Sun GlassFish Web Space Server 10.0 OpenSSO Add-On Guide

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

Part No: 820–7277
March 2009

090701@22510

Contents

◆ ◆ ◆ CHAPTER 1

Overview

The Sun Microsystems OpenSSO Add-On for Sun GlassFish Web Space Server 10.0 software provides enterprise-grade single sign-on and authentication features for Web Space Server portals and portlets. This Add-On also provides convenience features for mapping OpenSSO and Access Manager users, roles, filtered roles, groups, and realms to Web Space Server users, communities, and organizations. This guide provides instructions for installing, using, and troubleshooting the OpenSSO Add-On.

This chapter includes the following topics:

Who Should Read This Guide?

This guide is intended for registered Web Space Server developers and administrators who want use the OpenSSO Add-On for Sun GlassFish Web Space Server package to enhance the power of Web Space Server software with OpenSSO single sign-on and authentication features. This guide is also of interest to developers and administrators who are looking to migrate OpenSSO or Access Manager—based Portal Server user, role, group, and realm configurations to corresponding Web Space Server configurations.

Note – This guide does not provide detailed usage instructions for using Web Space Server in general. For such information, refer to the rest of the Sun GlassFish Web Space Server Document Collection. Note also that this guide does not explain how to install and configure your OpenSSO server. You must have a working OpenSSO server configured before installing the OpenSSO Add-On.

What Are Sun GlassFish Web Space Server Add-Ons?

The OpenSSO Add-On for Sun GlassFish Web Space Server is one of several Add-On packages available for Sun GlassFish Web Space Server software. These add-ons, also sometimes called *accelerators*, are an evolving set of standalone feature packages that provide performance enhancements and/or easier integration with third-party software tools. Please see the Sun GlassFish Web Space Server product page for the most current list of Add-On packages available for Web Space Server.

Where Can You Get Web Space Server Add-On Packages?

The Sun GlassFish Web Space Server Add-On packages are available for free to registered Web Space Server users through the Sun GlassFish Update Tool. The specific Add-On packages that are available to you depend on how your Web Space Server software is registered:

- Registered users with a **paid Web Space Server service contract** have unlimited access to the full set of Web Space Server add-ons.
- Registered users who do not have a paid Web Space Server service contract have access to a limited subset of the Web Space Server Add-On collection.

It is important to note that while Sun GlassFish Web Space Server software is a free, **open source** product, the Web Space Server add-ons are proprietary components developed and licensed by Sun Microsystems, Inc.

To learn more about Web Space Server, Add-On products for Web Space Server, and Web Space Server service contracts, go to the Sun GlassFish Web Space Server product page.

Additional Sun GlassFish Web Space Server Documentation

Each Web Space Server Add-On package has its own user's guide. Please see the Sun GlassFish Web Space Server Add-On Document Collection for links to documentation for the currently available Add-On products. Be sure to check back often, as the list of available add-ons is updated frequently.

For complete documentation for the core Sun GlassFish Web Space Server 10.0 software product, see the Sun GlassFish Web Space Server Document Collection. Additional portal-related documentation is also available on the Liferay wiki and OpenPortal documentation sites.

◆ ◆ ◆ CHAPTER 2

About the OpenSSO Add-On

Based on the open sourceOpenSSO project and the Sun OpenSSO Enterprise (formerly known as Federated Access Manager) product, the OpenSSO Add-On provides enterprise-grade single sign-on and authentication features for Web Space Server portals and portlets.

The Add-On also provides convenience features for mapping OpenSSO and Access Manager users, roles, filtered roles, groups, and realms to Web Space Server users, communities, and organizations. This makes the Add-On particularly useful for migrating existing OpenSSO or Access Manager—based Portal Server user, role, group, and realm configurations to corresponding Web Space Server configurations.

Note – Most of the concepts and features of the OpenSSO Add-On apply equally to OpenSSO and Access Manager authentication servers. Throughout this document, except where noted, the term *OpenSSO* can be used interchangeably with the term *Access Manager*.

Who Should Use the OpenSSO Add-On?

The Web Space Server OpenSSO Add-On is intended for developers who want to implement single sign-on and authentication features in their portals and portlets in general.

In addition, the OpenSSO Add-On is useful for developers and administrators who are migrating from Portal Server to Web Space Server. In this regard, the OpenSSO Add-On is particularly useful in three scenarios:

- When upgrading a Sun Java System Portal Server 7.*x* installation to Web Space Server 10.0, the OpenSSO Add-On enables the mapping of user role-based content assignments in Portal Server to analogous community-based content assignments in Web Space Server 10.0.
- For developers and administrators familiar with Portal Server software, the OpenSSO Add-On enables you to define role-based content privileges in Web Space Server, similar to the functionality provided in Portal Server.
- When migrating an existing Portal Server user base to Web Space Server, the OpenSSO Add-On makes it possible to perform bulk imports of Portal Server user accounts into Web Space Server.

How Does the OpenSSO Add-On Work?

The OpenSSO Add-On enables the exchange of user authentication data between a Web Space Server site and an OpenSSO server. From the standpoint of a Web Space Server administrator, the OpenSSO Add-On provides a *Community Mapper* portlet, which is GUI-based administration tool for associating OpenSSO users, roles, filtered roles, groups, and realms with Web Space Server users, communities, and organizations.

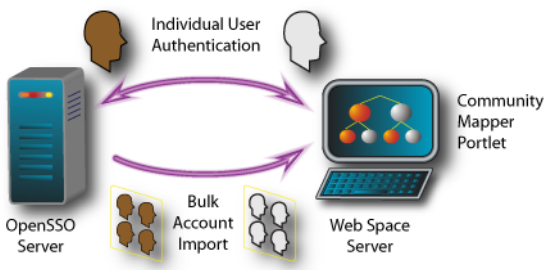


FIGURE 2–1 OpenSSO Add-On Overview

There are two general scenarios through which account information is mapped from an OpenSSO server and a Web Space Server:

- When an individual user initiates a login to a Web Space Server account
- When a Web Space Server site administrator performs a bulk import of OpenSSO accounts, often as part of a migration from Portal Server to Web Space Server

These two scenarios are described in more detail below.

Individual User Login Scenario

When an individual user connects to a Web Space Server site:

1. The attempt to connect to the Web Space Server site is redirected to the OpenSSO server for authentication.
   - If access to public pages on the Web Space Server site is allowed, then the public pages are displayed without further authentication.
   - If an attempt is made to access any Web Space Server private pages, or if the user initiates a login request by clicking the *Sign In* link on the Web Space Server page, the user is redirected to an OpenSSO login page.
2. After successful OpenSSO login, the user is redirected back to the Web Space Server page.
   - If a Web Space Server account corresponding to the account used to log in through the OpenSSO server already exists, the user is logged in to Web Space Server and is redirected to his or her home page.
   - If a corresponding Web Space Server account does not exist, a new Web Space Server account is created.
     - If the user belongs to an OpenSSO realm that is mapped to a Web Space Server organization, then his or her account is assigned to that mapped organization.
     - If the user has an OpenSSO membership (role, filtered role, or group) that is mapped to a Web Space Server community, then the user added to the mapped community, and Web Space Server content available to that community is displayed.
     - If the user's OpenSSO membership has been subsequently removed, then the user is also removed from the mapped community.
3. Once a user has been authenticated through OpenSSO, he or she is also signed on with all applications that use those OpenSSO credentials.
4. Logging out of Web Space Server or any other application that uses OpenSSO causes the user to be logged out of Web Space Server, OpenSSO, and any other application that uses those OpenSSO credentials.

Bulk User Import Scenario

In this scenario, typically performed by a Web Space Server site administrator as part of a migration from Portal Server to Web Space Server, an existing set of OpenSSO user accounts is imported in a single step. Instructions for performing a bulk user import are provided later in this guide, in "Performing Bulk Imports of OpenSSO User Accounts" on page 38.

