Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Sun Java System Application Server 8.1/8.2/9.0/9.1 and GlassFish

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

Part No: 820–4578–11
November 9, 2009

091110@22749

Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Sun Java System Application Server 8.1/8.2/9.0/9.1 and GlassFish

Last update November 9, 2009

The Application Server and GlassFish policy agent is a version 3.0 Java EE agent (formerly called a J2EE agent) that functions with Sun™ OpenSSO Enterprise to protect resources deployed on Sun Java™ System Application Server 8.1/8.2/9.0/9.1 and GlassFish, the open source application server.

Contents

For general information about Java EE agents, including the new features in version 3.0 agents, see the *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for J2EE Agents*.

Note – Sun also provides version 2.2 policy agents for Application Server 8.1 and Application Server 8.2/9.0/9.1. However, to use the new version 3.0 features, you must deploy the version 3.0 agent described in this guide.

Supported Platforms, Compatibility, and Coexistence for the Application Server and GlassFish Agent

Supported Platforms for the Application Server and GlassFish Agent

The Application Server and GlassFish agent is supported on these platforms:

- Solaris OS on SPARC platforms, versions 9 and 10 (32–bit/64–bit)
- Solaris OS on x86 platforms, versions 9 and 10 (32–bit/64–bit)
- Red Hat Enterprise Linux Advanced Server 4.0 and 5.0 (32–bit/64–bit)
- Windows 2003, Enterprise Edition (32–bit/64–bit)
- Windows 2003, Standard Edition (32–bit/64–bit)

Supported Deployment Containers for the Application Server and GlassFish Agent

You can deploy the Application Server and GlassFish agent on these deployment containers:

- Sun Java System Application Server 8.1, 8.2, 9.0, and 9.1. For documentation, see:
  - Application Server 8.1: `http://docs.sun.com/coll/1343.1`
  - Application Server 8.2: `http://docs.sun.com/coll/1343.2`
  - Application Server 9.0: `http://docs.sun.com/coll/1343.3`
  - Application Server 9.1: `http://docs.sun.com/coll/1343.4`
- GlassFish:
  - Sun GlassFish: `http://www.sun.com/software/products/glassfish_portfolio/index.jsp`
  - GlassFish V2 UR2: `https://glassfish.dev.java.net/downloads/v2ur2-b04.html`
  - GlassFish V2 UR1: `https://glassfish.dev.java.net/downloads/v2ur1-b09d.html`

  For more information, see the GlassFish project: `http://glassfish.dev.java.net`

Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4

Access Manager 7.1 and Access Manager 7 2005Q4 are compatible with version 3.0 policy agents. However, because Access Manager does not support centralized agent configuration, a version 3.0 agent deployed with Access Manager must store its configuration data locally in the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files. The `OpenSSOAgentBootstrap.properties` file contains the information required for the agent to start and initialize itself.

Coexistence With Version 2.2 Policy Agents

OpenSSO Enterprise supports both version 3.0 and version 2.2 agents in the same deployment. The version 2.2 agents, however, must continue to store their configuration data locally in the `AMAgent.properties` file. And because the version 2.2 agent configuration data is local to the agent, OpenSSO Enterprise centralized agent configuration is not supported for version 2.2 agents. To configure a version 2.2 agent, you must continue to edit the agent's `AMAgent.properties` file.

For documentation about version 2.2 agents, see `http://docs.sun.com/coll/1322.1`.

Pre-Installation Tasks for the Application Server and GlassFish Agent

Setting Your `JAVA_HOME` Environment Variable

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

Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File

▼ To Download and Unzip the `appserver_v9_agent.zip` Distribution File

1. **Login into the server where you want to install the agent.**
2. **Create a directory to unzip the `appserver_v9_agent.zip` distribution file.**
3. **Download and unzip the `appserver_v9_agent.zip` distribution file from one of the following sites:**
   - Sun Downloads site under Identity Management > Policy Agents: `http://www.sun.com/download/index.jsp`
   - OpenSSO project site: `https://opensso.dev.java.net/public/use/index.html`

   The following table shows the layout after you unzip the agent distribution file.

   These files are relative to *AgentHome*`/j2ee_agents/appserver_v9_agent`, where *AgentHome* is where you unzipped the agent distribution file.

   PolicyAgent-base (also used in this guide) is *AgentHome*`/j2ee_agents/appserver_v9_agent`.

File or Directory	Description
`README.txt` and `license.txt`	Readme and license files
`/bin`	`agentadmin` and `agentadmin.bat` programs
`/config`	Template, properties, and XML files
`/data`	`license.log` file. Do not edit this file.
`/etc`	Agent application (`agentapp.war`) For information, see "Deploying the Agent Application" on page 18.
`/lib`	Required JAR files
`/locale`	Required properties files
`/install-logs`	Log files
`/sampleapp`	Policy agent sample application. For information, see "Deploying the Policy Agent Sample Application" on page 22.

Creating a Password File

A password file is an ASCII text file with only one line specifying the password in clear text. By using a password file, you are not forced to expose a password at the command line during the agent installation. When you install the WebLogic Server/Portal 10 agent using the agentadmin program, you are prompted to specify paths to following password files:

- An **agent profile password file** is required for both the agentadmin default and custom installation options.
- An **agent administrator password file** is required only if you use the custom installation option and have the `agentadmin` program automatically create the agent profile in OpenSSO Enterprise server during the installation.

▼ To Create a Password File

1. **Create an ASCII text file for the agent profile. For example:** `/tmp/as91agentpw`
2. **If you want the** `agentadmin` **program to automatically create the agent profile in OpenSSO Enterprise server during the installation, create another password file for the agent administrator. For example:** `/tmp/agentadminpw`
3. **Using a text editor, enter the appropriate password in clear text on the first line in each file.**
4. **Secure each password file appropriately, depending on the requirements for your deployment.**

Creating an Agent Administrator

An agent administrator can manage agents in OpenSSO Enterprise, including:

- **Agent management**: Use the agent administrator to manage agents either in the OpenSSO Enterprise Console or by executing the `ssoadm` utility.
- **Agent installation**: If you install the agent using the custom installation option (`agentadmin --custom-install`) and want to have the installation program create the agent profile, specify the agent administrator (and password file) when you are prompted.

▼ To Create an Agent Administrator

1. **Login to OpenSSO Enterprise Console as** `amadmin`**.**
2. **Create a new agents administrator group:**
   a. **Click** `Access Control`**,** *realm-name*`, Subjects`**, and then** `Group`**.**

b. Click `New`**.**

c. In `ID`**, enter the name of the group. For example:** `agentadmingroup`

d. Click `OK`**.**

3 Create a new agent administrator user and add the agent administrator user to the agents administrator group:

a. Click `Access Control`**,** *realm-name*, `Subjects`**, and then** `User`**.**

b. Click `New` **and provide the following values:**

- **ID**: Name of the agent administrator. For example: `agentadminuser`

  This is the name you will use to login to the OpenSSO Enterprise Console .
- **First Name** (optional), **Last Name**, and **Full Name**.

