



# **Sun OpenSSO Enterprise Policy Agent 3.0 Guide for BEA WebLogic Server/Portal 10**



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

Part No: 820-4580  
October 3, 2008

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

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

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

This distribution may include materials developed by third parties.

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

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

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

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

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

---

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

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

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

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

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

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

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

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

# Sun OpenSSO Enterprise Policy Agent 3.0 Guide for BEA WebLogic Server/Portal 10

---

Last revised October 3, 2008

The WebLogic Server/Portal 10 policy agent is a version 3.0 J2EE agent that functions with Sun™ OpenSSO Enterprise to protect applications and resources such as HTML files, servlets, JSPs, and EJBs deployed on BEA WebLogic® Server 10 or BEA WebLogic Portal 10.

A version 2.2 agent also exists for WebLogic Server/Portal 10. However, to use the new version 3.0 features described in [“What’s New in Version 3.0 Policy Agents” on page 4](#), you must deploy the version 3.0 WebLogic Server/Portal 10 agent.

This guide provides specific information about the WebLogic Server/Portal 10 agent, including:

- [“What’s New in Version 3.0 Policy Agents” on page 4](#)
- [“Supported Platforms, Compatibility, and Coexistence for the WebLogic Server/Portal 10 Agent” on page 5](#)
- [“Pre-Installation Tasks for the WebLogic Server/Portal 10 Agent” on page 7](#)
- [“Installing the WebLogic Server/Portal 10 Agent” on page 12](#)
- [“Post-Installation Tasks for the WebLogic Server/Portal 10 Agent” on page 21](#)
- [“Managing the WebLogic Server/Portal 10 Agent” on page 30](#)
- [“Uninstalling the WebLogic Server/Portal 10 Agent” on page 31](#)
- [“Installing and Configuring the WebLogic Server/Portal 10 Agent in a Cluster” on page 35](#)
- [“Installing and Configuring the WebLogic Server/Portal 10 Agent on WebLogic Portal 10” on page 39](#)
- [“Migrating a Version 2.2 WebLogic Server/Portal 10 Policy Agent” on page 49](#)
- [“Revision History” on page 52](#)

## What's New in Version 3.0 Policy Agents

Sun is developing version 3.0 policy agents in conjunction with OpenSSO Enterprise 8.0. The version 3.0 agents have the following new features and improvements over the version 2.2 agents:

- Centralized agent configuration

The centralized agent configuration feature moves the agent configuration properties from the `AMAgent.properties` file to the OpenSSO Enterprise centralized data repository.

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

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

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

For backward compatibility with Access Manager 7.1 and Access Manager 7 2005Q4, a version 3.0 agent supports the local configuration option. See [“Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4” on page 6](#).

- Agent types

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

- Agent groups

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

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

- More hot-swappable agent configuration properties

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

- One-level wildcard support in URL policy

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

**Default** (`agentadmin --install`): The `agentadmin` program displays a minimal number of prompts and uses default values for the other options. Use the default install option when the default options, as shown in [Table 1](#), meet your deployment requirements.

**Custom** (`agentadmin --custom-install`): The `agentadmin` program displays a full set of prompts, similar to the version 2.2 program. Use the custom install option when you want to specify values other than the default options shown in [Table 1](#), or when you want to install the agent in a WebLogic Portal domain.
- Option to create the agent profile in the server during installation

The 3.0 agent installer can create the agent profile in the OpenSSO Enterprise server during the agent installation, so you don't have to create the profile manually using the OpenSSO Enterprise Console or `ssoadm` utility.
- Automated migration support

You can migrate a version 2.2 agent to a version 3.0 agent using the `agentadmin` program with the `--migrate` option.

## Supported Platforms, Compatibility, and Coexistence for the WebLogic Server/Portal 10 Agent

- [“Supported Platforms for the WebLogic Server/Portal 10 Agent” on page 5](#)
- [“Supported Containers for the WebLogic Server/Portal 10 Agent” on page 6](#)
- [“Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4” on page 6](#)
- [“Coexistence With Version 2.2 Policy Agents” on page 7](#)

## Supported Platforms for the WebLogic Server/Portal 10 Agent

The WebLogic Server/Portal 10 agent is supported on these platforms:

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

## Supported Containers for the WebLogic Server/Portal 10 Agent

You can deploy the WebLogic Server/Portal 10 agent on these containers:

- WebLogic Server 10.0 and WebLogic Server 9.2  
Product information: [http://www.bea.com/framework.jsp?CNT=index.htm\[amp \]FP=/content/products/weblogic/server/](http://www.bea.com/framework.jsp?CNT=index.htm[amp ]FP=/content/products/weblogic/server/)  
Documentation: <http://edocs.bea.com/wls/docs100/>
- WebLogic Portal 10.2, WebLogic Portal 10, and WebLogic Portal 9.2  
Product information: [http://www.bea.com/framework.jsp?CNT=index.htm\[amp \]FP=/content/products/weblogic/portal/](http://www.bea.com/framework.jsp?CNT=index.htm[amp ]FP=/content/products/weblogic/portal/)  
Documentation: <http://edocs.bea.com/wlp/docs102/>

## 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 the centralized agent configuration feature, a version 3.0 agent deployed with Access Manager must store its configuration data locally in the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` files.

The `com.sun.identity.agents.config.repository.location` property in the OpenSSO Enterprise server Agent Service schema (`AgentService.xml` file) specifies where the agent configuration data is stored:

- `local`: Configuration data is stored locally in the `OpenSSOAgentConfiguration.properties` file on the server where the agent is deployed.
- `centralized`: Configuration data is stored in the OpenSSO Enterprise centralized data repository. This option applies to OpenSSO Enterprise only and not to Access Manager 7.1 or Access Manager 7 2005Q4.

To set this property, use either the OpenSSO Enterprise Administration Console or the `ssoadm` utility.

For both configurations, the `OpenSSOAgentBootstrap.properties` file on the server where the agent is deployed 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 WebLogic Server/Portal 10 Agent

- “Setting Your `JAVA_HOME` Environment Variable” on page 7
- “Downloading and Unzipping the WebLogic Server/Portal 10 Agent Distribution File” on page 7
- “Creating a Password File” on page 8
- “Creating an Agent Administrator” on page 9
- “Creating an Agent Profile” on page 10

## 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 want 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 WebLogic Server/Portal 10 Agent Distribution File

The distribution file for the WebLogic Server/Portal 10 agent is `weblogic_v10_agent_3.zip`.

### ▼ To Download and Unzip the Agent Distribution File

- 1 Login to the server where you want to install the agent.
- 2 Create a directory to unzip the agent distribution file.
- 3 Download and unzip the `weblogic_v10_agent_3.zip` distribution file from the OpenSSO project site:

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

The following table shows the layout after you unzip the `weblogic_v10_agent_3.zip` file. *PolicyAgent-base* is where you unzipped the distribution file.

File or Directory	Description
<i>PolicyAgent-base</i> /j2ee_agents/weblogic_v10_agent	
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 <a href="#">“Deploying the Agent Application” on page 23</a> .
/lib	Required JAR files
/locale	Required properties files
/logs	Log files
/sampleapp	Policy agent sample application. For information, see <a href="#">“Deploying the Policy Agent Sample Application” on page 28</a> .