Note – Bulk import only imports basic OpenSSO user account credentials, and does not map memberships to communities or organizations.

Default Mapping Tables

This section provides reference tables that list the default mappings used by the OpenSSO Add-On. In most cases, you will not need to refer to these tables because the Community Mapper Portlet provided by the OpenSSO Add-On uses these mappings in mostly automatic ways.

Primary Entity Mappings

Table 2–1 lists the primary entity mappings between OpenSSO and Web Space Server.

TABLE 2–1 Entity Mappings Between OpenSSO (SSO) and Web Space Server (WSS)

SSO Entity	WSS Entity	Comments
Realm	Org	Org is the "Regular" type of `org` in Web Space Server. Users inherit permissions/roles from the Organization and Location to which they belong.
User	User	
(Static) Role	Community	Map to a private community. Users can belong to any number of Communities and inherit permissions/roles from them.
Filtered Role	Community	Map to a private community.
Group	Community	Map to a private community.
N/A	Locations	This is another type of `org` in Web Space Server. An Organization to which a User belongs must be the parent of the Location to which that User belongs.
N/A	User Groups	User Groups are arbitrary collections of Users. Users can belong to any number of User Groups, and can inherit permissions/roles from User Groups. This is a grouping of users that can be used for bulk operations in Web Space Server.
N/A	Role	Roles in Web Space Server are containers for permissions.

Default User Attribute Mappings

Table 2–2 lists the user attribute mappings use to import OpenSSO (SSO) user accounts into Web Space Server (WSS). These default mappings can be changed prior to installing the OpenSSO Add-On by modifying the `portal-ext.properties` file, located in the *webspace_dir*`/webspace/opensso/templates/` directory.

TABLE 2–2 Default User Attribute Mappings

WSS Attribute	SSO Attribute
`firstName`	`cn`
`lastName`	`sn`
`screenName`	`givenName`
`emailAddress`	`mail`

Default Configuration Files

This section lists the properties and default values in the `portal-ext.properties` and `AMConfig.properties` files, which are the primary configuration files for the OpenSSO Add-On. All customization of the OpenSSO Add-On is performed through these two files. You may find it useful to refer to the tables in this section as you configure the OpenSSO for your particular Web Space Server site.

As described in "Installing the OpenSSO Add-On" on page 23, there are several site-specific modifications you must make to the `portal-ext.properties` and `AMConfig.properties` files before installing the OpenSSO Add-On. In addition, these are also the files you will need to modify if you want to make any post-installation customizations to the OpenSSO Add-On. Note that any customizations made to these files after the OpenSSO Add-On has been installed require that you also rebuild the Web Space Server WAR files, as described in "Customizing the OpenSSO Add-On" on page 41.

Locations of the `portal-ext.properties` and `AMConfig.properties` Files

The location of the `portal-ext.properties` and `AMConfig.properties` files that you should modify varies depending on whether you are performing the modifications **before** or **after** the OpenSSO Add-On has been installed.

- **Before installing the OpenSSO Add-On**

  Before installation of the OpenSSO Add-On, the `portal-ext.properties` and `AMConfig.properties` files you need to modify are located in the *glassfish_dir*`/webspace/opensso/templates` directory.

  When you first download the OpenSSO Add-On, there are two sample versions of these two files, named `portal-ext.properties.template` and `AMConfig.properties.template`. It is strongly recommended that you make copies of these template files and then only make modifications to the copies. After modifying the copies, make sure that the copies are named `portal-ext.properties` and `AMConfig.properties` (no `.template` extension) before proceeding with the OpenSSO Add-On installation.

- **After installing the OpenSSO Add-On**

  After the OpenSSO Add-On has been installed, any additional customizations you want to make must only be made to the `portal-ext.properties` and `AMConfig.properties` files that are located in the *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/classes` directory.

`portal-ext.properties` Properties File

Listed below are the properties and default values in the `portal-ext.properties` file.

- `access.manager.auth.enabled`

  Default: `true`

  Enable the OpenSSO Add-On

- `access.manager.sync.enabled`

  Default: `true`

  Enable automatic synchronization of users from OpenSSO to Web Space Server

- `access.manager.import.enabled`

  Default: `true`

  Enable the automatic import of the OpenSSO user account if the corresponding account does not already exist in Web Space Server

- `access.manager.allow.public.pages`

  Default: `true`

  Allow access to Web Space Server public pages with first being redirected to OpenSSO server for user authentication

- `access.manager.email.attr`

  Default: `mail`

  Web Space Server user email property corresponding to OpenSSO email property

- `access.manager.first.name.attr`

  Default: `givenName`

  Web Space Server user first name property corresponding to OpenSSO first name property

- `access.manager.last.name.attr`

  Default: `sn`

  Web Space Server user last name property corresponding to OpenSSO last name property

- `access.manager.screen.name.attr`

  Default: `uid`

  Web Space Server user ID property corresponding to OpenSSO user ID property

- `access.manager.login.url`

  Default:
  `http://localhost:8080/opensso/UI/Login?goto=http://localhost:8080/c/portal/login`

  URL for OpenSSO authentication login redirect; use only when authenticating through OpenSSO; enabled by default

- `access.manager.logout.url`

  Default:
  `http://localhost:8080/opensso/UI/Logout?goto=http://localhost:8080/portal`

  URL for OpenSSO authentication logout redirect; use only when authenticating through OpenSSO; enabled by default

- `access.manager.login.url`

  Default:
  `http://localhost:8080/amserver/UI/Login?goto=http://localhost:8080/c/portal/login`

  URL for Access Manger authentication login redirect; use only when authenticating through Access Manager; disabled by default

- `access.manager.logout.url`

  Default:
  `http://localhost:8080/amserver/UI/Logout?goto=http://localhost:8080/portal`

  URL for Access Manager authentication logout redirect; use only when authenticating through Access Manager; disabled by default

- `auto.login.hooks`

  Default: `com.sun.portal.security.auth.AccessManagerAutoLogin,`
  `com.liferay.portal.security.auth.CASAutoLogin,`
  `com.liferay.portal.security.auth.NtlmAutoLogin,`
  `com.liferay.portal.security.auth.OpenIdAutoLogin,`
  `com.liferay.portal.security.auth.OpenSSOAutoLogin,`
  `com.liferay.portal.security.auth.ParameterAutoLogin,`
  `com.liferay.portal.security.auth.RememberMeAutoLogin`

Classes required to enable OpenSSO autologin features; you should not need to modify these properties

- `application.startup.events`

  Default: `com.sun.portal.opensso.startup.OpenssoAddonStartupAction`

  Parameter passed to the Sun GlassFish Enterprise Server to start the OpenSSO Add-On

`AMConfig.properties` Properties File

Listed below are the properties and default values in the `AMConfig.properties` file.

- `com.iplanet.am.cookie.encode`

  Default: `true`

  Allows authentication server to *URLencode* the cookie value, converting characters to ones that are understandable by HTTP

- `com.iplanet.am.cookie.name`

  Default: `iPlanetDirectoryPro`

  Name of the persistent cookie

- `com.iplanet.am.cookie.secure`

  Default: `false`

  Set secure mode in which browser will only return the cookie when a secure protocol like HTTP(s) is used

- `com.iplanet.am.naming.url`

  Default: `http://localhost:8080/opensso/namingservice`

  URI for the authentication server naming service; use with OpenSSO

- `com.iplanet.am.notification.url`

  Default: `http://localhost:8080/opensso/notificationservice`

  URI of the authentication server notification service; allows authentication server to send notifications to registered applications when an event has occurred, and enables single sign-on cache to stay up to date; use with OpenSSO

- `com.iplanet.am.naming.url`

  Default: `http://localhost:8080/amserver/namingservice`

  URI for the authentication server naming service; use with Access Manager; disabled by default

- `com.iplanet.am.notification.url`

  Default: `http://localhost:8080/amserver/notificationservice`

URI of the authentication server notification service; use with Access Manager; disabled by default

- `com.iplanet.am.service.password`

  Default: `anonymous`

  Specifies the password of the user with permission to read OpenSSO Enterprise configuration data.