  For simplicity, use the same name for each of these values that you specified in the previous step for ID.
- **Password** (and confirmation)
- **User Status**: Active

c. Click `OK`**.**

d. Click the new agent administrator name.

e. On the `Edit User` **page, click** `Group`**.**

f. Add the agents administrator group from `Available` **to** `Selected`**.**

g. Click `Save`**.**

4 Assign read and write access to the agents administrator group:

a. Click `Access Control`**,** *realm-name*, `Privileges` **and then on the new agents administrator group link.**

b. Check `Read and write access to all configured Agents`**.**

c. Click `Save`**.**

Next Steps Login into the OpenSSO Enterprise Console as the new agent administrator. The only available top-level tab is `Access Control`. Under *realm-name*, you will see only the `Agents` tab and sub tabs.

Creating an Agent Profile

The Application Server and GlassFish agent uses an agent profile to communicate with OpenSSO Enterprise server. You can create an agent profile using any of these three methods:

- Create the agent profile during installation when you run the `agentadmin` program with the `--custom-install` option. The program prompts you for this information:
  - Agent profile name and path to the agent profile password file
  - Agent administrator name and path to the agent administrator password file
- Use the OpenSSO Enterprise Console, as described in "Creating an Agent Profile" on page 9.
- Use the `ssoadm` command-line utility with the `create-agent` subcommand. For more information about the `ssoadm` command, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

▼ To Create an Agent Profile in the OpenSSO Enterprise Console

1. **Login into the OpenSSO Enterprise Administration Console as `amAdmin`.**
2. **Click `Access Control`, *realm-name*, `Agents`, and then `J2EE`.**
3. **Under `Agent`, click `New`.**
4. **In the `Name` field, enter the name for the new agent profile. For example: `AS9Agent`**
5. **Enter and confirm the `Password`.**

   Important: This password must be the same password that you enter in the agent profile password file that you specify when you run the `agentadmin` program to install the agent.
6. **In the `Server URL` field, enter the OpenSSO Enterprise server URL.**

   For example: `http://openssohost.example.com:8080/opensso`
7. **In the `Agent URL` field, enter the URL for the agent application (`agentapp`).**

   For example: `http://agenthost.example.com:8090/agentapp`
8. **Click `Create`.**

   The console creates the agent profile and displays the `J2EE Agent` page again with a link to the new agent profile, `AS9Agent`.

   To do additional configuration for the agent profile, click this link to display the `Edit` agent page. For information about the agent configuration fields, see the Console online Help.

   If you prefer, you can also use the `ssoadm` command-line utility to edit the agent profile. For more information, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

Installing the Application Server and GlassFish Agent

Gathering Information to Install the Application Server and GlassFish Agent

The following table describes the information you will need to provide when you run the `agentadmin` program to install the Application Server and GlassFish agent. For some `agentadmin` prompts, you can accept the default value displayed by the program, if you prefer.

TABLE 1 Information Required to Install the Application Server and GlassFish Agent

Prompt Request	Description
Application Server Configuration Directory	Path to the directory used by Application Server to store its configuration files. Applies to both default and custom installation options. Default: `/var/opt/SUNWappserver/domains/domain1/config`
Application Server Instance Name	Name of the Application Server instance secured by this agent. Applies only to the custom installation option. Default: `server`
Access Manager URL	URL where OpenSSO Enterprise is running. Applies to both default and custom installation options. For example: `http://openssohost.example.com:8080/opensso`
Is the agent installed on the DAS host for a remote instance?	Default: `false` See "Installing the Application Server 9.1 / GlassFish 2.1 Agent on the Domain Administration Server (DAS)" on page 25. Applies only to the custom installation option.

TABLE 1 Information Required to Install the Application Server and GlassFish Agent *(Continued)*

Prompt Request	Description
Agent URL	Applies to both default and custom installation options. Agent protected Application Server URL For example: `http://agenthost.example.com:8090/agentapp` **Note**: The version 3.0 `agentadmin` program does not prompt you for the deployment URI for the agent application, because `/agentapp` is combined with this URL.
Encryption Key	Key used to encrypt the agent profile password. The encryption key should be at least 12 characters long. You can accept the default key or create a new key using the `agentadmin --getEncryptKey` command. Applies only to the custom installation option.
Agent Profile Name	A policy agent communicates with OpenSSO Enterprise using the name and password in the agent profile. Applies to both default and custom installation options. For information, see "Creating an Agent Profile" on page 9.
Agent profile password file	ASCII text file with only one line specifying the agent profile password. You create the agent profile password file as a pre-installation step. Applies to both default and custom installation options. For information, see "Creating a Password File" on page 7.

TABLE 1 Information Required to Install the Application Server and GlassFish Agent *(Continued)*

Prompt Request	Description
Option to create the agent profile The `agentadmin` program displays the following prompt if the agent profile previously specified for the Agent Profile Name prompt does not already exist in OpenSSO Enterprise: `Enter true if the Agent Profile is being created into OpenSSO Enterprise by the installer. Enter false if it will be not be created by installer.`	To have the installation program create the agent profile, enter `true`. The program then prompts you for: ■ Agent administrator who can create, update, or delete the agent profile. For example: `agentadmin` **Important**: To use this option, the agent administrator must already exist in OpenSSO Enterprise and must have agent administrative privileges. For information see, "Creating an Agent Administrator" on page 7. If you prefer, you can also specify `amadmin` as this user. ■ Path to the agent administrator password file. For information, see "Creating a Password File" on page 7. Applies only to the custom installation option.

Installing the Application Server and GlassFish Agent Using the `agentadmin` Program

The version 3.0 `agentadmin` program includes these installation options:

- Default install (`agentadmin --install`): The program asks a limited number of questions and uses default values for the other options. Use the default install option when the default options, as shown in Table 1, meet your deployment requirements.

  or

- Custom install (`agentadmin --custom-install`): The program asks a full set of questions similar to the version 2.2 program. Use the custom install option when you want to specify values other than the default options shown in Table 1.

Before you install the Application Server and GlassFish agent:

- An OpenSSO Enterprise server instance must be installed and running.
- The Application Server or GlassFish instance must be installed and configured on the server where you plan to install the agent.
- You must have downloaded and unzipped the distribution file, as described in "Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File" on page 6.

▼ To Install the Application Server and GlassFish Agent Using the `agentadmin` Program

1. **Login into the server where you want to install the agent.**

   Important: To install the agent, you must have write permission to the Application Server or GlassFish instance files and directories.

2. **If they are running, shut down the following server instances:**

   - Domain Administration Server (DAS) instance on the server where you want to install the agent
   - Application Server or GlassFish instance that will be protected by the agent

3. **Change to the following directory:**

   PolicyAgent-base`/j2ee_agents/appserver_v9_agent/bin`

4. **On Solaris and Linux systems, set the permissions for the `agentadmin` program as follows, if needed:**

   ```
   # chmod 755 agentadmin
   ```

5. **Start the agent installation:**

   Default install: `# ./agentadmin --install`

   or

   Custom install: `# ./agentadmin --custom-install`

   On Windows systems, run the `agentadmin.bat` program.