## 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/wl10agentpw`



- 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 a Policy 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 WebLogic Server/Portal 10 agent uses an agent profile and associated password to communicate with OpenSSO Enterprise server. To create an agent profile, use any of these methods:

- Create the agent profile automatically during installation when you run the agentadmin program with the `--custom-install` option.

**Note:** To create the agent profile automatically during installation, the agentadmin program prompts you for an administrator with agent administrative privileges in OpenSSO Enterprise (and the path to the associated password file). Therefore, this user must exist in OpenSSO Enterprise before you run the agentadmin program. If you prefer, you can specify amadmin as this user.

- Use the OpenSSO Enterprise Administration Console, as described in [“To Create an Agent Profile in the OpenSSO Enterprise Console” on page 11.](#)
- 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 to the Console as `amAdmin`.**
- 2 **Click `Access Control`, `realm-name`, `Agents`, and `J2EE`.**
- 3 **Under `Agent`, click `New`.**
- 4 **In the `Name` field, enter the name for the new agent profile. For example: `WLS10Agent`**
- 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 **For `Configuration`, check the location of the agent configuration properties:**
  - **Local:** Properties are stored in the `OpenSSOAgentConfiguration.properties` file on the server where the agent is deployed.
  - **Centralized:** Properties are stored in the OpenSSO Enterprise centralized data repository. (This option applies to OpenSSO Enterprise only and not to Access Manager 7.1 or Access Manager 7 2005Q4.)
- 7 **In the `Server URL` field, enter the OpenSSO Enterprise server URL.**  
 For example: `http://openssohost.example.com:58080/opensso`
- 8 **In the `Agent URL` field, enter the URL for the agent application (`agentapp`).**  
 For example: `http://agenthost.example.com:8090/agentapp`
- 9 **Click `Create`.**  
 The console creates the agent profile and displays the `J2EE Agent` page again with a link to the new agent profile.  
 To do additional configuration for the agent, click this link to display the `Edit agent` page. For information about the agent configuration fields, see the Console online Help.

# Installing the WebLogic Server/Portal 10 Agent

- “Gathering Information to Install the WebLogic Server/Portal 10 Agent” on page 12
- “Installing the WebLogic Server/Portal 10 Agent Using the agentadmin Program” on page 14
- “Considering Specific Deployment Scenarios for the WebLogic Server/Portal 10 Agent” on page 20

## Gathering Information to Install the WebLogic Server/Portal 10 Agent

The version 3.0 agentadmin program includes these installation options:

- Default installation (agentadmin - - install): The program displays a minimal number of prompts 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 installation (agentadmin - - custom-install): The program displays a full set of prompts, similar to the version 2.2 program. Use the custom install option when you want to specify values other than the default options shown in Table 1, or when you want to install the agent in a WebLogic Portal domain.

TABLE 1 Information Required to Install the WebLogic Server/Portal 10 Agent

Prompt Request	Description
Startup script location	Path to the location of the script used to start the WebLogic domain.  Applies to both default and custom installation options.  Default: /usr/local/boa/user_projects/domains/base_domain/startWebLogic.sh
WebLogic server instance	WebLogic Server instance secured by the agent.  Applies only to the custom installation option.  Default: AdminServer
WebLogic home directory	WebLogic Server home directory.  Applies to both default and custom installation options.  Default: /usr/local/boa/wlserver_10.0

**TABLE 1** Information Required to Install the WebLogic Server/Portal 10 Agent *(Continued)*

Prompt Request	Description
OpenSSO Enterprise URL	<p>URL where OpenSSO Enterprise is running.</p> <p>Applies to both default and custom installation options.</p> <p>For example:</p> <p><code>http://openssohost.example.com:58080/opensso</code></p>
Portal domain	<p>WebLogic Portal domain</p> <p>Applies only to the custom installation option.</p> <p>Default: <code>false</code>. Specify <code>true</code> only if you are installing the agent on a WebLogic Portal domain.</p>
Deployment URI for the portal application	<p>Deployment URI for the portal application that is protected by the agent.</p> <p>Applies only to the custom installation option.</p> <p>Displayed if you answered <code>true</code> to the previous prompt, because you are installing the agent on a WebLogic Portal domain.</p>
Agent URL	<p>Agent URL, including the deployment URI.</p> <p>Applies to both default and custom installation options.</p> <p>For example: <code>http://agent.example.com:8090/agentapp</code></p>
Encryption Key	<p>Key used to encrypt the agent profile password.</p> <p>Applies only to the custom installation option.</p> <p>The encryption key should be at least 12 characters long. You can accept the default key or create a new key using the <code>agentadmin --getEncryptKey</code> command.</p>
Agent profile name	<p>Agent profile name. A policy agent communicates with OpenSSO Enterprise using the name and password in the agent profile.</p> <p>Applies to both default and custom installation options.</p> <p>For information, see <a href="#">“Creating an Agent Profile” on page 10</a>.</p>
Agent profile password file	<p>ASCII text file with only one line specifying the agent profile password.</p> <p>Applies to both default and custom installation options.</p> <p>For information, see <a href="#">“Creating a Password File” on page 8</a>.</p>

TABLE 1 Information Required to Install the WebLogic Server/Portal 10 Agent (Continued)

Prompt Request	Description
Option to create the agent profile	To have the installation program create the agent profile, enter true. The program then prompts you for:
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:	<ul style="list-style-type: none"><li>Agent administrator who can create, update, or delete the agent profile. For example: agentadmin</li></ul> <b>Important:</b> To use this option, the agent administrator must already exist in OpenSSO Enterprise and must have agent administrative privileges. For information see, “ <a href="#">Creating an Agent Administrator</a> ” on page 9. If you prefer, you can also specify amadmin as this user.
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.	<ul style="list-style-type: none"><li>Path to the agent administrator password file. For information, see “<a href="#">Creating a Password File</a>” on page 8.</li></ul>
	Applies only to the custom installation option.

## Installing the WebLogic Server/Portal 10 Agent Using the agentadmin Program

This section describes how to install the agent in a standalone environment. For information about a cluster, see “[Installing and Configuring the WebLogic Server/Portal 10 Agent in a Cluster](#)” on page 35.

**Requirements.** Before you install the WebLogic Server/Portal 10 agent:

- OpenSSO Enterprise server must be installed and accessible.
- The WebLogic Server/Portal 10 container 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 WebLogic Server/Portal 10 Agent Distribution File](#)” on page 7.

### ▼ To Install the WebLogic Server/Portal 10 Agent Using the agentadmin Program

#### 1 Login to the server where you want to install the agent.

**Important:** To install the agent, you must have write permission to the WebLogic Server/Portal 10 agent container files and directories.