- `com.iplanet.security.encryptor`

  Default: `com.iplanet.services.util.JCEEncryption`

  Specifies the encrypting class implementation; available classes are `com.iplanet.services.util.JCEEncryption` and `com.iplanet.services.util.JSSEncryption`

- `com.iplanet.services.debug.directory`

  Default: `/var/opt/sun/identity/debug`

  Directory in which debug messages are stored

- `com.iplanet.services.debug.level`

  Default: `error`

  Severity of debug messages recorded in server log; possible values are: `off` | `error` | `warning` | `message`

- `com.sun.identity.agents.app.username`

  Default: `anonymous`

  Defines a user with permission to read the OpenSSO Enterprise configuration data

◆ ◆ ◆ CHAPTER 3

Getting and Installing the OpenSSO Add-On

This chapter explains how to download and install the OpenSSO Add-On for Web Space Server.

Before You Begin

This section explains some basic requirements and concepts you should review before proceeding with OpenSSO Add-On for Web Space Server 10.0 software installation.

System Requirements

The OpenSSO Add-On for Web Space Server 10.0 requires the following:

- **Sun GlassFish Web Space Server 10.0 software**

  The Web Space Server software should be installed as described in the *Sun GlassFish Web Space Server 10.0 Getting Started Guide*. Note that the requirements listed in "Software and Hardware Requirements" in *Sun GlassFish Web Space Server 10.0 Getting Started Guide* also apply to the OpenSSO Add-On.

  While any of the Web Space Server 10.0 packages will work with the OpenSSO Add-On, the recommended Web Space Server package for production environments is `webspace-10-fcs-for-gfv2.zip`, which is the standalone Web Space Server package that includes neither GlassFish nor the Web Space Server sample site and user sets. See the Sun

GlassFish Web Space Server page or "Getting Sun GlassFish Web Space Server Software" in *Sun GlassFish Web Space Server 10.0 Getting Started Guide* for information about the different Web Space Server 10.0 downloads.

- **Sun GlassFish Enterprise Server 2.1 software**

  Other versions of Sun GlassFish Enterprise Server software will work with Web Space Server, such as GlassFish v3 Prelude, but are recommended for evaluation or testing purposes only, rather than a production environment.

- **Authentication Server**

  A working OpenSSO or Access Manager authentication server with which you want Web Space Server to interact must be installed and configured prior to installing the OpenSSO Add-On for Web Space Server software.

  The recommended OpenSSO server version is Enterprise 8.0, which is available for download from the OpenSSO Project page. Note that this guide does *not* explain how to install or configure your authentication server.

Installation Directories

The directories in which Web Space Server and Sun GlassFish Enterprise Software may vary, so throughout these installation instructions, the root Web Space Server server installation directory is referred to as *webspace_dir*, and the Sun GlassFish Enterprise Server root directory is referred to as *glassfish_dir*.

Platform-Specific Path Separators

The instructions and examples in this document use UNIX-style forward slash (`/`) path separators in file and command names. If Web Space Server and Sun GlassFish Enterprise Server are installed on a Windows system, be sure to use backslashes (`\`) instead of forward slashes; for example:

- **UNIX systems or Linux systems** — *glassfish_dir*`/bin/asadmin`
- **Windows systems** — *glassfish_dir*`\bin\asadmin`

Getting the OpenSSO Add-On

As with all Web Space Server Add-On packages, the OpenSSO Add-On is downloaded using the Sun GlassFish Update Tool.

Note – The version of Update Tool included with some versions of GlassFish is not compatible with the Web Space Server Add-On package repositories. You must use the version of Update Tool that comes with Web Space Server 10.0 software.

Update Tool also includes a command-line (CLI) Image Packaging System (IPS) utility, called `pkg`, which provides the same core functionality as its GUI-based counterpart. This IPS tool is started with the *webspace_dir*`/bin/pkg` command. See the Update Center wiki for complete information about Update Tool and the `pkg` command.

- "To Get the OpenSSO Add-On Using the GUI-Based Update Tool" on page 19
- "To Get the OpenSSO Add-On Using the CLI-Based `pkg` Tool" on page 22

▼ To Get the OpenSSO Add-On Using the GUI-Based Update Tool

Before You Begin Make sure that Sun GlassFish Enterprise Server v2 or later and Sun GlassFish Web Space Server 10.0 are both **installed and running** on your system, as described in "System Requirements" on page 17.

In these instructions, the root Web Space Server server installation directory is referred to as *webspace_dir*, and the Sun GlassFish Enterprise Server root directory is referred to as *glassfish_dir*.

1. **In a command shell for your operating system, change to the** *webspace_dir*`/bin` **directory and run the** `updatetool` **command.**

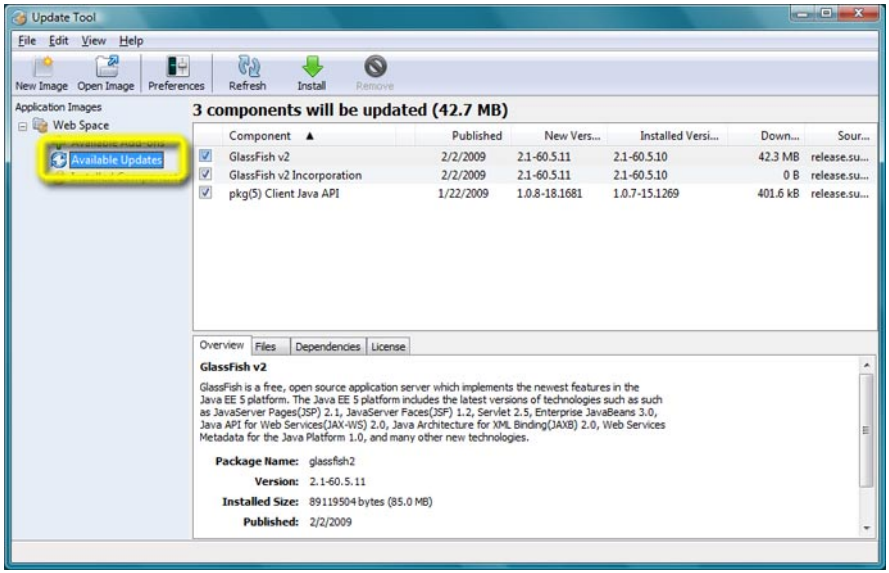
   If this is the first time you have launched `updatetool`, the full Update Tool product will not yet be installed, and you are prompted to allow installation to proceed.

   a. **Type y when prompted to install Update Tool.**

      The installer downloads and installs the full Update Tool product and then exits.

   b. **Enter the** `updatetool` **command again to launch Update Tool.**

The Update Tool main window is displayed, with Available Updates highlighted.

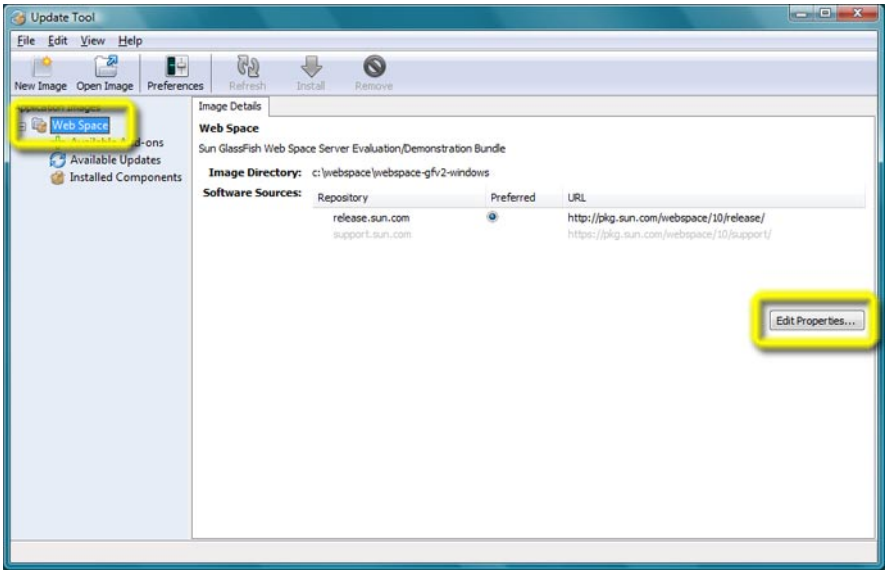


2 *(Optional)* **You can choose at this time to install any available updates.**

Note that if you choose to install updates at this time, you will in most cases need to restart GlassFish and Web Space Server before proceeding with the remainder of OpenSSO Add-On installation.