6. **Enter information as requested by the `agentadmin` program, or accept the default values displayed by the program.**

   After you have made your choices, the `agentadmin` program displays a summary of your responses. For example:

   ```
   ---------------------------------------------
   SUMMARY OF YOUR RESPONSES
   ---------------------------------------------
   Application Server Config Directory :
   /opt/SUNWappserver/domains/domain1/config
   Application Server Instance name : server
   OpenSSO Enterprise URL : http://openssohost.example.com:8080/opensso

   Domain Administration Server Host is remote : false
   Agent URL : http://agenthost.example.com:8090/agentapp
   Encryption Key : Hpmw1eyip3sRmUlFCKjJeQUhU5DRX3aT
   Agent Profile name : AS91Agent
   ```

```
Agent Profile Password file name : as91agentpw
Agent installed on the DAS host for a remote instance : false

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:
```

7 Verify your choices and either continue with the installation (selection 1, the default) , or make any necessary changes.

If you continue, the program installs the agent and displays a summary of the installation. For example:

```
SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/agents/j2ee_agents/appserver_v9_agent
  /Agent_001/config/OpenSSOAgentBootstrap.properties
Agent Configuration file location
/agents/j2ee_agents/appserver_v9_agent
  /Agent_001/config/OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/agents/j2ee_agents/appserver_v9_agent/Agent_001/install-logs/audit
Agent Debug directory location:
/agents/j2ee_agents/appserver_v9_agent/Agent_001/install-logs/debug

Install log file location:
/agents/j2ee_agents/appserver_v9_agent/install-logs/audit/custom.log
```

8 After the installation finishes successfully, if you wish, check the installation log file in the following directory:

PolicyAgent-base`/install-logs/audit`

9 Restart the Application Server or GlassFish instance that is being protected by the agent.

Note – After you install the Application Server and GlassFish agent for a specific domain, you cannot use that same agent on the same host for a different domain. To use the Application Server and GlassFish agent for another domain on the same host, you must install the agent specifically for that domain.

Example 1 Sample `agentadmin` Program Installation for the Application Server and GlassFish Agent

```
***************************************************************************
Welcome to the Sun OpenSSO Enterprise Policy Agent 3.0 for Sun Java
System Application Server 8.1/8.2/9.0/9.1.
***************************************************************************

Enter the complete path to the directory which is used by Application Server
to store its configuration Files. This directory uniquely identifies the
Application Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Application Server Config Directory Path
[/var/opt/SUNWappserver/domains/domain1/config]:
/opt/SUNWappserver/domains/domain1/config

Enter the name of the Application Server instance that is secured by this
Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the Application Server Instance name [server]:

Enter the URL where the OpenSSO Enterprise is running. Please include
the deployment URI also as shown below:
(http://opensso.sample.com:58080/opensso)
[ ? : Help, < : Back, ! : Exit ]
OpenSSO Enterprise URL: http://openssohost.example.com:8080/opensso

Enable this field only when the agent is being installed on a remote server
instance host.
[ ? : Help, < : Back, ! : Exit ]
Is Domain administration server host remote ? [false]:

Enter the Agent URL. Please include the deployment URI also as shown below:
(http://agent1.sample.com:1234/agentapp)
[ ? : Help, < : Back, ! : Exit ]
Agent URL: http://agenthost.example.com:8090/agentapp

Enter a valid Encryption Key.
[ ? : Help, < : Back, ! : Exit ]
Enter the Encryption Key [Hpmw1eyip3sRmUlFCKjJeQUhU5DRX3aT]:

Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: AS91Agent

Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
```

```
Enter the path to the password file: as91agentpw

Enter true only if agent is being installed on a remote instance from the
Domain Administration server host.
[ ? : Help, < : Back, ! : Exit ]
Is the agent being installed on the DAS host for a remote instance ? [false]:

-----------------------------------------------
SUMMARY OF YOUR RESPONSES
-----------------------------------------------
Application Server Config Directory :
/opt/SUNWappserver/domains/domain1/config
Application Server Instance name : server
OpenSSO Enterprise URL : http://openssohost.example.com:8080/opensso

Domain Administration Server Host is remote : false
Agent URL : http://agenthost.example.com:8090/agentapp
Encryption Key : Hpmw1eyip3sRmUlFCKjJeQUhU5DRX3aT
Agent Profile name : AS91Agent
Agent Profile Password file name : as91agentpw
Agent installed on the DAS host for a remote instance : false

Verify your settings above and decide from the choices below.
1. Continue with Installation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:

Creating a backup for file
/opt/SUNWappserver/domains/domain1/config/login.conf ...DONE.

Creating a backup for file
/opt/SUNWappserver/domains/domain1/config/server.policy ...DONE.

Adding Agent Realm to
/opt/SUNWappserver/domains/domain1/config/login.conf file ...DONE.

Adding java permissions to
/opt/SUNWappserver/domains/domain1/config/server.policy file ...DONE.

Creating directory layout and configuring Agent file for Agent_001
instance ...DONE.

Reading data from file
/agents/j2ee_agents/appserver_v9_agent/bin/as91agentpw and
encrypting it ...DONE.
```

```
Generating audit log file name ...DONE.

Creating tag swapped OpenSSOAgentBootstrap.properties file for instance
Agent_001 ...DONE.

Creating the Agent Profile AS91Agent ...DONE.

Creating a backup for file
/opt/SUNWappserver/domains/domain1/config/domain.xml ...DONE.

Adding Agent parameters to
/opt/SUNWappserver/domains/domain1/config/domain.xml file ...DONE.


SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/agents/j2ee_agents/appserver_v9_agent
  /Agent_001/config/OpenSSOAgentBootstrap.properties
Agent Configuration file location
/agents/j2ee_agents/appserver_v9_agent
  /Agent_001/config/OpenSSOAgentConfiguration.properties
Agent Audit directory location:
/agents/j2ee_agents/appserver_v9_agent/Agent_001/install-logs/audit
Agent Debug directory location:
/agents/j2ee_agents/appserver_v9_agent/Agent_001/install-logs/debug

Install log file location:
/agents/j2ee_agents/appserver_v9_agent/install-logs/audit/custom.log

Thank you for using Sun OpenSSO Enterprise Policy Agent 3.0.
```

After You Finish the Install

Agent Instance Directory

The installation program creates the following directory for each agent instance:

PolicyAgent-base/`Agent_`*nnn*

where *nnn* identifies the agent instance as `Agent_001`, `Agent_002`, and so on for each additional agent instance.

Each agent instance directory contains the following subdirectories:

- `/config` contains the configuration files for the agent instance, including `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties`.
- `/install-logs` contains the following subdirectories

- `/audit` contains local audit trail for the agent instance.
- `/debug` contains the debug files for the agent instance when the agent runs in debug mode.

Post-Installation Tasks for the Application Server and GlassFish Agent

Required Post-Installation Tasks for the Application Server and GlassFish Policy Agent

Deploying the Agent Application

The agent application (`agentapp`) is a housekeeping application used by the agent for notifications and other functions such as cross domain single sign-on (CDSSO) support.

