4: User Data Store Settings:

Click **Use Other User Data Store** to specify Sun Java System Directory Server.

Specify the following Directory Server values from the existing Access Manager or Federation Manager instance:

- **SSL Enabled** (check box)
Note: To upgrade, SSL should be disabled for the user data store.
- **Directory Name**
- **Port**
- **Root Suffix**
- **Login ID:** Directory Server Admin DN
- **Password:** Directory Server Admin password
- **User Data Store Type:** Check LDAP with OpenSSO Schema

Click **Next** to continue.

7 Step 5: Site Configuration

Check **No** and Click **Next** to continue

8 Step 6: Default Policy Agent User

Enter and confirm the password for the default Policy Agent user (UrlAccessAgent). which is usually the amldapuser password.

Click **Next** to continue

9 Step 7: Configuration Summary Details

If the settings in the Summary are correct, click **Create Configuration**.

When the configuration is complete, the Configurator displays a link to redirect you to the OpenSSO Enterprise Administration Console.

10 Log in to the OpenSSO Enterprise Administration Console as `amadmin` using the password you specified during the configuration.

At this point, OpenSSO Enterprise is running against the existing Access Manager or Federation Manager schema (or DIT), which is known as co-existence mode.

Upgrading the Access Manager or Federation Manager Schema

The `ssoupgrade` script upgrades the Access Manager or Federation Manager schema to the OpenSSO Enterprise 8.0 schema.

▼ To Upgrade the Access Manager or Federation Manager Schema

- 1 Log on as super user (`root`).**
- 2 Make sure that your `JAVA_HOME` environment variable points to JDK 1.5 or later.**
- 3 Change to the `zip-root/opensso/upgrade/scripts` directory.**

4 Run the `ssoupgrade` script:

- Solaris and Linux systems: `./ssoupgrade`
- Windows: `ssoupgrade.bat`

5 When prompted by the script, provide the following information:

- OpenSSO Enterprise 8.0 Upgrade Base Directory
- OpenSSO Enterprise 8.0 Configuration Directory
- OpenSSO Enterprise 8.0 Staging Directory
- Directory Server full qualified host name
- Directory Server port
- Top-level Administrator DN (`amAdmin` DN)
- Top-level Administrator Password (`amAdmin` password)
- Enable Realms

This prompt is displayed only if the existing instance is in Legacy mode or is a Federation Manager instance. To migrate to Realm mode, enter `y`. Sun recommends that you migrate to Realm mode because Legacy mode will be decrypted.

6 Restart the Open SSO Enterprise web container.

Next Steps Log in to the OpenSSO Enterprise Console using the following URL:

protocol://host:port/deployURI/UI/Login

For example: `http://serverhost.example.com:8080/amserver`

Optional OpenSSO Enterprise Open SSO Enterprise 8.0 Post-Upgrade Steps

The following steps are optional:

- On Windows, you must the uninstall the Access Manager packages manually. For information, see the *Sun Java Enterprise System 5 Installation Guide for Microsoft Windows* (<http://docs.sun.com/doc/819-5699>).
- If you wish, you can manually remove the Federation Manager 7.0 staging directory.

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.

Accessing Sun Resources Online

The docs.sun.comSM web site enables you to access Sun technical documentation online. You can browse the docs.sun.com archive or search for a specific book title or subject. Books are available as online files in PDF and HTML formats. Both formats are readable by assistive technologies for users with disabilities.

To access the following Sun resources, go to <http://www.sun.com>:

- Downloads of Sun products
- Services and solutions
- Support (including patches and updates)
- Training
- Research
- Communities (for example, Sun Developer Network)

Third-Party Web Site References

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 or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to <http://docs.sun.com> and click Send Comments. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the book's title page or in the document's URL. For example, the part number of this book is 820-5019.

Revision History

Date (Part Number)	Description of Changes
October 3, 2008 (820-5019-10)	Initial review draft