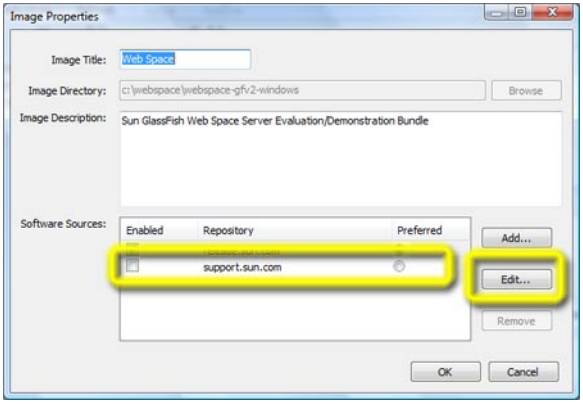
3 **Click the Web Space node in the Application Images pane on the left in Update Tool.**

Details about the currently selected software repositories are displayed. To get the Web Space Server Add-On, a restricted-access repository must be added to this list.



4 **Click *Edit Properties* on the right side of the Image Details pane.**

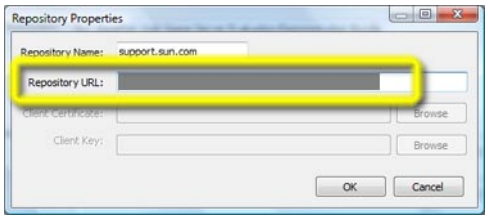
The Image Properties window is displayed.



Note that the repository named `support.sun.com` is not enabled.

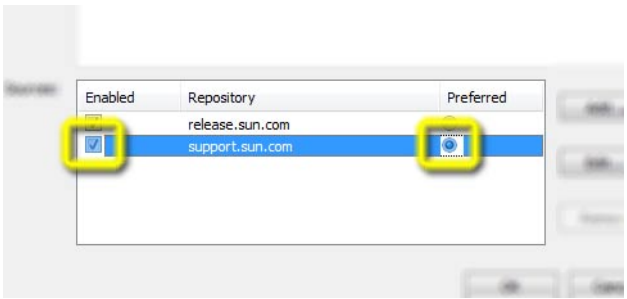
5 **Select the checkbox next to the `support.sun.com` repository, and then click *Edit*.**

The Repository Properties window is displayed.



6 **Ask your SunSolve service representative for the correct URL to use, enter the URL here, and then click *OK*.**

7 **Verify that the `support.sun.com` repository is now *Enabled* and selected as *Preferred*, and then click *OK*.**



8 **Back in the Update Tool main window, choose the *Available Add-Ons* node in the Application Images pane to display the list of available Add-On packages.**

9 **Select the packages you want, and then click *Install*.**

10 **Proceed to "Installing the OpenSSO Add-On" on page 23 for the remaining installation instructions.**

▼ To Get the OpenSSO Add-On Using the CLI-Based `pkg` Tool

Before You Begin Make sure that Sun GlassFish Enterprise Server v2 or later and Sun GlassFish Web Space Server 10.0 are both **installed and running** on your system, as described in "System Requirements" on page 17.

In these instructions, the root Web Space Server server installation directory is referred to as *webspace_dir*, and the Sun GlassFish Enterprise Server root directory is referred to as *glassfish_dir*.

1. **In a command shell for your operating system, change to the *webspace_dir*`/bin` directory and run the `updatetool` command.**

   If this is the first time you have launched `updatetool`, the full Update Tool product will not yet be installed, and you are prompted to allow installation to proceed.

2. **Type y when prompted to install Update Tool.**

   The installer downloads and installs the full Update Tool product and then exits.

3. **Change to the *webspace_dir*`/pkg/bin` directory.**

4. **Enter the following command to download the OpenSSO Add-On:**

   ```
   pkg set-authority -P --enable -O http://pkg.sun.com/webspace/10/<repository_name>
   ```

   Ask your SunSolve service representative for the correct <*repository_name*>to use, enter the URL here, and then click *OK*.

5. **Enter the following command to perform the base OpenSSO Add-On installation:**

   ```
   pkg install webspace-opensso-addon
   ```

6. **Proceed to "Installing the OpenSSO Add-On" on page 23 for the remaining installation instructions.**

Installing the OpenSSO Add-On

After using Update Tool to get the OpenSSO Add-On package, as described in "Getting the OpenSSO Add-On" on page 18, installing the package involves performing some minor configuration steps and then running an Ant script.

▼ To Install the OpenSSO Add-On

Before You Begin

- Make sure your OpenSSO server and your Web Space Server site are both **running and accessible**.
- Make note of the OpenSSO server host name, port number, and protocol used to access the OpenSSO administration application, as these will be needed later in this procedure.

1. **Change to the *webspace_dir*`/webspace/opensso/templates` directory.**

2. **Make copies of the `AMConfig.properties.template` and `portal-ext.properties.template` files, dropping the `.template` extension from the names of the copies.**

   For example:

   ```
   cp AMConfig.properties.template AMConfig.properties
   cp portal-ext.properties.template portal-ext.properties
   ```

3. **Modify the `AMConfig.properties` file, as follows:**

   a. **Comment or uncomment, as appropriate, the lines for OpenSSO or Access Manager, depending on the type of authentication server you are using.**

      The lines for OpenSSO configuration are uncommented by default. If you are instead using Access Manager, comment out the OpenSSO lines and uncomment the Access Manager lines.

   b. **Replace `localhost` with the appropriate OpenSSO host name, port number, and protocol in the two lines containing the `com.iplanet.am.*.url=` properties.**

      For example, if your OpenSSO server is `ssofoo.bar.com` running on HTTP port `7080`, you would change:

      ```
      com.iplanet.am.naming.url=http://localhost:8080/opensso/namingservice
      ```

      to:

      ```
      com.iplanet.am.naming.url=http://ssofoo.bar.com:7080/opensso/namingservice
      ```

   c. **Change `com.iplanet.am.cookie.name` from `iPlanetDirectoryPro` to the name of the cookie used by the OpenSSO server.**

4. **Modify the `portal-ext.properties` file, as follows:**

   a. **Comment or uncomment, as appropriate, the lines for OpenSSO or Access Manager, depending on the type of authentication server you are using.**

      The lines for OpenSSO configuration are uncommented by default. If you are instead using Access Manager, comment out the OpenSSO lines and uncomment the Access Manager lines.

   b. **Verify that the `access.manager.auth.enabled` property is set to `true`, and that the line is ucommented.**

   c. **Replace the first `localhost` in each `access.manager.*` property with the appropriate OpenSSO host name, port number, and protocol.**

d. Replace the second `localhost`, in each `access.manager.*` property (after the `goto` parameter), with the Web Space Server host name, port number, and protocol.

For example, if your OpenSSO server is `ssofoo.bar.com` running on HTTP port `7080`, and your Web Space Server is running on `webspace.bar.com` on port `8080`, you would change:

```
access.manager.login.url=http://localhost:8080/opensso/UI/Login? \
goto=http://localhost:8080/c/portal/login
```

to:

```
access.manager.login.url=http://ssofoo.bar.com:7080/opensso/UI/Login? \
goto=http://webspace.bar.com:8080/c/portal/login
```

(Note that these statements should each be on a single line; they are wrapped to fit the page width here.)