▼ To Deploy the Agent Application

Before You Begin This application is bundled with the `appserver_v9_agent.zip` distribution file and is available as a WAR file in the following location after you unzip the file:

PolicyAgent-base`/etc/agentapp.war`

- **Deploy the agent application on the Application Server or GlassFish instance using the Application Server or GlassFish administration console or deployment command.**

  You must use the same deployment URI that you specified in the "Agent protected Application Server URL" prompt during the agent installation.

  For example, if you accepted the default value (`/agentapp`) as the deployment URI for the agent application, then use this same URI to deploy the `agentapp.war` file in the Application Server or GlassFish instance.

Installing the Agent Filter for the Application Server and GlassFishAgent

Install the agent filter by modifying the deployment descriptor of each application that you want to protect.

▼ To Install the Agent Filter

1 **Ensure that the application you want to protect is not currently deployed on the Application Server or GlassFish instance.**

If the application is deployed, undeploy it before continuing.

2 **Backup the application's `web.xml` file before modifying the descriptors.**

The backup copy can be useful if you need to uninstall the agent.

3 **Edit the application's descriptors in the `web.xml` file as follows:**

a. **Set the `<DOCTYPE>` element as shown in the following example:**

```
<!DOCTYPE web-app version="2.4"
xmlns="http://java.sun.com/xml/ns/j2ee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://java.sun.com/xml/ns/j2ee
http://java.sun.com/xml/ns/j2ee/web-app_2_4.xsd">
```

Note: Application Server and GlassFish supports the Java Servlet specification version 2.4. Version 2.4 is fully backward compatible with version 2.3. Therefore, all existing servlets should work without modification or recompilation.

b. **Add the `<filter>` elements to the deployment descriptor.**

Specify the agent filter as the first `<filter>` element and the agent filter mapping as the first `<filter-mapping>` element. For example:

```
<web-app>
...
    <filter>
        <filter-name>Agent</filter-name>
        <filter-class> com.sun.identity.agents.filter.AmAgentFilter </filter-class>
    </filter>
    <filter-mapping>
        <filter-name>Agent</filter-name>
        <url-pattern>/*</url-pattern>
        <dispatcher>REQUEST</dispatcher>
        <dispatcher>INCLUDE</dispatcher>
        <dispatcher>FORWARD</dispatcher>
        <dispatcher>ERROR</dispatcher>
    </filter-mapping>
```

```
...
</web-app>
```

4 **Deploy (or redeploy) the application on Application Server and GlassFish.**

The agent filter is added to the application.

Next Steps You can also protect an application with J2EE declarative security. To learn more about protecting your application with J2EE declarative security, consider deploying the sample application. For information, see "Deploying the Policy Agent Sample Application" on page 22.

Note – Ensure that role-to-principal mappings in container specific deployment descriptors are replaced with OpenSSO Enterprise roles or principals. To retrieve OpenSSO Enterprise roles or principals, use the OpenSSO Enterprise (or Access Manager) Console to browse the user profile.

Optional Post-Installation Tasks for the Application Server and GlassFish Agent

Changing the Password for an Agent Profile

After you install the agent, you can change the agent profile password, if required for your deployment.

▼ To Change the Password for an Agent Profile

1 **On the OpenSSO Enterprise server:**

a. **Login into the Administration Console as** `amAdmin`**.**

b. **Click** `Access Control`**,** *realm-name*`,` `Agents`**,** `J2EE`**, and then the name of the agent profile you want to update.**

The Console displays the `Edit` page for the agent profile.

c. **Enter and confirm the new unencrypted password.**

d. **Click** `Save`**.**

2. **On the server where the Application Server and GlassFish agent is installed:**

   a. **In the agent profile password file, replace the old password with the new unencrypted password.**

   b. **Change to the** *PolicyAgent-base*`/bin` **directory.**

   c. **Encrypt the new password using the** `agentadmin --encrypt` **command following this syntax.**

      `agentadmin --encrypt` *agent-instance password-file*

      For example:

      ```
      # ./agentadmin --encrypt Agent_001 /export/temp/as9agentpw
      ```

      The `agentadmin --encrypt` command returns the new encrypted password. For example:

      ```
      ASEWEJIowNBJHTv1UGD324kmT==
      ```

   d. **In the** *agent-instance*`/config/OpenSSOAgentBootstrap.properties` **file, set the following property to the new encrypted password from the previous step. For example:**

      ```
      com.iplanet.am.service.secret=ASEWEJIowNBJHTv1UGD324kmT==
      ```

   e. **Restart the Application Server or GlassFish instance that is being protected by the policy agent.**

Creating the Necessary URL Policies

If the Application Server and GlassFish agent is configured to operate in the `URL_POLICY` or `ALL` filter mode, you must create the appropriate URL policies. For instance, if Application Server and GlassFish is available on port 8080 using the HTTP protocol, you must create at minimum, a policy to allow access to the following resource:

```
http://myhost.mydomain.com:8080/agentsample
```

where `agentsample` is the context URI for the sample application.

If no policies are defined and the agent is configured to operate in the `URL_POLICY` or `ALL` filter mode, then no user is allowed access to the resources protected by the Application Server and GlassFish agent.

For information about how to create these policies using the OpenSSO Enterprise Console or command-line utilities, see the *Sun OpenSSO Enterprise 8.0 Administration Guide*.

Deploying the Policy Agent Sample Application

After you install the Application Server and GlassFish agent, consider deploying the J2EE policy agent sample application to help you better understand the key features, functions, and configuration options of J2EE agents, including:

- Single sign-on (SSO)
- Web-tier declarative security
- Programmatic security
- URL policy evaluation
- Session, policy, and profile attribute fetch

The sample application can be especially useful if you are writing a custom agent application.

After you install the Application Server and GlassFish agent, the sample application is available as:

PolicyAgent-base`/sampleapp/dist/agentsample.ear`

For information about compiling, deploying, and running the sample application, see the `readme.txt` file in the `/sampleapp` directory.

Installing and Configuring the Agent in an Application Server 9.1 or Sun GlassFish 2.1 Cluster

In this deployment scenario, you want to deploy the agent to protect Java EE applications deployed in a Sun Java System Application Server 9.1 or Sun GlassFish Enterprise Server 2.1 cluster.