#### 2 Change to the following directory:

*PolicyAgent-base/j2ee\_agents/weblogic\_v10\_agent/bin*

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

```
# chmod 755 agentadmin
```

- 4 **If necessary, stop the WebLogic Server/Portal 10 container.**

- 5 **Start the agent installation:**

Default (minimal) installation: `./agentadmin --install`

or

Custom installation: `./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.**

After you have made your choices, the agentadmin program displays a summary of your responses. For example, for an `--custom-install` installation:

```
-----
SUMMARY OF YOUR RESPONSES
-----
Startup script location :
/opt/bea/user_projects/domains/base_domain/startWebLogic.sh
WebLogic Server instance name : AdminServer
WebLogic home directory : /opt/bea/wlserver_10.0
OpenSSO Enterprise URL : http://openssohost.example.com:58080/opensso
Agent Installed on Portal domain : false
Agent URL : http://agent.example.com:8090/agentapp
Encryption Key : 6w2Tb03H0crt0cU2G5Jmphi0oY6e42Pn
Agent Profile name : WebLogicAgent
Agent Profile Password file name : /tmp/wl10agentpw
Agent Profile will be created right now by agent installer : true
Agent Administrator : agentadmin
Agent Administrator's password file name : /tmp/agentadminpw

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 (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:

/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent

/Agent\_001/config/OpenSSOAgentBootstrap.properties

Agent Configuration file location

/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent

/Agent\_001/config/OpenSSOAgentConfiguration.properties

Agent Audit directory location:

/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/Agent\_001/logs/audit

Agent Debug directory location:

/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/Agent\_001/logs/debug

Install log file location:

/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/logs/audit/custom.log

Thank you for using Sun OpenSSO Enterprise Policy Agent 3.0.

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

*PolicyAgent-base/j2ee\_agents/weblogic\_v10\_agent/logs/audit*

**9 Restart the WebLogic Server/Portal 10 container.**

---

**Note** – After you install the WebLogic Server/Portal 10 agent for a specific domain, you cannot use that same agent on the same host for a different domain. To use the WebLogic Server/Portal 10 agent for another domain on the same host, you must install the agent specifically for that domain.

---

**Example 1 Sample agentadmin - - custom - install for the WebLogic Server/Portal 10 Agent**

\*\*\*\*\*

Welcome to the Sun OpenSSO Enterprise Policy Agent 3.0 for BEA WebLogic  
10.0 Platform.

\*\*\*\*\*

Enter the path to the location of the script used to start the WebLogic domain.  
Please ensure that the agent is first installed on the admin server instance  
before installing on any managed server instance.

[ ? : Help, ! : Exit ]



```
Enter the Startup script location
[/usr/local/boa/user_projects/domains/base_domain/startWebLogic.sh]:
/opt/boa/user_projects/domains/base_domain/startWebLogic.sh

Enter the name of the WebLogic Server instance secured by the agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the WebLogic Server instance name [AdminServer]:

Enter the WebLogic home directory
[ ? : Help, < : Back, ! : Exit ]
Enter the WebLogic home directory [/usr/local/boa/wlserver_10.0]:
/opt/boa/wlserver_10.0

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:58080/opensso

Enter true if the agent is being installed on a Portal domain
[ ? : Help, < : Back, ! : Exit ]
Is the agent being installed on a Portal domain ? [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://agent.example.com:8090/agentapp

Enter a valid Encryption Key.
[ ? : Help, < : Back, ! : Exit ]
Enter the Encryption Key [6w2Tb03H0crt0cU2G5Jmphi0oY6e42Pn]:

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

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: /tmp/wl10agentpw

WARNING:
Agent profile/User: WebLogicAgent does not exist in OpenSSO!
Either "Hit the Back button, and re-enter the correct agent profile
name/user name", or "Create this agent profile when asked (available only in
custom-install)", or "Continue without validating it because agent
profile is in sub realm", or "Continue without validating/creating it, and
manually validate/create it in OpenSSO Enterprise after installation".
```

Enter true if the Agent Profile is being created into OpenSSO by the installer. Enter false if it will be not be created by installer.  
[ ? : Help, < : Back, ! : Exit ]  
This Agent Profile does not exist in OpenSSO Enterprise, will it be created by the installer? (Agent Administrator's name and password are required) [true]:

Agent Administrator is the Administrator user that can create, delete or update agent profile.

[ ? : Help, < : Back, ! : Exit ]

Enter the Agent Administrator's name: agentadmin

Enter the path to a file that contains the password of Agent Administrator

[ ? : Help, < : Back, ! : Exit ]

Enter the path to the password file that contains the password of Agent Administrator: /tmp/agentadminpw

-----  
SUMMARY OF YOUR RESPONSES  
-----

Startup script location :  
/opt/bea/user\_projects/domains/base\_domain/startWebLogic.sh  
WebLogic Server instance name : AdminServer  
WebLogic home directory : /opt/bea/wlserver\_10.0  
OpenSSO Enterprise URL :  
http://openssohost.example.com:58080/opensso  
Agent Installed on Portal domain : false  
Agent URL : http://agent.example.com:8090/agentapp  
Encryption Key : 6w2Tb03H0crt0cU2G5Jmphi0oY6e42Pn  
Agent Profile name : WebLogicAgent  
Agent Profile Password file name : /tmp/wl10agentpw  
Agent Profile will be created right now by agent installer : true  
Agent Profile type : J2EEAgent  
Agent Administrator : agentadmin  
Agent Administrator's password file name : /tmp/agentadminpw

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]:

Copy amauthprovider.jar to  
/opt/bea/wlserver\_10.0/server/lib/mbeantypes ...DONE.

Creating directory layout and configuring Agent file for Agent\_001 instance ...DONE.

Reading data from file /tmp/wl10agentpw and encrypting it ...DONE.

Generating audit log file name ...DONE.

Creating tag swapped OpenSSOAgentBootstrap.properties file for instance Agent\_001 ...DONE.

Configure  
/opt/BEA/user\_projects/domains/base\_domain/setAgentEnv\_AdminServer.sh  
...DONE.

Configure  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent  
/config/OpenSSOAgentBootstrap.properties  
...DONE.

Creating the Agent Profile WebLogicAgent ...DONE.

#### SUMMARY OF AGENT INSTALLATION

-----  
Agent instance name: Agent\_001  
Agent Bootstrap file location:  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent  
/Agent\_001/config/OpenSSOAgentBootstrap.properties  
Agent Configuration file location  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent  
/Agent\_001/config/OpenSSOAgentConfiguration.properties  
Agent Audit directory location:  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/Agent\_001/logs/audit  
Agent Debug directory location:  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/Agent\_001/logs/debug  
  
Install log file location:  
/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/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/j2ee\_agents/weblogic\_v10\_agent/Agent\_nnn*

where:

- *PolicyAgent-base* is where you unzipped the `weblogic_v10_agent_3.zip` file.
- *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`.
- `/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.

## Considering Specific Deployment Scenarios for the WebLogic Server/Portal 10 Agent

- [“Installing the Agent on Multiple WebLogic Server/Portal 10 Instances on the Same Domain” on page 20](#)
- [“Installing the Agent on a Different WebLogic Server/Portal 10 Domain” on page 20](#)

### Installing the Agent on Multiple WebLogic Server/Portal 10 Instances on the Same Domain

If the agent is installed on a particular domain, you can install the agent on more than one WebLogic Server/Portal 10 instance associated with the same domain by running the `agentadmin` program again with the `-custom-install` option. When you are prompted to enter the startup script location and WebLogic Server instance name, enter values for the new instance, so the agent can distinguish between the various instances.

### Installing the Agent on a Different WebLogic Server/Portal 10 Domain

After the agent is installed for a specific WebLogic Server/Portal 10 domain, you cannot use the same agent binary files on the same server for a different domain. If you attempt to use previously installed agent binary files on the same server but on a different domain, the installation will fail. The agent associates a specific set of agent binary files with a particular domain on WebLogic Server/Portal 10.

To install the agent on a different domain, copy the agent distribution file (`weblogic_v10_agent_3.zip`) to a different location before you install the agent on the second domain.

# Post-Installation Tasks for the WebLogic Server/Portal 10 Agent

- “Required Post-Installation Tasks for the WebLogic Server/Portal 10 Policy Agent” on page 21
- “Optional Post-Installation Tasks for the WebLogic Server/Portal 10 Agent” on page 27

## Required Post-Installation Tasks for the WebLogic Server/Portal 10 Policy Agent

- “Configuring a WebLogic Server 10 Instance With the Agent `classpath` and Java Options” on page 21
- “Deploying the Agent Application” on page 23
- “Configuring the Agent Authentication Provider for the WebLogic Server/Portal 10 Agent” on page 23
- “Adding a WebLogic Administrator to the Bypass List for the WebLogic Server/Portal 10 Agent” on page 25
- “Installing the Agent Filter for the WebLogic Server/Portal 10 Agent” on page 25

## Configuring a WebLogic Server 10 Instance With the Agent `classpath` and Java Options

This section applies to WebLogic Server 10 only. For instructions specific to WebLogic Portal 10, see “Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10” on page 40.

During the agent installation, the installer creates the following environment variable script in *domain-directory*:

- Solaris and Linux systems: `setAgentEnv_server-instance.sh`
- Windows systems: `setAgentEnv_server-instance.cmd`

where:

- *domain-directory* represents the domain name associated with the WebLogic Server 10 instance. The default path name of *domain-directory* is:  
`/usr/local/BEA/user_projects/domains/domain-name`
- *server-instance* represents the WebLogic Server 10 instance name entered during installation. For example: `server1` or `server2`.

The agent environment variable script is called during the server's startup sequence and sets the `classpath` and Java options for the agent.

## ▼ To Configure a WebLogic Server 10 Instance With the Agent classpath and Java Options

### 1 Using a text editor, edit the following WebLogic Server 10 instance startup script, depending on your platform:

- Solaris and Linux systems: *domain-directory*/bin/startWebLogic.sh
- Windows systems: *domain-directory*\bin\startWebLogic.cmd

*domain-directory* represents the domain name associated with the WebLogic Server 10 instance.

### 2 Add the path of the agent environment variable script to the WebLogic Server 10 startup script:

- Solaris and Linux systems: After the line, `. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*`, add the path:

```
. domain-directory/setAgentEnv_${SERVER_NAME}.sh
```

For example, for a domain directory named `base_domain`:

```
. /usr/local/boa/user_projects/domains/base_domain/setAgentEnv_${SERVER_NAME}.sh
```

Therefore, the startup script would then contain these two lines:

```
. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*  
. /usr/local/boa/user_projects/domains/base_domain/setAgentEnv_${SERVER_NAME}.sh
```

- Windows systems: After the line, `call "%DOMAIN_HOME%\bin\setDomainEnv.cmd" %*`, add the path:

```
call "domain-directory\setAgentEnv_%SERVER_NAME%.cmd"
```

For example, for a domain directory named `base_domain`:

```
call  
"C:\boa\user_projects\domains\base_domain\setAgentEnv_%SERVER_NAME%.cmd"
```

Therefore, the startup script would then contain these two lines:

```
call "%DOMAIN_HOME%\bin\setDomainEnv.cmd" %*  
call "C:\boa\user_projects\domains\base_domain\setAgentEnv_%SERVER_NAME%.cmd"
```

The `${SERVER_NAME}` or `%SERVER_NAME%` variable represents the WebLogic Server 10 instance and is dynamically replaced when the script is executed.

### 3 Restart the WebLogic Server 10 instance.

## Deploying the Agent Application

This section applies to both WebLogic Server 10 and WebLogic Portal 10. The agent application (agentapp.war) 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 weblogic\_v10\_agent\_3.zip distribution file and is available as a WAR file in the following location after you unzip the file:

*PolicyAgent-base/j2ee\_agents/weblogic\_v10\_agent/etc/agentapp.war*

- **Deploy the agent application on the WebLogic Server/Portal 10 container using the WebLogic Server/Portal 10 administration console or deployment command.**

You must use the same deployment URI that you specified for 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 WebLogic Server/Portal 10 container.

## Configuring the Agent Authentication Provider for the WebLogic Server/Portal 10Agent

This section applies only to WebLogic Server 10. For instructions specific to WebLogic Portal 10, see “[Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10](#)” on page 40.

Using the security service provider API provided by WebLogic Server 10, the agent plugs its custom security authenticator into the container. Once the Agent Authenticator is configured, all requests call it. You need to set the Agent Authenticator only once per WebLogic Server 10 domain.

For more information about WebLogic Server 10 security providers, see <http://e-docs.bea.com/wls/docs100/dvspisec/intro.html>.

Add the authentication provider using the WebLogic Server 10 Administration Console.

### ▼ To Configure the Agent Authentication Provider for WebLogic Server 10

- 1 **Log in to the WebLogic Server 10 Administration Console.**
- 2 **In the left pane, under Domain Structure and under the host name of the server you are configuring, click Security realms.**

- 3 In the right pane, click the name of the realm you are configuring.**
- 4 Click Providers.**
- 5 Click the Authentication tab.**
- 6 In the left pane, click Lock & Edit.**
- 7 In the right pane, click New.**
- 8 Specify Type as AgentAuthenticator.**
- 9 Specify Name with a name of your choice.**
- 10 Click OK.**
- 11 Click the newly created policy agent authentication provider.**
- 12 Change the control flag value to OPTIONAL.**
- 13 Click Save.**
- 14 Click Providers.**  
The Authentication Providers Table appears.
- 15 Click Default Authenticator.**
- 16 Change the control flag to OPTIONAL.**
- 17 Click Save.**
- 18 In the left pane, click Activate changes.**
- 19 Restart the WebLogic Server 10 instance for the changes to take effect.**

#### **More Information** Default Security Realm

If you create a new security realm instead of using the default security realm to configure the agent, ensure that the control flag value for the Agent Authenticator and any additional authentication providers are set to OPTIONAL.



## Adding a WebLogic Administrator to the Bypass List for the WebLogic Server/Portal 10 Agent

This section applies to both WebLogic Server 10 and WebLogic Portal 10. After you complete this task, the WebLogic administrator you add can bypass the authentication process for the OpenSSO Enterprise realm.

### ▼ To Add a WebLogic Administrator to the Bypass List for the WebLogic Server/Portal 10 Agent

- 1 **Login to the OpenSSO Enterprise Console as `amadmin`.**
- 2 **Under Access Control, *realm-name*, Agents, and J2EE, click the name of the agent profile you want to update.**  
The Console displays the Edit page for the agent profile.
- 3 **Click Miscellaneous and then Bypass Principal List.**
- 4 **Enter the WebLogic administrator name in New Value and click Add.**
- 5 **Click Save.**

#### More Information Using the `ssoadm` Utility

If you prefer to set this option using `ssoadm`, set the `com.sun.identity.agents.config.bypass.principal` property. This property is hot-swappable, so you do not need to restart the WebLogic Server/Portal 10 container after you set the property.

## Installing the Agent Filter for the WebLogic Server/Portal 10 Agent

This section applies to both WebLogic Server 10 and WebLogic Portal 10. 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 WebLogic Server/Portal 10.**  
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:** WebLogic Server/Portal 10 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 `<filter>`, `<filter-mapping>`, and `<dispatcher>` elements immediately after the `<web-app>` 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 WebLogic Server/Portal 10.

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 28](#).

---

**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 Console to browse the user profile. For more information, see [“Mapping OpenSSO Enterprise Roles to Principal Names” on page 29](#).

---

## Optional Post-Installation Tasks for the WebLogic Server/Portal 10 Agent

- [“Changing the Password for an Agent Profile” on page 27](#)
- [“Creating the Necessary URL Policies” on page 28](#)
- [“Deploying the Policy Agent Sample Application” on page 28](#)
- [“Mapping OpenSSO Enterprise Roles to Principal Names” on page 29](#)

### Changing the Password for an Agent Profile

This section applies to both WebLogic Server 10 and WebLogic Portal 10. 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 to the Administration Console as `amAdmin`.
  - b. Under Access Control, *realm-name*, Agents, and J2EE, click 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 WebLogic Server/Portal 10 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/j2ee\_agents/weblogic\_v10\_agent/bin* directory.  
*PolicyAgent-base* is where you unzipped the `weblogic_v10_agent_3.zip` distribution file.

- 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 /tmp/wl10agentpw
```