5 Change to the *webspace_dir*`/webspace/opensso` directory and run the `install-gfv2.xml` Ant script

```
ant -f install-gfv2.xml
```

6 Follow the prompts to complete the OpenSSO Add-On installation.

The OpenSSO installation stops the Web Space Server domain and installs the following JAR and WAR files in the *glassfish_dir*`/glassfish2/domains/`*domain_name* directory for the *domain_name* you chose during installation:

```
./applications/j2ee-modules/FAMWebSynergyMapping/WEB-INF/lib/openssoclientsdk-v1.b5.jar
./applications/j2ee-modules/opensso-web/WEB-INF/lib/opensso-web-service.jar
./applications/j2ee-modules/opensso-web/WEB-INF/lib/openssoclientsdk-v1.b5.jar
./applications/j2ee-modules/websynergy/WEB-INF/lib/opensso-login-filters.jar
./applications/j2ee-modules/websynergy/WEB-INF/lib/openssoclientsdk-8.0.b6.jar
./autodeploy/FAMWebSynergyMapping.war
./autodeploy/opensso-web.war
./autodeploy/opensso-web.war_deployed
./lib/opensso-web-service.jar
./websynergy/deploy/opensso-web.war
```

7 Restart the Web Space Server domain when the OpenSSO Add-On installation is complete.

```
cd glassfish_dir/glassfish2/bin
./asadmin start-domain domain_name
```

▼ To Uninstall the OpenSSO Add-On

1 Stop the Web Space Server domain.

2. **Change to the** *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/classes` **directory and modify the** `portal-ext.properties` **file.**

   a. **Remove the OpenSSO Add-On entry from** `application.startup.events`**:**

      ```
      com.sun.portal.opensso.startup.OpenssoAddonStartupAction
      ```

   b. **Remove all properties related to OpenSSO.**

      The complete list of properties is available in the `portal-ext.properties.template` file located in *webspace_dir*`/webspace/opensso/templates`.

3. **Change to the** *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF` **directory and remove all the** `<filter>` **and** `<filter-mapping>` **entries named** `AM Filter`**.**

4. **Change to the** *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/lib` **directory and remove the following two files:**

   - `openssoclientsdk-8.0.b6.jar`
   - `opensso-login-filters.jar`

5. **Change to the** *webspace_dir*`/var/webspace/war-workspace` **directory and run the** `synchronize.xml` **Ant script.**

   ```
   ant -f synchronize.xml
   ```

   This rebuilds the Web Space Server `webspace.war` file.

6. **Restart the Web Space Server domain and launch the Sun GlassFish Enterprise Server admin console.**

   For example:

   ```
   http://fooserver:4848
   ```

7. **Navigate to the Web Applications node and undeploy the** `communitymapperportlet.war` **and** `opensso-web.war` **applications.**

8. **Stop the Web Space Server domain.**

9. **Change to the** *glassfish_dir*`/domains/<`*webspaceserver_domain*`>/lib` **directory and remove the** `opensso-web-service.jar` **file.**

10. **Restart the Web Space Server domain.**

◆ ◆ ◆ CHAPTER 4

Using the OpenSSO Add-On

This chapter explains how to use the OpenSSO Add-On, using as a basis a sample Web Space Server with the OpenSSO Add-On and a sample OpenSSO server.

About the Examples in This Chapter

The examples used in this chapter are based on the sample site and user sets bundled with the evaluation versions of Web Space Server 10.0 software. In most cases, in actual production environments, this sample site and these user sets will not be available to you. The examples presented here are for illustration purposes only.

Refer to "Getting Sun GlassFish Web Space Server Software" in *Sun GlassFish Web Space Server 10.0 Getting Started Guide* for more information about the OpenSSO evaluation bundles.

Sample Servers Used in This Chapter

The examples in this chapter are based on a pair of sample Sun GlassFish Enterprise 2.1 server instances:

Web Space Server	Web Space Server10.0 instance running the Web Space Server sample site with the OpenSSO Add-On using a GlassFish domain named `domain1`
OpenSSO Server	OpenSSO Enterprise 8.0 authentication server using a GlassFish domain named `reasonsso`

Note – For security reasons, all URLs and domain names in screenshots in this guide have been blanked out. Similarly, none of the URLs or domain names used in the examples in this guide point to real servers.

Preparing the Web Space Server Administrator Account

One of the primary concepts to remember when working with the OpenSSO Add-On is that for a user to be able to log in to an OpenSSO-enabled Web Space Server site, he or she must have a corresponding user account on the OpenSSO server that is providing authentication services for the Web Space Server site.

With this in mind, before using the Community Mapper Portlet provided by the OpenSSO Add-On with the sample Web Space Server site used in these examples, an account corresponding to the Web Space Server sample administrator account must be created on the OpenSSO server.

▼ To Create a Web Space Server Administrator Account in OpenSSO

This task will likely be unnecessary in most Web Space Server production environments. It is only necessary in cases where the Web Space Server site administrator does not have an OpenSSO account with correspondingly sufficient privileges to perform administrative tasks on the Web Space Server site.

This example demonstrates how to create an OpenSSO account corresponding to the Web Space Server administrative account, `admin@example.com`.

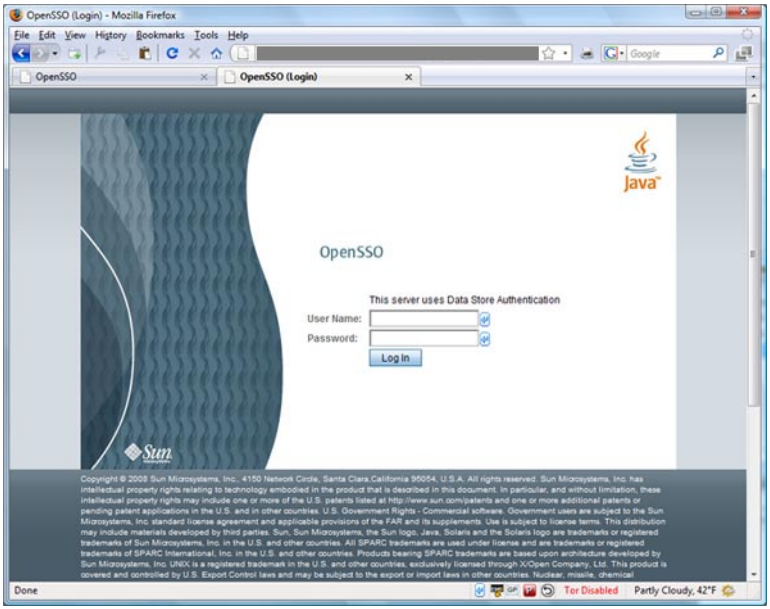
1. **Gather the credentials for the Web Space Server administrator for whom you want to create a corresponding account on the OpenSSO server.**

   In particular, make note of the user name, password, and email address.