Application Server 9.1 or Sun GlassFish 2.1 Cluster Deployment Scenario

The cluster deployment scenario described in this section includes the following components:

- Software or hardware load balancer. For example, the Big-IP load balancer
- Application Server 9.1 or Sun GlassFish 2.1 cluster named `agents30` with these components:
  - Domain Administration Server (DAS) on Host A

- Remote Node Agent on Host B with two Application Server 9.1 or Sun GlassFish 2.1 instances

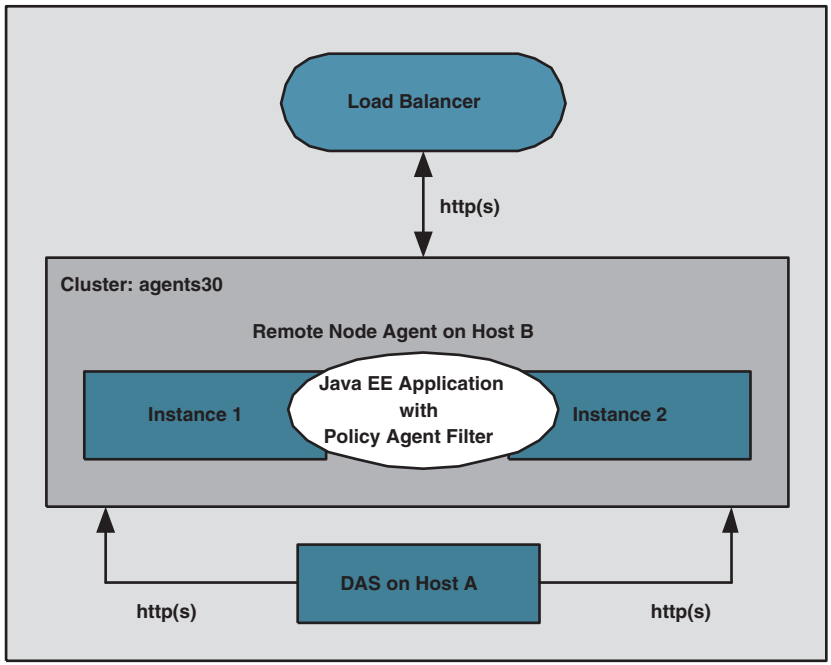

FIGURE 1 Policy Agent in an Application Server 9.1 or GlassFish 2.1 Cluster

Setting up the cluster is outside the scope of this guide. For information, see the following documentation:

- Sun GlassFish Enterprise Server 2.1:
  - Sun GlassFish Portfolio: `http://www.sun.com/software/products/glassfish_portfolio/index.jsp`
  - Sun documentation collection: `http://docs.sun.com/coll/1343.6`
- Sun Java System Application Server 9.1: `http://docs.sun.com/coll/1343.5`

Considerations for the Cluster

Several considerations for the cluster are:

- Because the cluster profile sets the admin port as non-SSL, set `AS_ADMIN_SECURE=false` in the `config/asadminenv.conf` file.

- After the cluster is setup, you are ready to install the agents. This section uses `agents30` as the cluster name with the corresponding `'agents30-config'` node in the `domain.xml` file (or `agents30-config` from the console) This configuration name is key information that you will need to configure the Application Server and GlassFish agent.
- To verify the cluster setup, access the `clusterjsp` sample application using the load balancer URL. For example:

  `http://is-lb-2.example.com:38181/clusterjsp`

Useful Commands for the Cluster

To create a password file:

```
P_FILE=/tmp/.gfpass
echo 'AS_ADMIN_ADMINPASSWORD=password' > $P_FILE
echo 'AS_ADMIN_PASSWORD=password'' >> $P_FILE
echo 'AS_ADMIN_MASTERPASSWORD=password'' >> $P_FILE
```

To create a cluster using the following names:

- Cluster name: `agents30`
- Domain name: `telco`
- Instance names: `sales` and `eng`

```
INSTALL_DIR/bin/asadmin create-domain --adminport 34848
--user admin --passwordfile $P_FILE --interactive=false --profile cluster telco

INSTALL_DIR/bin/asadmin start-domain --user admin --passwordfile $P_FILE telco

INSTALL_DIR/bin/asadmin create-node-agent --user admin --port 34848
--interactive=false --passwordfile $P_FILE telco-nodeagent

INSTALL_DIR/bin/asadmin create-cluster --port 34848 agents30

INSTALL_DIR/bin/asadmin create-instance --port 34848 --nodeagent telco-nodeagent
--systemproperties HTTP_LISTENER_PORT=38080 --cluster agents30 sales

INSTALL_DIR/bin/asadmin create-instance --port 34848 --nodeagent telco-nodeagent
--systemproperties HTTP_LISTENER_PORT=38081 --cluster agents30 eng

INSTALL_DIR/bin/asadmin start-node-agent --user admin --interactive=false
--passwordfile $P_FILE telco-nodeagent

INSTALL_DIR/bin/asadmin deploy --target agents30 --port 34848 -
-availabilityenabled=true samples/quickstart/clusterjsp/clusterjsp.ear

INSTALL_DIR/bin/asadmin start-cluster --port 34848 --interactive=false
--passwordfile $P_FILE agents30
```

To start and stop a cluster:

```
asadmin stop-cluster --port 34848 agents30
asadmin stop-node-agent
asadmin stop-domain telco

asadmin start-domain telco
asadmin start-node-agent --syncinstances=true
asadmin start-cluster agents30
```

Installing the Application Server 9.1 / GlassFish 2.1 Agent on the Domain Administration Server (DAS)

The Domain Administration Server (DAS) manages the cluster.

▼ To Install the Application Server 9.1 / GlassFish 2.1 Agent on the DAS

1. **Download and unzip the `appserver_v9_agent_3.zip` distribution file in a directory that can be accessed by the DAS instance.**

   Follow the instructions described in "Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File" on page 6.

2. **Create an agent password file, as described in "Creating a Password File" on page 7.**

3. **Stop all GlassFish domains, instances, and node agents before starting the installation process.**

   Otherwise, you might lose the OpenSSO policy agent installation changes in the DAS `domain.xml` file.

4. **Install the agent using the `agentadmin --custom-install` option, as described in "Installing the Application Server and GlassFish Agent" on page 10. The installer prompts you for the following values:**

   - `CONFIG_DIR` is the path to the GlassFish configuration directory.
   - `INSTANCE_NAME` should be the default value `server`.
   - `AM_SERVER_URL` is URL where OpenSSO server is running. For example: `http://openssohost.example.com:8080/opensso`
   - `DAS_HOST_IS_REMOTE` should be `false`.
   - `AGENT_URL` is the agent URL. For example: `http://agenthost.example.com:8090/agentapp`
   - `AGENT_ENCRYPT_KEY` is the key used to encrypt the agent profile password. Use the default value or specify a new value as described in Table 1.

- `AGENT_PROFILE_NAME` is the agent profile name. This guide uses `remotecluster` as the name.
- `AGENT_PASSWORD_FILE` is the agent profile password file, which is an ASCII text file with only one line specifying the agent profile password in plain text.
- `CREATE_AGENT_PROFILE_NAME` should be `false` in this scenario.
- `AGENT_ADMINISTRATOR_NAME` should be blank, unless you have created an agent administrator.
- `AGENT_ADMINISTRATOR_PASSWORD_FILE` should be blank, unless you have created an agent administrator and corresponding password file.
- `REMOTE_INSTANCE_LOCAL_DAS` should be `false`.
- `AGENT_INSTANCE_NAME` should be blank.
- `REMOTE_AGENT_INSTALL_DIR` should be blank.

For an example response file for a silent installation, see "Silent Agent Installation and Configuration Response File" on page 26.