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 WebLogic Server/Portal 10 container.**

## Creating the Necessary URL Policies

This section applies only to WebLogic Server 10. For instructions specific to WebLogic Portal 10, see [“Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10” on page 40](#).

If the WebLogic Server 10 agent is configured to operate in the `URL_POLICY` or `ALL` filter mode, you must create the appropriate URL policies. For instance, if WebLogic Server 10 is available on port 8080 using the HTTP protocol, you must create at minimum, a policy to allow access to the sample application. For example:

```
http://agenthost.example.com:8090/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 WebLogic Server 10 agent.

For information about how to create these policies using the OpenSSO Enterprise Console or `ssoadm` utility, see the *Sun OpenSSO Enterprise 8.0 Administration Guide*.

## Deploying the Policy Agent Sample Application

This section applies to both WebLogic Server 10 and WebLogic Portal 10.

After you install the WebLogic Server/Portal 10 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 WebLogic Server/Portal 10 agent, the sample application is available as:

*PolicyAgent-base/j2ee\_agents/weblogic\_v10\_agent/sampleapp/dist/agentsample.ear*

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

## Mapping OpenSSO Enterprise Roles to Principal Names

This section applies only to WebLogic Server 10. If the agent is set to the J2EE\_POLICY filter mode, map OpenSSO Enterprise roles to the principal names in the respective application's deployment descriptor file(s):

- *weblogic.xml*
- *weblogic-ejb-jar.xml*

OpenSSO Enterprise roles are represented in UUIDs. Ensure that the keys in the mapping are UUIDs corresponding to your site's OpenSSO Enterprise installation. A UUID for a OpenSSO Enterprise role is mapped to the respective principal name in the *weblogic.xml* or *weblogic-ejb-jar.xml* file. Specifically, the principal name is located within the `<principal-name>` element.

To configure the WebLogic Server/Portal 10 agent to use privileged attribute mapping, use one of these methods:

- In the OpenSSO Enterprise Administration Console:
  1. Login to the Console as *amadmin*.
  2. Under Access Control, *realm-name*, Agents, and J2EE, click the name of the agent profile you want to update.

The Console displays the Edit page for the agent profile.
  3. Under Application, click **Privilege Attributes Processing**.
  4. For **Enable Privileged Attribute Mapping**, check **Enabled**.
  5. In the **Privileged Attribute Mapping** list, Add the mapping entries.
  6. When you are finished, click **Save**.

or

- Use the *ssoadm* utility to set the these properties:

```
com.sun.identity.agents.config.privileged.attribute.mapping.enable=true
com.sun.identity.agents.config.privileged.attribute.mapping[id=manager,
ou=group,dc=example,dc=com]=am_manager_role
```

Starting with WebLogic Server 9.0, a principal name in the `weblogic.xml` file or `weblogic-ejb-jar.xml` file must use the NMToken format, which is mandated by the corresponding schema files. Access Manager UUIDs include the following characters: equal sign (=), comma (,), and ampersand (&).

## Managing the WebLogic Server/Portal 10 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 available on the OpenSSO Enterprise server 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
- Set agent configuration properties

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, you deploy the agent with Access Manager 7.1 or Access Manager 7 2005Q4, which do not support centralized agent configuration.

To set the WebLogic Server/Portal 10 agent to use a local configuration, use one of these methods:

- In the OpenSSO Enterprise Administration Console, on the Edit *agent-name* page, set Location of Agent Configuration Repository to local.
- or
- Use the `ssoadm` utility to set the following property:  
`com.sun.identity.agents.config.repository.location=local`

Then, 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 careful, or the agent might not function properly.

## Uninstalling the WebLogic Server/Portal 10 Agent

- [“Preparing to Uninstall the WebLogic Server/Portal 10 Agent” on page 31](#)
- [“Uninstalling the WebLogic Server/Portal 10 Agent Using the agentadmin Program” on page 33](#)

## Preparing to Uninstall the WebLogic Server/Portal 10 Agent

- [“Removing the Agent Authentication Provider” on page 31](#)
- [“To Remove the Agent Authentication Provider” on page 31](#)
- [“Unconfiguring the WebLogic Server/Portal 10 Agent” on page 32](#)

### Removing the Agent Authentication Provider

To remove the Agent Authentication Provider that was configured after the agent was installed, use the WebLogic Server/Portal 10 Administration Console.

#### ▼ To Remove the Agent Authentication Provider

- 1 Login to the WebLogic Server/Portal 10 Administration Console.
- 2 In the left pane, under Domain Structure and under the host name of the server you are configuring, click Security realms.

- 3 In the right pane, click the name of the realm you are configuring.
- 4 Click Providers.
- 5 Click the Authentication tab.
- 6 In the left pane, click Lock & Edit.
- 7 In the right pane, specify the Policy Agent Authentication Provider.
- 8 Click Delete.
- 9 Click Yes.
- 10 In the left pane, click Activate changes.

The Agent Authentication Provider is not removed from the configuration until you restart the WebLogic Server/Portal 10 instance. The best practice is to restart the WebLogic Server/Portal 10 instance after you perform the following tasks.

## Unconfiguring the WebLogic Server/Portal 10 Agent

### ▼ To Unconfigure the WebLogic Server/Portal 10 Agent

- 1 Undeploy any applications protected by the WebLogic Server/Portal 10 agent.
- 2 Restore the deployment descriptors of these applications to their original deployment descriptors. (Backup files are useful here if you have them.)
- 3 If you are permanently removing the WebLogic Server/Portal 10 agent, undeploy the agent application.  
However, if you plan to re-install this agent , you don't need to undeploy the agent application.
- 4 If the WebLogic Server/Portal 10 instance was originally configured using Node Manager, remove the `classpath` and agent Java options using the WebLogic Server/Portal 10 Administration Console. For more information, see:  
[“Configuring a WebLogic Server 10 Instance With the Agent classpath and Java Options” on page 21](#)  
or  
[“WebLogic Portal 10: Configuring the Agent classpath and Java Options” on page 42](#)
- 5 Ensure that the WebLogic Server/Portal 10 container is stopped.



# Uninstalling the WebLogic Server/Portal 10 Agent Using the agentadmin Program

## ▼ To Uninstall the WebLogic Server/Portal 10 Agent

### 1 Change to the following directory:

*PolicyAgent-base*/j2ee\_agents/weblogic\_v10\_agent/bin

where *PolicyAgent-base* is where you unzipped the weblogic\_v10\_agent\_3.zip file.

### 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 When prompted, enter the Startup script location.

### 4 The uninstall program displays your response and then asks if you want to continue:

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

## Example 2 Uninstallation Sample for the WebLogic Server/Portal 10 Agent