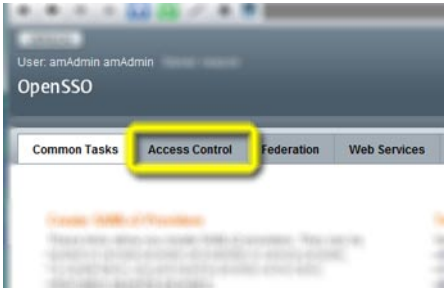
2. **Go to the URL for the your OpenSSO server and log in as the OpenSSO adminstrator.**

   For example:

   ```
   http://ssofoo.bar.com:7080/opensso
   ```

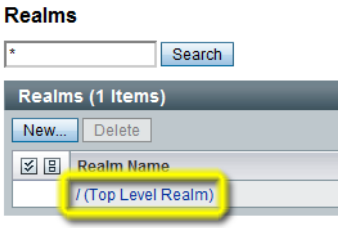


3 **In the OpenSSO Administration Console main screen, choose the *Access Control* tab.**

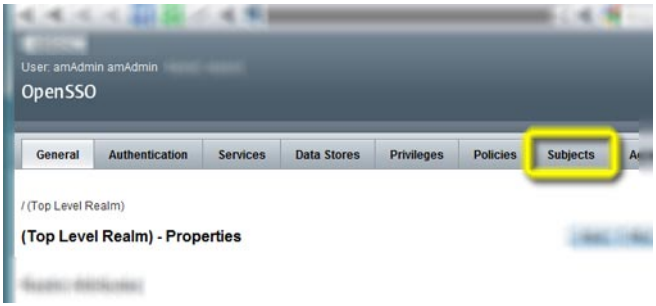


4 **Choose the name of the realm in which you want to create the Web Space Server `admin` user.**

In this example, the `/ (Top Level Realm)` is chosen.



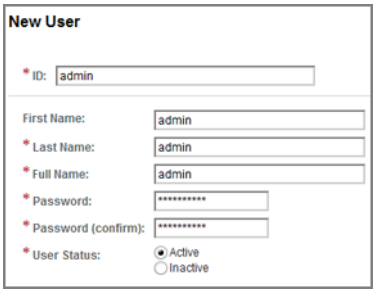
5 **On the Realm Properties page, choose the *Subjects* tab.**



6 **Make sure the *User* tab is selected, and then choose *New*.**

7 **Enter the information for the Web Space Server `admin` user, as appropriate, and then click *OK*.**

Note – Do *not* use the same password here as is defined for the `admin` user in Web Space Server.

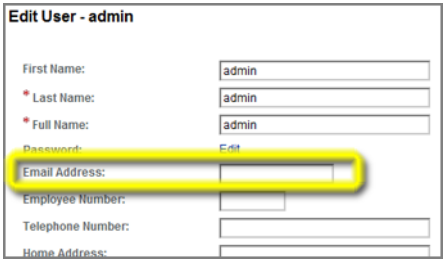


8 **Back on the Subjects->User page, click the name of the new `admin` user.**

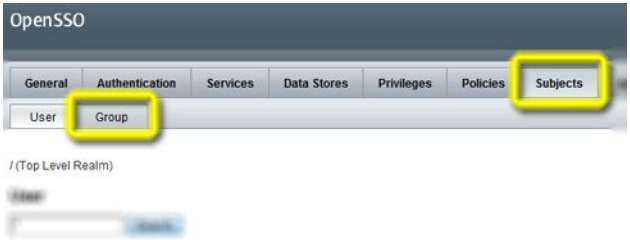
The *Edit User — admin* page is displayed.

9 **Enter additional information for the `admin` user, and then click *Save* and *Back to Subjects*.**

In this, in order to work with the Web Space Server sample site, the email address for the `admin` user, `admin@example.com`, is entered here.



10 **Back on the *Subjects* page, choose the *Group* tab.**



11 **Choose *New* to create a new group.**

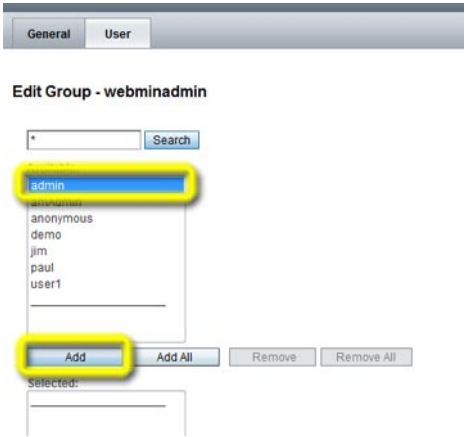
12 **Enter an ID for the new group, and then click *OK*.**

In this example, the group name `webminadmin` is used.

13 **Back on the** *Subjects->Group* **page, click the name of the new** `webminadmin` **group.**

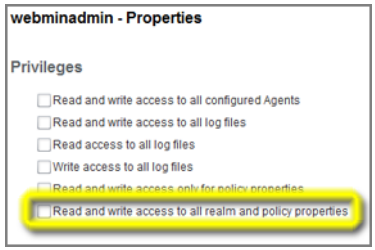
14 **On the** *Edit Group — webminadmin* **page choose the** *User* **tab.**

15 **Select the new** `admin` **user from the** *Available* **list, and then click** *Save* **and** *Back to Subjects*.



16 **Choose the** *Privileges* **tab to display the realm** *Privileges* **page.**

17 **Choose the name of the new group,** `webminadmin`**, to display the group** *Properties* **page.**



18 **Enable the bottom checkbox, "`Read and write access to all realm and policy properties`," and then choose** *Save* **and** *Back to Privileges*.

19 **Log out of the OpenSSO administration console, and log in as `admin` to the Web Space Server site using the account information you defined on the OpenSSO server.**

The admin user will now be logged in and have full administrative privileges on the Web Space Server site.

Using the Community Mapper Portlet

The Community Mapper portlet provided by the OpenSSO Add-On for Web Space Server software enables Web Space Server site administrators to:

- Map OpenSSO realm-based user roles, filtered roles, and groups to Web Space Server users and communities
- Map OpenSSO realms to Web Space Server organizations

This section explains the following procedures:

- "To Launch the Community Mapper Portlet" on page 33
- "To Map an OpenSSO Group to a Web Space Server Community" on page 35
- "To Map an OpenSSO Realm to a Web Space Server Organization" on page 36
- "To Delete a Mapping Definition" on page 37

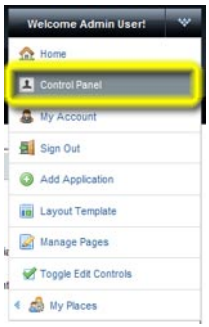
▼ To Launch the Community Mapper Portlet

Before You Begin The OpenSSO Community Mapper portlet is only available when logged in using a Web Space Server administrator account. The portlet is not available when logged in as a regular user.

1 **Log in to the Web Space Server site administrator account.**

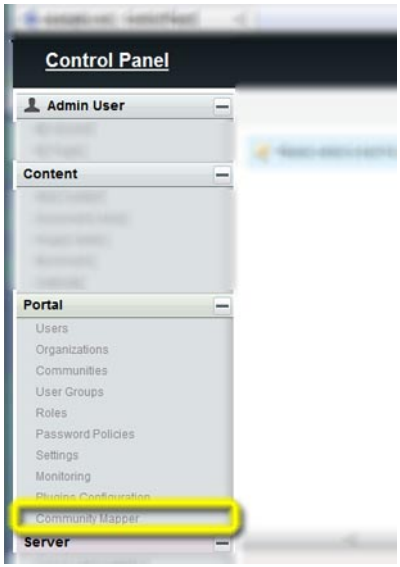
The Web Space Server site administrator Home page is displayed.

2 **Open the Web Space Server Control Panel from the Web Space Server Welcome menu.**



The administrator Control Panel page is displayed.

3 **Choose** *Community Mapper* **from the** *Portal* **section of the Control Panel menu.**



The OpenSSO Community Mapper portlet is displayed.