5 **In the OpenSSO Console, create an agent profile, as described in "Creating an Agent Profile" on page 9.**

For the agent profile Name (`remotecluster` used in examples), Password, Server URL, and Agent URL, use same values you specified during the agent installation in the previous step. For Configuration, specify Centralized (the default).

Silent Agent Installation and Configuration Response File

The following example shows a response file named `agentinstall.inf` that you could use as input for a silent installation and configuration of the agent to the DAS instance. To use this file, invoke the following command:

```
./agentadmin custom-install useResponse agentinstall.inf
```

```
## Agent User Response File START OF FILE
CONFIG_DIR= /export/sun/gf2.1/domains/telco/config
INSTANCE_NAME= server
AM_SERVER_URL= http://openssohost.example.com:8080/opensso
DAS_HOST_IS_REMOTE= false
AGENT_URL= http://is-lb-2.example.com:38181/agentapp
AGENT_ENCRYPT_KEY= cW18Pj2R9Mt7mdvzDUL5+LMMUhm+qeIp
AGENT_PROFILE_NAME= remotecluster
AGENT_PASSWORD_FILE= /tmp/pass
CREATE_AGENT_PROFILE_NAME= false
AGENT_ADMINISTRATOR_NAME=
AGENT_ADMINISTRATOR_PASSWORD_FILE=
REMOTE_INSTANCE_LOCAL_DAS= false
AGENT_INSTANCE_NAME=
```

```
REMOTE_AGENT_INSTALL_DIR=
##Agent User Response File END OF FILE
```

Changes Made by the Agent Installer

The policy agent installer (`agentadmin`) makes following changes in the DAS instance:

- Adds the Java Class Path Suffix with the JAR and locale files of the agent to the `domain.xml` file for the `server-config` target only (because `server` was the instance name specified during the installation). This change is not made to the `default-config` or the `agents30-config` targets. This distinction is critical to make sure you properly configure the agent to protect the applications deployed on the target `agents30-config`. For example:

  ```
  ${path.separator}/export/sun/j2ee_agents/appserver_v9_agent/lib/agent.jar\$
  {path.separator}/export/sun/j2ee_agents/appserver_v9_agent/lib/openssoclientsdk.-
  jar\${path.separator}/export/sun/j2ee_agents/appserver_v9_agent/locale\$
  {path.separator}/export/sun/j2ee_agents/appserver_v9_agent/Agent_001/config
  ```

  where:

  - `/export/sun` is the base directory (`BASE_DIR`) where you unzipped the agent distribution file (`appserver_v9_agent_3.zip`).
  - `Agent_001` identifies the agent instance that was created during installation.
- Adds the JVM option for the target `server-config` to enable the policy agents logging:

  ```
  - Djava.util.logging.config.file=<BASE_DIR>/j2ee_agents/appserver_v9_agent/config/
  OpenSSOAgentLogConfig.properties
  ```
- Adds the following J2EE permissions to read the agent JAR files in the `server.policy` file:

  ```
  grant codeBase "file:<BASE_DIR>/j2ee_agents/appserver_v9_agent/lib/*" {
  permission java.security.AllPermission;
  };
  ```
- Adds the agent realm in `config/login.conf` as follows:

  ```
  agentRealm {
  com.sun.identity.agents.appserver.v81.AmASLoginModule required;
  };
  ```
- Creates a new default authentication realm named `agentRealm` for the `server` instance.

Now, you must apply these changes to the cluster configuration so the applications deployed on the cluster can be protected by the agent.

Configuring the Application Server 9.1 / GlassFish 2.1 Agent in the Cluster

This task involves running a sequence of GlassFish administrative commands using the `asadmin` command-line utility. If you also plan to use `asadmin`, make sure that the command is in your `PATH` variable. For example:

```
export PATH=/export/sun/gf2.1/bin/:$PATH
```

where `/export/sun/gf2.1` is the GlassFish installation directory.

▼ To Configure the Application Server 9.1 / GlassFish 2.1 Agent in the Cluster

1 Start the DAS instance (but not the cluster instances).

2 Login to the DAS server (Host A).

3 Copy the agents configuration and library files from the DAS instance to the cluster configuration directory so that these files will be available to the remote instances:

a. Change to the `<BASE_DIR>/j2ee_agents/appserver_v9_agent` directory, where `<BASE_DIR>` is where you unzipped the agent distribution file.

b. Copy the `config`, `lib`, and `locale` directories to the cluster configuration directory. For example:

```
/bin/cp -r Agent_001 config lib locale
${com.sun.aas.instanceRoot}/config/agents30config/
```

`Agent_001` is the agent instance created by the agent installer (`agentadmin`).

Now, you can manage the policy agent configuration files from the centralized location (in this case from the DAS). Any subsequent changes that you make in these directories must also be copied to the above location; otherwise, the cluster will not get the updates you make in the agent configuration files.

4 Create a text file named `P_FILE` containing the GlassFish administrator and master passwords. For example:

```
P_FILE=/tmp/.gfpass
echo 'AS_ADMIN_ADMINPASSWORD=adminpassword' > $P_FILE
echo 'AS_ADMIN_PASSWORD=adminpassword' >> $P_FILE
echo 'AS_ADMIN_MASTERPASSWORD=masterpassword' >> $P_FILE
```

5. **Set the logging properties. For example:**

```
./asadmin create-jvm-options --port 34848 --user admin --passwordfile $P_FILE
--target agents30config
"-Djava.util.logging.config.file=\${com.sun.aas.instanceRoot}
/config/agents30config/config/OpenSSOAgentLogConfig.properties"
```

6. **Set the compatibility mode to OFF. For example:**

```
./asadmin create-jvm-options --port 34848 --user admin --passwordfile $P_FILE
--target agents30config "-DLOG_COMPATMODE=Off"
```

7. **Create the agent authentication realm.**

```
./asadmin create-auth-realm --port 34848 --user admin --passwordfile $P_FILE
--classname com.sun.identity.agents.appserver.v81.AmASRealm
--property jaas-context=agentRealm --target agents30-config agentRealm
```

8. **Set the default realm to the agents realm. For example:**

```
./asadmin set agents30-config.security-service.default-realm=agentRealm
```

9. **Add the Classpath suffix. For example:**

```
./asadmin set agents30-config.java-config.classpath-suffix="\${path.separator}/\$
{com.sun.aas.instanceRoot}/config/agents30-config/lib/agent.jar\${path.separator}\$
{com.sun.aas.instanceRoot}/config/agents30-config/lib/openssoclientsdk.jar\${path.separator}/\$
{com.sun.aas.instanceRoot}/config/agents30-config/locale\${path.separator}\$
{com.sun.aas.instanceRoot}/config/agents30-config/Agent_001/config"
```

Note: The `$` character is escaped with a backslash (`\`), which is required when the command is executed in the shell environment.

10. **If you have enabled the Java Security Manager (that is, you have the `-Djava.security.manager` JVM option) for the cluster, you must allow permission to read the agent's JAR files located in the `{com.sun.aas.instanceRoot}/config/agents30-config/lib` directory.**

    Edit the `{com.sun.aas.instanceRoot}/config/server.policy` file and append the following lines:

```
grant codeBase "file:${com.sun.aas.instanceRoot}/config/agents30-config/lib/-" {
permission java.security.AllPermission;
};
```

11. **Deploy the agent application (`agentapp.war`) on the cluster. For example:**

```
./asadmin deploy --target agents30 --host hostA.example.com --port 34848
--availabilityenabled=true
/export/sun/j2ee_agents/appserver_v9_agent/etc/agentapp.war
```

    The agent application is required for the agent to receive notifications and to perform Cross Domain Single Sign-on (CDSSO).

12 **Restart the DAS instance and then start the cluster instances.**

Verifying the Application Server 9.1 / GlassFish 2.1 Agent in the Cluster

You can now test the cluster. This task uses the `agentsample.ear` sample application, which is in the following directory after you unzip the agent distribution file.

```
<BASE_DIR>/j2ee_agents/appserver_v9_agent/sampleapp/dist
```

▼ To Verify the Application Server 9.1 / GlassFish 2.1 Agent in the Cluster

1 **On the host where the DAS instance is running, deploy the `agentsample.ear` sample application to your cluster . For example, using `asadmin` with the `deploy` option:**

```
./asadmin deploy --target agents30 --port 34848 --availabilityenabled=true
/export/sun/j2ee_agents/appserver_v9_agent/sampleapp/dist/agentsample.ear
```

2 **On the OpenSSO server, modify the Agent Filter Mode:**

a. **Log in to the OpenSSO Administration Console.**

b. **Click `Access Control`, *realm-name*, `Agents`, `J2EE`, and then the name of the agent profile (`remotecluster`).**

c. **Under Agent Filter Mode, remove the value `ALL` and add the value `SSO_ONLY`.**

The `SSO_ONLY` value will ask only for authentication for the resource being accessed from the cluster URL, which is `http://is-lb-2.example.com:38181/agentsample/index.html`. When a user accesses this URL, the cluster will redirect the user to the OpenSSO server for authentication.

d. **Click Save.**

3 **Restart the DAS instance and cluster together with node agent to get the configuration changes propagated.**

Also, when you restart the node agent, specify the `syncinstances=true` option to have the configuration changes reflected in the remote instances.

See Also You can use the `agentsample.ear` sample application to learn more about policy agents and OpenSSO server features. For information, see "Deploying the Policy Agent Sample Application" on page 22.

Managing the Application Server and GlassFish Agent

OpenSSO Enterprise stores version 3.0 policy agent configuration data (as well as server configuration data) in a centralized repository. To manage this configuration data, use these options:

- OpenSSO Enterprise Administration Console

  You can manage both version 3.0 J2EE and web agents from the OpenSSO Enterprise Console. Tasks that you can perform include creating, deleting, updating, listing, and displaying agent configurations. Using the Console, you can set properties for an agent that you previously set by editing the agent's `AMAgent.properties` file.

  For more information, refer to the Administration Console online Help.

- `ssoadm` command-line utility

  The `ssoadm` utility is the command-line interface to OpenSSO Enterprise server and is available after you install the tools and utilities in the `ssoAdminTools.zip` file. The `ssoadm` utility includes subcommands to manage policy agents, including:

  - Creating, deleting, updating, listing, and displaying agent configurations
  - Creating deleting, listing, and displaying agent groups
  - Adding and removing an agent to and from a group

  For information about the `ssoadm` utility, including the syntax for each subcommand, see the *Sun OpenSSO Enterprise 8.0 Administration Reference*.

Managing a Version 3.0 Agent With a Local Configuration

In some scenarios, you might need to deploy a version 3.0 agent using a local configuration. For example, if you deploy the agent with Access Manager 7.1 or Access Manager 7 2005Q4, which do not support centralized agent configuration, local configuration is used by default.

The following property in the OpenSSO Enterprise server Agent Service schema (`AgentService.xml` file) indicates that the configuration is local:

```
com.sun.identity.agents.config.repository.location=local
```

In this scenario, you must manage the version 3.0 agent by editing properties in the agent's local `OpenSSOAgentConfiguration.properties` file (in the same manner that you edit the `AMAgent.properties` file for version 2.2 agents).

Caution – A version 3.0 agent also stores configuration information in the local `OpenSSOAgentBootstrap.properties` file. The agent uses information in the bootstrap file to start and initialize itself and to communicate with OpenSSO Enterprise server. In most cases, you won't need to edit the bootstrap file; however, if you do edit the file, be very careful, or the agent might not function properly.

Uninstalling the Application Server and GlassFish Agent

Preparing to Uninstall the Application Server and GlassFish Agent

▼ To Prepare to Uninstall Application Server and GlassFish Agent

1. **Undeploy any applications protected by the Application Server and GlassFish agent.**
2. **Restore the deployment descriptors of these applications to their original deployment descriptors. (Backup files are useful here if you have them.)**
3. **Conditionally, if you are permanently removing the Application Server and GlassFish agent, undeploy the agent application.**

   However, if you plan to re-install this agent , you don't need to undeploy the agent application.
4. **Ensure that the following server instances are stopped:**
   - Domain Administration Server (DAS)
   - Application Server or GlassFish instance that is being protected by the agent.

Uninstalling the Application Server and GlassFish Agent Using the `agentadmin` Program

▼ To Uninstall the Application Server and GlassFish Agent

1. **Change to the following directory:**

   PolicyAgent-base`/bin`

2. **Issue one of the following commands:**

   ```
   # ./agentadmin --uninstall
   ```

   or

   ```
   # ./agentadmin --uninstallAll
   ```

   The `--uninstall` removes only one instance of the agent, while the `--uninstallAll` option prompts you to remove all configured instances of the agent.

3. **The `uninstall` program prompts you for the Application Server configuration directory path. For example:**

   Default: `/var/opt/SUNWappserver/domains/domain1/config`

4. **The `uninstall` program displays your choices and then asks if you want to continue:**

   To continue with the uninstallation, select 1 (the default).

Example 2 Uninstallation Sample for the Application Server and GlassFish Agent

```
****************************************************************************
Welcome to the Sun OpenSSO Enterprise Policy Agent 3.0 for Sun Java
System Application Server 8.1/8.2/9.0/9.1.
****************************************************************************

Enter the complete path to the directory which is used by Application Server
to store its configuration Files. This directory uniquely identifies the
Application Server instance that is secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Application Server Config Directory Path
[/var/opt/SUNWappserver/domains/domain1/config]: /opt/SUNWappserver/domains/domain1/config

---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
Application Server Config Directory :
/opt/SUNWappserver/domains/domain1/config
```

```
Verify your settings above and decide from the choices below.
1. Continue with Uninstallation
2. Back to the last interaction
3. Start Over
4. Exit
Please make your selection [1]:

Removing Agent parameters from
/opt/SUNWappserver/domains/domain1/config/login.conf file ...DONE.

Removing java permissions from
/opt/SUNWappserver/domains/domain1/config/server.policy file ...DONE.

Removing Agent parameters from
/opt/SUNWappserver/domains/domain1/config/domain.xml file ...DONE.

Deleting the config directory
/agents/j2ee_agents/appserver_v9_agent/Agent_001/config ...DONE.

Uninstall log file location:
/agents/j2ee_agents/appserver_v9_agent/install-logs/audit/uninstall.log

Thank you for using Sun OpenSSO Enterprise Policy Agent 3.0.
```

After You Finish the Uninstall

- The `/config` directory is removed from the agent instance directory, but the `/install-logs` directory still exists.
- The `uninstall` program creates an uninstall log file in the *PolicyAgent-base*`/install-logs/audit` directory.
- The agent instance directory is not automatically removed. For example, if you uninstall the agent for Agent_001, a subsequent agent installation creates the Agent_002 instance directory. To remove an agent instance directory, you must manually remove the directory.