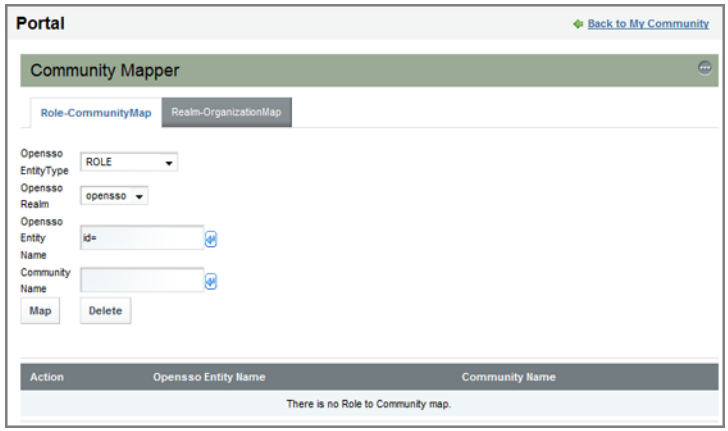


FIGURE 4–1 Community Mapper portlet

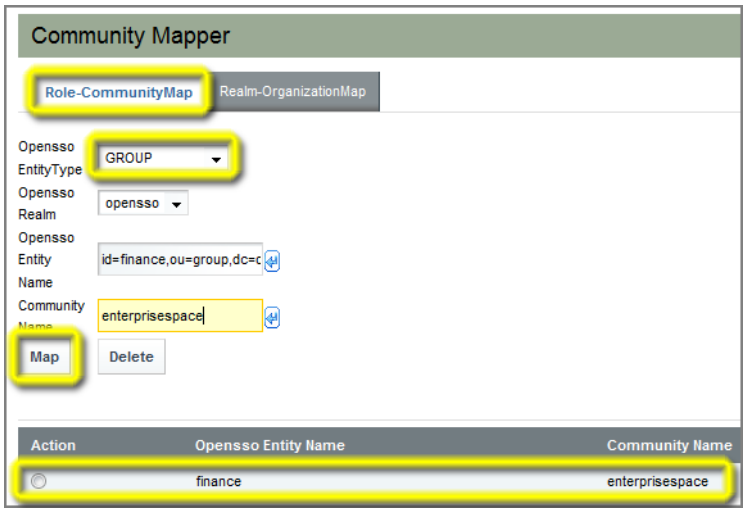
▼ To Map an OpenSSO Group to a Web Space Server Community

This procedure demonstrates how to map an OpenSSO group to a Web Space Server community. Note that, when using Access Manager or SunDS as the authentication provider, the general steps described in this procedure apply equally to mapping user roles and filtered roles to a Web Space Server community.

After mapping, any changes to the OpenSSO group or Web Space Server community will automatically be reflected in the mapped entity on the corresponding server.

1. **Launch the Community Mapper portlet, as described in "To Launch the Community Mapper Portlet" on page 33.**

2. **Make sure the *Role-CommunityMap* tab is selected, and then choose** GROUP **as the OpenSSO Entity Type.**



3 **Specify the mapping parameters you want to use.**

- **OpenSSO Realm** – Name of an existing OpenSSO realm; in this example, a realm named `opensso` is used.
- **OpenSSO Entity** – Name of an existing OpenSSO group; in this example, a group named `finance` is used. Note that a list of available groups pops up when you pause at the `id=` prefix. Note that the autocomplete feature adds the fully qualified group ID parameters; in this example, `id=finance,ou=group,dc=opensso,dc=java,dc=net`.
- **Community Name** – Name of an existing Web Space Server community; in this example, a community named `enterprisespace` is used.

4 **Click *Map* to perform the mapping.**

The mapping definition is displayed in the list at the bottom of the Community Mapper portlet.

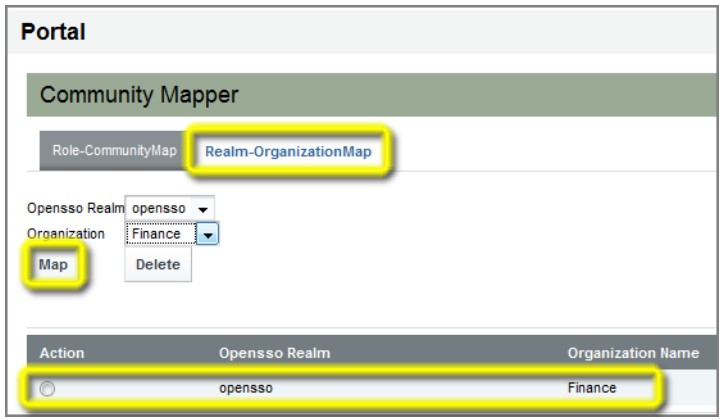
▼ To Map an OpenSSO Realm to a Web Space Server Organization

This procedure demonstrates how to map an OpenSSO realm to a Web Space Server organization.

After mapping, any changes to the OpenSSO realm or Web Space Server organization will automatically be reflected in the mapped entity on the corresponding server.

1 **Launch the Community Mapper portlet, as described in "To Launch the Community Mapper Portlet" on page 33.**

2 **Make sure the *Realm-OrganizationMap* tab is selected.**



3 **Specify the mapping parameters you want to use.**

- **OpenSSO Realm** – Name of an existing OpenSSO realm; in this example, a realm named `opensso` is used.
- **Organization Name** – Name of an existing Web Space Server organization; in this example, an organization named `Finance` is used.

4 **Click *Map* to perform the mapping.**

The mapping definition is displayed in the list at the bottom of the Community Mapper portlet.

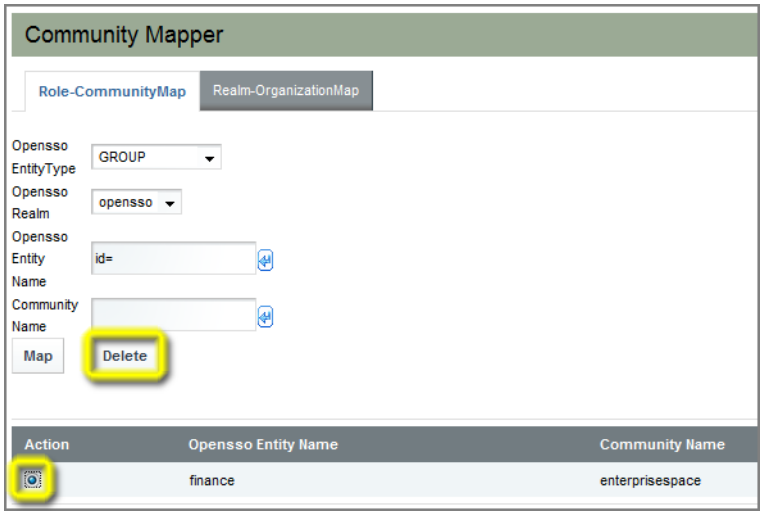
▼ To Delete a Mapping Definition

This procedure describes how to delete a Role↔Community map or a Realm↔Organization map.

1 **Launch the Community Mapper portlet, as described in "To Launch the Community Mapper Portlet" on page 33.**

2 **Choose the tab for the type of mapping you want to delete.**

3 **Select the button next to the map you want to delete in the list at the bottom of the Community Mapper pane, and then click *Delete*.**



Performing Bulk Imports of OpenSSO User Accounts

By default, the OpenSSO Add-On automatically creates a corresponding Web Space Server user account when a user logs in to Web Space Server for the first time using OpenSSO—based credentials. This one-time process can sometimes, depending on the status of the authentication server, cause an unacceptably long delay.

An alternative to this per-user import process is to perform a bulk import of user credentials. In this scenario, all user OpenSSO user accounts with parameters corresponding to an OpenSSO Add-On map in Web Space Server are automatically imported at once, before a user even attempts to log in to Web Space Server, thereby avoiding the one-time delay.

▼ To Perform a Bulk Import of OpenSSO User Accounts

This procedure uses LDAP mechanisms for the bulk import process. This procedure is typically performed only one time or infrequently, and does not related directly to OpenSSO authentication mechanisms.

Bulk imports can be performed in either of two ways:

- By directly modifying the `portal-ext.properties` file
- By using the Web Space Server Control Panel GUI

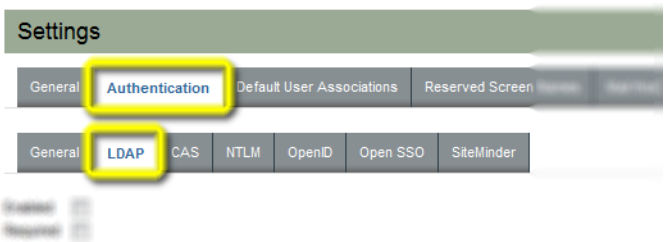
Of the two methods, using the Web Space Server Control Panel is GUI is recommended because it is simpler and less subject to error. With this in mind, this procedure describes performing a bulk import using the Web Space Server Control Panel GUI.

1 Log in to the Web Space Server site administrator account.

2 **Open the Web Space Server Control Panel from the Web Space Server Welcome menu.**

3 **Choose *Settings* from the *Portal* section in the Control Panel menu on the left.**

4 **Navigate to the *Authentication* tab, and then choose the *LDAP* tab.**



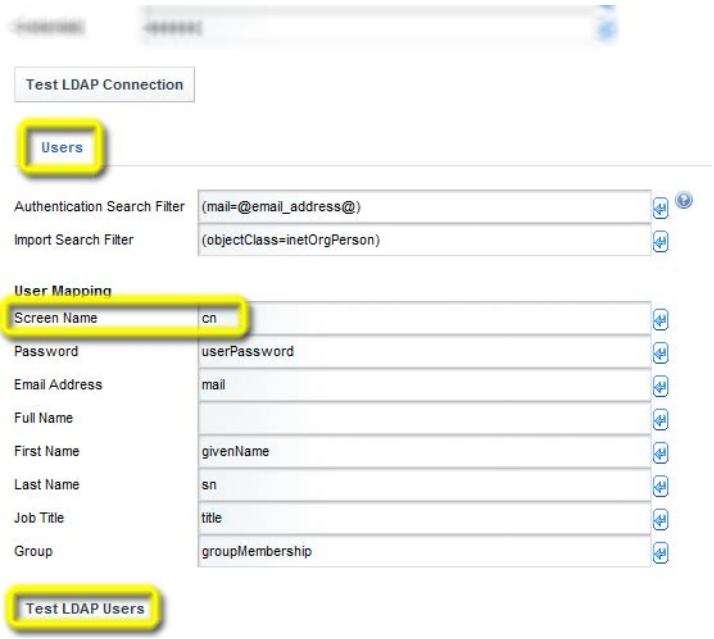
5 **Select *OpenLDAP* or *Other Directory Server* if you are using Sun Java System Directory Server.**

6 **Provide valid values for `Base Provider URL`, `Base DN`, and `Principal Credentials`, and then click *Test LDAP Connection*.**

For anonymous users, leave the `Principal` and `Credentials` fields blank.

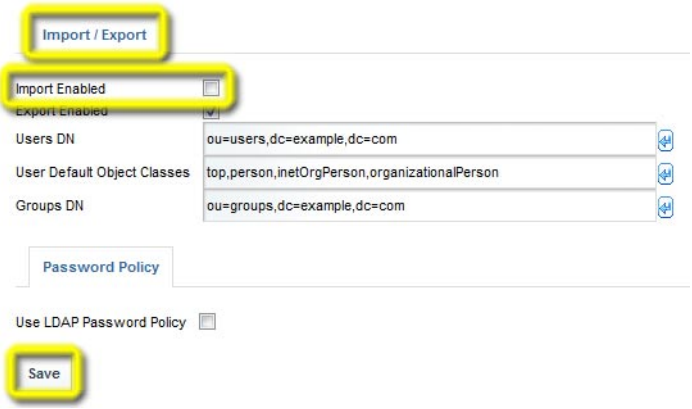
Proceed to the next step after you get a "Connection successful" message.

7 **Scroll down to the *Users* section and change the *Screen Name* from `cn` to `uid`.**



A pop-up listing all users available through LDAP should be displayed. If no users are shown, then one or more of you input parameters is incorrect. If so, correct your settings and try again. Do not proceed to the next step until a list of available users is successfully returned.

8 Scroll down to the *Import/Export* section, select *Import Enabled*, then click *Save*.



9 Log out of Web Space Server and restart the Web Space Server domain.

The user accounts will be imported when the Web Space Server domain is restarted.

Synchronizing Account Information Between OpenSSO and Web Space Server

By default, the OpenSSO Add-On enables automatic, one-way synchronization of user accounts on an OpenSSO server and a Web Space Server. For example, if a user account is deleted on the OpenSSO server, the corresponding user account is deleted in Web Space Server.

This automatic synchronization, which is enabled by default, can be disabled or enabled by means of the `access.manager.sync.enabled` property in the `portal-ext.properties` for the Web Space Server domain.

▼ To Disable or Enable Automatic Synchronization

1. **Change to the** *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/classes` **directory.**
2. **Edit the** `portal-ext.properties` **file, modifying the** `access.manager.sync.enabled` **as follows.**
   - `access.manager.sync.enabled=true` – Automatic synchronization is enabled (default)
   - `access.manager.sync.enabled=false` – Automatic synchronization is disabled
3. **Stop the Web Space Server domain.**
4. **Change to the** *webspace_dir*`/var/webspace/war-workspace` **directory.**
5. **Run the** `synchronize.xml` **Ant script.**

   ```
   ant -f synchronize.xml
   ```
6. **Restart the Web Space Server.**

Customizing the OpenSSO Add-On

Customizing the OpenSSO Add-On involves modifying the `portal-ext.properties` and `AMConfig.properties` files and then rebuilding the Web Space Server WAR files.

▼ To Customize the OpenSSO Add-On

Before You Begin After the OpenSSO Add-On has been installed, any additional customizations you want to make must only be made to the `portal-ext.properties` and `AMConfig.properties` files that are located in the *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/classes` directory. Note that this post-installation location is different than the location of the `portal-ext.properties` and `AMConfig.properties` that you should modify prior to installing the OpenSSO Add-On.

1. **Change to the** *webspace_dir*`/var/webspace/war-workspace/customs/webspace/WEB-INF/classes` **directory.**

2. **Edit the** `portal-ext.properties` **and/or** `AMConfig.properties` **file(s) as desired.**

   Refer to "Default Configuration Files" on page 11 for listings of the properties in the `portal-ext.properties` and `AMConfig.properties` files.

3. **Stop the Web Space Server domain.**

4. **Change to the** *webspace_dir*`/var/webspace/war-workspace` **directory.**

5. **Run the** `synchronize.xml` **Ant script.**

   ```
   ant -f synchronize.xml
   ```

6. **Restart the Web Space Server.**

◆ ◆ ◆ CHAPTER 5

Troubleshooting OpenSSO Issues

This chapter provides solutions to some common problems you may encounter when using the OpenSSO Add-On.

Reporting Problems With the OpenSSO Add-On

If you encounter a problem with the OpenSSO Add-On that is not listed in this chapter, contact your Sun support representative.

Known OpenSSO Add-On Issues and Limitations

Problem: Infinite redirection after two or more successful logins when OpenSSO is configured.

Solution: Enable `cookie encode true` in the OpenSSO server configuration.

Problem: After enabling the OpenSSO Add-On, cannot log in as Web Space Server administrator.

Solution: Create the "`Web Space Admin`" user in the OpenSSO server first and then try to login again.

Problem: The OpenSSO organizations are not displayed for the admin user in the Community mapping portlet.

Solution: Verify that the admin user has the `Top Level Admin Role` assigned. The steps for doing this depend on the authentication server configuration:

- **If Using OpenSSO**

  Follow the instructions for creating an admin user account in "Preparing the Web Space Server Administrator Account" on page 28.

- **If Using Access Manager or OpenSSO With Directory Server**
  1. Log in to the authentication server using the administrator account.
  2. Navigate to the name of the user you want to use as the Web Space Server administrator.
  3. Navigate to the *Roles* tab.
  4. Select the and add the `Top Level Admin` role to the user.

Problem: Forgot to update `AMConfig.properties` and `portal-ext.properties` files before running the OpenSSO Add-On installer.

Solution: Refer to the instructions in "Customizing the OpenSSO Add-On" on page 41, entering the required `AMConfig.properties` and `portal-ext.properties` properties described in "Installing the OpenSSO Add-On" on page 23.