Migrating a Version 2.2 Policy Agent

The version 3.0 `agentadmin` program includes the new `--migrate` option to migrate a version 2.2 agent to version 3.0. After you migrate a version 2.2 agent, the agent can use the new version 3.0 agent features.

The migration process migrates the agent's binary files, updates the agent's deployment container configuration, and converts the agent's `AMAgent.properties` file to the new version 3.0 `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files.

Migrating a version 2.2 agent involves these general steps:

1. On the server where the version 2.2 agent is installed, run the version 3.0 `agentadmin` program with the `--migrate` option.

   To get the version 3.0 `agentadmin` program, you must download the version 3.0 agent that corresponds to the version 2.2 agent you are migrating. For example, if you are migrating the version 2.2 Application Server 8.2/9.0/9.1 agent, download the version 3.0 Application Server and GlassFish agent.
2. On the OpenSSO Enterprise server, run the `ssoadm` utility to create the new version 3.0 agent configuration in the centralized agent configuration repository.

   Therefore, the `ssoadm` utility must be installed from the `ssoAdminTools.zip` file on the OpenSSO Enterprise server. For information, see "Installing the OpenSSO Enterprise Utilities and Scripts" in the *Sun OpenSSO Enterprise 8.0 Installation and Configuration Guide*.

The `agentadmin` program creates a new deployment directory for the migrated agent, starting with Agent_001. The program does not modify the version 2.2 agent deployment directory files, in case you need these files after you migrate.

The following procedure, the migrated version 3.0 agent instance uses a new agent profile name, which is AS9v3Agent in the examples. The old version 2.2 and new version 3.0 agent profile passwords are the same. If you need to change the password for the new version 3.0 agent profile, see "Changing the Password for an Agent Profile" on page 20.

▼ To Migrate a Version 2.2 Agent:

1 Login to the server where the version 2.2 agent is installed.

To migrate the agent, you must have write permission to the version 2.2 agent's deployment container files and directories.

2 Stop the Application Server instance for the version 2.2 agent.

3 Create a directory to download and unzip the version 3.0 agent. For example: `v30agent`

4 Download and unzip the version 3.0 agent that corresponds to the version 2.2 agent you are migrating.

The version 3.0 agents are available from the sites listed in "Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File" on page 6.

5 Change to the version 3.0 agent's `/bin` directory.

For example, if you downloaded and unzipped the version 3.0 Application Server and GlassFish agent in the `v30agent` directory:

```
cd /v30agent/j2ee_agents/appserver_v9_agent/bin
```

6 **On Solaris and Linux systems, set the permissions for the** `agentadmin` **program as follows, if needed:**

```
# chmod 755 agentadmin
```

7 **Run the version 3.0** `agentadmin` **program with the** `--migrate` **option. For example:**

```
./agentadmin --migrate
```

8 **When the** `agentadmin` **program prompts you, enter the path to the version 2.2 agent's deployment directory. For example:**

```
...
Enter the migrated agent's deployment directory:
/opt/j2ee_agents/appserver_v9_agent
...
```

In this example, `/opt` is the directory where you downloaded and upzipped the version 2.2 agent.

The `agentadmin` program migrates the version 2.2 agent.

9 **After the** `agentadmin` **program finishes, set the following properties:**

a. **In** `Agent_`*nnn*`/config/OpenSSOAgentBootstrap.properties`**, change:**

`com.sun.identity.agents.config.username =` *new-v3.0-agent-profile-name*

For example:

```
com.sun.identity.agents.config.username = AS9v3Agent
```

10 **Copy the** `Agent_`*nnn*`/config/OpenSSOAgentConfiguration.properties` **file to the** `/bin` **directory where** `ssoadm` **is installed on the OpenSSO Enterprise server.**

11 **In** `OpenSSOAgentConfiguration.properties`**, add the un-encrypted version 2.2 agent profile password at the end of the file, as follows:**

`userpassword=`*v2.2–agent-profile-password*

12 **On OpenSSO Enterprise server, create a password file for the OpenSSO Enterprise administrator (**`amadmin`**).**

This password file is an ASCII text file with only one line specifying the `amadmin` password in plain text. For example: `/tmp/amadminpw`

13 **On OpenSSO Enterprise server, run `ssoadm` to create a new agent configuration in the OpenSSO Enterprise centralized agent configuration repository. For example:**

```
cd tools_zip_root/opensso/bin
./ssoadm create-agent -e / -b AS9v3Agent -t J2EEAgent -u amadmin
-f /tmp/amadminpw -D ./OpenSSOAgentConfiguration.properties
```

In this example:

- *tools_zip_root* is the directory where you unzipped `ssoAdminTools.zip`.
- `-e /` specifies the specifies the root realm for the agent configuration.
- `-b AS9v3Agent` specifies the version 3.0 agent configuration name.
- `-t J2EEAgent` specifies the agent type for J2EE agents.
- `-u amadmin` species the OpenSSO Enterprise administrator
- `-f /tmp/amadminpw` specifies the path to the administrator password file.
- `-D ./OpenSSOAgentConfiguration.properties` specifies the agent configuration file

Caution: After you run `ssoadm`, you might want to delete `OpenSSOAgentConfiguration.properties` from the `/bin` directory. This file contains sensitive information, including as the agent profile password, and the original file is maintained on the server where the agent is installed.

14 **Restart the Application Server and GlassFish instance for the migrated agent.**

Next Steps After you migrate the agent, you can manage the new 3.0 agent configuration using the OpenSSO Enterprise Administration Console or the `ssoadm` utility, as described in "Managing the Application Server and GlassFish Agent" on page 31.

Sun Related Information

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://wwws.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.

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. To share your comments, go to `http://docs.sun.com/` and click `Feedback`. 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 title page or in the document's URL. For example, the title of this guide is *Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Sun Java System Application Server 8.1/8.2/9.0/9.1*, and the part number is 820-4578.

Revision History

Part Number	Date	Description
820–3578–11	November 9, 2009	■ Added GlassFish to the title. ■ Added the Sun Downloads site to "Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File" on page 6. ■ Added "Installing and Configuring the Agent in an Application Server 9.1 or Sun GlassFish 2.1 Cluster" on page 22.
820–3578–10	November 11, 2008	Initial release.
820–4578–05	June 25, 2008	Early Access (EA) release draft.