```
*****
Welcome to the Sun OpenSSO Enterprise Policy Agent 3.0 for BEA WebLogic
10.0 Platform.
*****
```

Enter the path to the location of the script used to start the WebLogic domain.  
Please ensure that the agent is first installed on the admin server instance  
before installing on any managed server instance.

[ ? : Help, ! : Exit ]

Enter the Startup script location

```
[/usr/local/boa/user_projects/domains/base_domain/startWebLogic.sh]:
```

```
/opt/boa/user_projects/domains/base_domain/startWebLogic.sh
```

```
-----
SUMMARY OF YOUR RESPONSES
-----
```

Startup script location :

```
/opt/boa/user_projects/domains/base_domain/startWebLogic.sh
```

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]:

Remove amauthprovider.jar from  
/export/home/opt/bea/wlserver\_10.0/server/lib/mbeantypes ...DONE.

Deleting the config directory  
/export/home/opt/agents/weblogic10/j2ee\_agents/weblogic\_v10\_agent/Agent\_001/config  
...DONE.

UnConfigure  
/opt/bea/user\_projects/domains/base\_domain/setAgentEnv\_AdminServer.sh  
...DONE.

Uninstall log file location:  
/export/home/opt/agents/weblogic10/j2ee\_agents  
/weblogic\_v10\_agent/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 /logs directory still exists.
- The uninstall program creates an uninstall log file in the *PolicyAgent-base/j2ee\_agents/weblogic\_v10\_agent/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.

# Installing and Configuring the WebLogic Server/Portal 10 Agent in a Cluster

Installing and configuring the WebLogic Server/Portal 10 agent in a clustered environment is similar to the process for a stand-alone environment. Exceptions are noted in this section.

- [“Installing the WebLogic Server/Portal 10 Agent in a Cluster” on page 35](#)
- [“Post-Installation Tasks for the WebLogic Server/Portal 10 Agent in a Cluster” on page 36](#)

## Installing the WebLogic Server/Portal 10 Agent in a Cluster

In a cluster, you must install the WebLogic Server/Portal 10 agent in this order:

1. First, install the agent on the Administration Server. The agent on the Administration Server sets up the Agent Authenticator for the entire domain. See [“Installing the WebLogic Server/Portal 10 Agent on the Administration Server” on page 35](#).
2. Then, install the agent on each of the Managed Servers that you want to protect. See [“Installing the WebLogic Server/Portal 10 Agent on a Managed Server” on page 36](#).

## Installing the WebLogic Server/Portal 10 Agent on the Administration Server

### ▼ To Install the WebLogic Server/Portal 10 Agent on the Administration Server

- 1 Ensure that the Administration Server is not running.
- 2 Install the agent as you would in a stand-alone environment. See [“Installing the WebLogic Server/Portal 10 Agent” on page 12](#).
- 3 Configure the agent `classpath` for the Administration Server. See [“Configuring a WebLogic Server 10 Instance With the Agent `classpath` and Java Options” on page 21](#).
- 4 Start the Administration Server.
- 5 Configure the Agent Authentication Provider. See [“Configuring the Agent Authentication Provider for the WebLogic Server/Portal 10 Agent” on page 23](#).

## Installing the WebLogic Server/Portal 10 Agent on a Managed Server

### ▼ To Install the WebLogic Server/Portal 10 Agent on a Managed Server

- 1 Ensure that the Managed Server is not running.
- 2 Install the WebLogic Server/Portal 10 agent as you would in a stand-alone environment, with these exceptions:
  - When you are prompted to enter the startup script location, specify the same path that you provided when you installed the agent on the Administration Server.
  - When you are prompted to enter the WebLogic Server instance name, specify the Managed Server instance name. For example: `server1`
- 3 Start the Managed Server using the appropriate startup script:
  - Solaris and Linux systems: `domain-name/bin/startManagedWeblogic.sh`
  - Windows systems: `domain-name\bin\startManagedWeblogic.cmd`

where *domain-name* is where you located the domain.

For example, on a Solaris system:

```
cd /opt/bea/user_projects/domains/domain1/bin
./startManagedWeblogic.sh server1 http://adminhost.example.com:7001
```

Alternatively, you can start a Managed Server instance using Node Manager. See [“Configuring Node Manager for the WebLogic Server/Portal 10 Agent in a Cluster”](#) on page 38.

## Post-Installation Tasks for the WebLogic Server/Portal 10 Agent in a Cluster

TABLE 2 Post-Installation Tasks for the WebLogic Server/Portal 10 Agent in a Cluster

Post-Installation Task	Where to go for Information
Adding a WebLogic Administrator to the Bypass List	<a href="#">“Adding a WebLogic Administrator to the Bypass List for the WebLogic Server/Portal 10 Agent”</a> on page 25
Enabling Agent Protection in Web Applications	<a href="#">“Installing the Agent Filter for the WebLogic Server/Portal 10 Agent”</a> on page 25
Deploying the Agent Application in a Cluster	<a href="#">“Deploying the Agent Application for the WebLogic Server/Portal 10 Agent in a Cluster”</a> on page 37

**TABLE 2** Post-Installation Tasks for the WebLogic Server/Portal 10 Agent in a Cluster *(Continued)*

Post-Installation Task	Where to go for Information
Configuring Node Manager for the WebLogic Server/Portal 10 Agent in a Cluster	<a href="#">“Configuring Node Manager for the WebLogic Server/Portal 10 Agent in a Cluster” on page 38.</a>

For additional tasks, see [“Post-Installation Tasks for the WebLogic Server/Portal 10 Agent” on page 21.](#)

## Deploying the Agent Application for the WebLogic Server/Portal 10 Agent in a Cluster

Deploy the agent application (`agentapp.war`) on each instance in the cluster on which the agent is installed, including the Administration Server and each Managed Server. Instances in the cluster require the agent application to receive notifications.

A deployment can have multiple applications protected by the same agent running on the same Managed Server instance. All applications hosted on the same Managed Server instance use the agent application deployed for that instance.

Deploy the agent application using either the WebLogic Server command-line tools or Administration Console.

### ▼ To Deploy the Agent Application Using the WebLogic Server/Portal 10 Administration Console

- 1 **Login to the WebLogic Server/Portal 10 Administration Console**
- 2 **Expand the Deployments tab.**
- 3 **Click Lock & Edit.**
- 4 **In the right pane, click Install.**
- 5 **Click upload your file(s).**

Upload the `agentapp.war` file from the following directory:

*PolicyAgent-base/etc/agentapp.war*

When selecting the target for the Web Application module, select either the entire cluster or individual servers. Deploy the `agentapp.war` file for each server node on which you installed the agent.

## Configuring Node Manager for the WebLogic Server/Portal 10 Agent in a Cluster

You have the option of starting Managed Servers in a cluster using the WebLogic Server/Portal 10 Node Manager.

### ▼ To Configure Node Manager for the WebLogic Server/Portal 10 Agent in a Cluster

- 1 In the WebLogic Server/Portal 10 Administration Console, expand the **Servers** node.
- 2 Select the node for the server you want to manage with Node Manager.
- 3 Configure the agent classpath in Node Manager:

- a. In the Administration Console, select the **Configuration** tab.
- b. Select the **Server Start** tab.
- c. Locate the agent classpath for the specific Managed Server as found in `setAgentEnv_sever-instance.sh`.
- d. Add the agent classpath to the following classpath text field:

```
${CLASSPATH}:PolicyAgent-base/lib/agent.jar:PolicyAgent-base/lib/amclientsdk.jar:PolicyAgent-base/locale:PolicyAgent-base/AgentInstance/config
```

where *AgentInstance* represents the agent instance directory, such as `Agent_001`.

---

**Tip** – To avoid typing errors, copy and paste the agent classpath entries from the `setAgentEnv_managed-sever-instance.sh` file.

---

*managed-server-instance* is the name of the Managed Server instance. For example, `server1`.

- e. To the same classpath text field referred to in the previous step, prepend the following classpath entries:

```
DeployContainer-base/BEA-Java-Home/lib/tools.jar:  
DeployContainer-base/wlserver_10.0/server/lib/weblogic.jar
```

*DeployContainer-base* is the directory in which WebLogic Server/Portal 10 was installed.

*BEA-Java-Home* is the directory that contains the JDK for the WebLogic Server/Portal 10 instance.

- f. Click Save.
  - g. Click Activate Changes.
- 4 **Configure the agent Java options in Server Start.**
- a. In the WebLogic Server/Portal 10 Administration Console, select the Configuration tab.
  - b. Select the Server Start tab.
  - c. Locate the Java options as found in `setAgentEnv_sever-instance.sh` for the specific Managed Server.
  - d. Add the Java options to the Arguments text field as follows:
 

```
-Djava.util.logging.config.file=PolicyAgent-base/config/
OpenSSOAgentLogConfig.properties
-DLOG_COMPATMODE=Off
```

---

**Tip** – To avoid typing errors, copy and paste the agent Java option entries from the `setAgentEnv_managed-sever-instance.sh` file.

---
  - e. Click Save.
  - f. Click Activate Changes.

## Installing and Configuring the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

Installation and configuration of the agent on WebLogic Portal 10 is similar to the same tasks on WebLogic Server 10. This section describes the differences, including:

- [“Installing the Agent on WebLogic Portal 10” on page 40](#)
- [“Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10” on page 40](#)
- [“Creating WebLogic Portal 10 Users in OpenSSO Enterprise” on page 47](#)
- [“Verifying Users in the WebLogic Portal 10 User Repository” on page 48](#)
- [“Testing the WebLogic Server/Portal 10 Agent on WebLogic Portal 10” on page 48](#)

The examples in this section show how to protect the sample portal, which by default is named `groupspace`. You can protect multiple portals with a single WebLogic Portal 10 instance. For each portal you configure, ensure that you use the correct portal application name.

# Installing the Agent on WebLogic Portal 10

To install the agent on WebLogic Portal 10, use the custom installation option. For example:

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

The installation process is then similar to installing the agent on WebLogic Server 10, with the exception of these prompts:

```
...
Enter true if the agent is being installed on a Portal domain
[ ? : Help, < : Back, ! : Exit ]
Is the agent being installed on a Portal domain ? [false]: true
```

Enter true.

```
...
Enter the Deployment URI for the portal application
that is protected by the agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the Deployment URI for the portal Application [/]: /groupspace
```

Enter the deployment URI. Examples in this section use the default sample portal, /groupspace.

For a description of the other installation prompts, see [“Installing the WebLogic Server/Portal 10 Agent” on page 12](#).

# Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

The post-installation tasks are similar to configuring the agent on WebLogic Server 10, with the exceptions noted in the following tables.

**TABLE 3** Required Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

Required Post-Installation Task	Where to go for Information
Configuring the Agent classpath and Java Options	Different for WebLogic Portal 10.  See <a href="#">“WebLogic Portal 10: Configuring the Agent classpath and Java Options” on page 42</a> .



**TABLE 3** Required Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10  
(Continued)

Required Post-Installation Task	Where to go for Information
Configuring the Agent Authentication Provider	Different for WebLogic Portal 10.  See <a href="#">“WebLogic Portal 10: Configuring the Agent Authentication Provider”</a> on page 42.
Adding a WebLogic Administrator to the Bypass List	Same as for WebLogic Server 10.  See <a href="#">“Adding a WebLogic Administrator to the Bypass List for the WebLogic Server/Portal 10 Agent”</a> on page 25.
Configuring the Agent Filter Modes	Different for WebLogic Portal 10.  See <a href="#">“WebLogic Portal 10: Configuring the Agent Filter Modes”</a> on page 44.
Setting Logout-Related Properties for the Sample Portal	Applies only to WebLogic Portal 10.  See <a href="#">“WebLogic Portal 10: Setting Logout-Related Properties for the Sample Portal”</a> on page 46.
Deploying the Agent Application	Same as for WebLogic Server 10.  See <a href="#">“Deploying the Agent Application”</a> on page 23.

**TABLE 4** Optional Post-Installation Tasks for the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

Optional Post-Installation Task	Where to go for Information
Changing the Password for an Agent Profile	Same as for WebLogic Server 10.  See <a href="#">“Changing the Password for an Agent Profile”</a> on page 27.
Creating the Necessary URL Policies	Same as for WebLogic Server 10.  See <a href="#">“Creating the Necessary URL Policies”</a> on page 28.
Deploying the Policy Agent Sample Application	Same as for WebLogic Server 10.  See <a href="#">“Deploying the Policy Agent Sample Application”</a> on page 28.
Mapping OpenSSO Enterprise Roles to Principal Names	Same as for WebLogic Server 10.  See <a href="#">“Mapping OpenSSO Enterprise Roles to Principal Names”</a> on page 29.

## WebLogic Portal 10: Configuring the Agent classpath and Java Options

### ▼ To Configure the WebLogic Portal 10 Instance With the Agent classpath and Java Options

**1 Using a text editor, edit the following WebLogic Portal 10 startup script, depending on your platform:**

- Solaris and Linux systems:  
*DeployContainer-base*/wlserver\_10.0/samples/domains/portal/bin/startWeblogic.sh
- Windows systems:  
*DeployContainer-base*\wlserver\_10.0\samples\domains\portal\bin\startWeblogic.cmd

*DeployContainer-base* represents the directory where the WebLogic Portal 10 instance is installed.

**2 Add the path of the agent environment variable script to the WebLogic Portal 10 startup script:**

- Solaris and Linux systems: After the line, `. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*`, add:

*DeployContainer-base*/samples/domains/portal/setAgentEnv\_\${SERVER\_NAME}.sh

Therefore, the startup script would then contain these two lines:

```
. ${DOMAIN_HOME}/bin/setDomainEnv.sh $*
DeployContainer-base/samples/domains/portal/setAgentEnv_${SERVER_NAME}.sh
```

- Windows systems: After the line, `call "%DOMAIN_HOME%\bin\setDomainEnv.cmd" %*`, add:  
`call`  
*DeployContainer-base*\wlserver\_10.0\samples\domains\portal\setAgentEnv\_%SERVER\_NAME%.cmd

Therefore, the startup script would then contain these two lines:

```
call "%DOMAIN_HOME%\bin\setDomainEnv.cmd" %*
call DeployContainer-base\wlserver_10.0\samples\domains\portal\setAgentEnv_%SERVER_NAME%.cmd
```

The `${SERVER_NAME}` or `%SERVER_NAME%` variable represents the WebLogic Portal 10 instance that is dynamically replaced.

**3 Restart the WebLogic Portal 10 instance.**

## WebLogic Portal 10: Configuring the Agent Authentication Provider

This section applies only to WebLogic Portal 10.

## ▼ **To Configure the Agent Authentication Provider for WebLogic Portal 10**

- 1** Log in to the WebLogic Portal 10 Administration Console.
- 2** In the left pane, under Domain Structure and the host name of the server you are configuring, click Security realm.
- 3** In the right pane, click the name of the realm you are configuring.
- 4** Click Providers.
- 5** Click the Authentication tab.
- 6** In the left pane, click Lock & Edit.
- 7** In the right pane, click New.
- 8** Specify Type as AgentAuthenticator.
- 9** Specify Name with a name of your choice.
- 10** Click OK.
- 11** Click the newly created policy agent authentication provider.
- 12** Change the control flag value to OPTIONAL.
- 13** Click Save.
- 14** Click Providers.  
The console displays the Authentication Providers Table .
- 15** Click SQLAuthenticator
- 16** Change the control flag to OPTIONAL.
- 17** Click Save.
- 18** Click the Providers tab.
- 19** Click SAMLAuthenticator
- 20** Change the control flag to OPTIONAL.

- 21 Click Save.
- 22 In the left pane, click **Activate changes**.
- 23 After you are finished, restart the server for the changes to take effect.

#### More Information Default Security Realm

If create a new security realm instead of using the default security realm to configure the agent, ensure that the control flag value for the Agent Authenticator and any additional authentication providers are set to `OPTIONAL`.

### WebLogic Portal 10: Configuring the Agent Filter Modes

Configuring the agent filter modes for WebLogic Portal 10 agent is different than for the WebLogic Server 10 agent because the following filter modes do not apply to WebLogic Portal 10:

- `SSL_ONLY`: If you are using WebLogic Portal 10 for single sign-on (SSO), use the `J2EE_POLICY` filter mode.
- `URL_POLICY`: If you are using WebLogic Portal 10 to protect URLs such as portal JSP files from being accessed directly, use the `ALL` filter mode.

To set the filter modes for the WebLogic Server/Portal 10 agent, use one of these methods:

- Use the OpenSSO Enterprise Administration Console:
  1. Login to the Console as `amadmin`.
  2. Under **Access Control**, *realm-name*, **Agents**, and **J2EE**, click the name of the agent profile you want to update.

The Console displays the **Edit** page for the agent profile.
  3. Under **Global**, add the filter mode to the **Agent Filter Mode**.
  4. Click **Save**.

or
- Use the `ssoadm` utility to set the `com.sun.identity.agents.config.filter.mode` property.

**Note** – When creating a OpenSSO Enterprise policy to protect the WebLogic Portal 10 instance, define the policy to give permission to only public portal URLs. For example:

```
http://agent.example.com:7041/groupspace/
```

```
http://agent.example.com:7041/groupspace/groupspace.jsp
```

---

## WebLogic Portal 10: Installing the Agent Filter for the Deployed Application

This section use the sample portal (groupspace) as the application whose deployment descriptor is modified. For example, the `web.xml` file for the sample portal is in the following location:

```
/usr/local/beamserver_10.0/samples/portal/portalApp/groupspaceSampleWeb/WEB-INF
```

### ▼ To Install the Agent Filter for the Deployed Application for WebLogic Portal 10

- **Edit the application's `web.xml` descriptor by adding the `<filter>` elements.**

Add the `<filter>`, `<filter-mapping>`, and `<dispatcher>` elements as the first filter element in the `web.xml` descriptor. 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>
```

**Important:** Make sure that this filter element is the first element in the descriptor.

## WebLogic Portal 10: Setting Logout-Related Properties for the Sample Portal

This task involves configuring logout-related properties for the sample portal (groupspace), using either the either in the OpenSSO Enterprise Console or the `ssoadm` utility.

To set the logout-related properties in the OpenSSO Enterprise Console:

1. Login to the Console as `amadmin`.
2. Under Access Control, *realm-name*, Agents, and J2EE, click the name of the agent profile you want to update.

The Console displays the Edit page for the agent profile.

3. Click Application and then Logout Processing. then set the following fields, depending on your requirements:
  - **Logout Application Handler:** An application-specific map that identifies a handler to be used for logout processing. The corresponding property is `com.sun.identity.agents.config.logout.application.handler`.
  - **Logout Application URI:** An application-specific map that identifies a request URI that indicates a logout event. The corresponding property is `com.sun.identity.agents.config.logout.uri`.
  - **Logout Request Parameter:** An application-specific map that identifies a parameter that when present in the HTTP request indicates a logout event. The corresponding property is `com.sun.identity.agents.config.logout.request.param`.
  - **Logout Introspect Enabled:** Check Enabled to allow the agent to search an HTTP request body to locate the logout parameter. The corresponding property is `com.sun.identity.agents.config.logout.introspect.enabled`.
  - **Logout Entry URI:** An application-specific map that identifies a URI to be used as an entry point after a successful logout and subsequent successful authentication if applicable. The corresponding property is `com.sun.identity.agents.config.logout.entry.uri`.
4. Click Save.

To use the `ssoadm` utility, set the logout-related agent properties. For example:

```
com.sun.identity.agents.config.logout.application.handler[] =  
com.sun.identity.agents.config.logout.uri[groupspace] = /groupspace/communityFiles/shell/logout.jsp  
com.sun.identity.agents.config.logout.request.param[groupspace] = logout  
com.sun.identity.agents.config.logout.introspect.enabled = true  
com.sun.identity.agents.config.logout.entry.uri[groupspace] = /groupspace/groupspace.jsp
```

All of these logout-related properties are hot-swappable.

## Creating WebLogic Portal 10 Users in OpenSSO Enterprise

Before configuring the agent, create the same users in OpenSSO Enterprise that exist in WebLogic Portal 10.

If the users in OpenSSO Enterprise have different names than the names in WebLogic Portal 10, you must configure user mapping, using either the OpenSSO Enterprise Console or the `ssoadm` utility.

To configure user mapping in the OpenSSO Enterprise Console:

1. Login to the Console as `amadmin`.
2. Under Access Control, *realm-name*, Agents, and J2EE, click the name of the agent profile you want to update.  
The Console displays the Edit page for the agent profile.
3. Click Global and then User Mapping, and then set the following fields, depending on your requirements:
  - **User Mapping Mode:** Mechanism the agent uses to determine the user ID (HTTP\_HEADER, PROFILE\_ATTRIBUTE, SESSION\_PROPERTY, or USER\_ID)
  - **User Attribute Name:** Name of the attribute that contains the user ID. The corresponding property is `com.sun.identity.agents.config.user.attribute.name`.
  - **User Principal Flag:** Check Enabled to use the principal instead of only the user ID for authenticating the user. The corresponding property is `com.sun.identity.agents.config.user.principal`.
  - **User Token Name:** Session property name for the user ID of the authenticated user in the session. The corresponding property is `com.sun.identity.agents.config.user.token`.
4. Click Save.

To use the `ssoadm` utility, set the following agent properties:

- `com.sun.identity.agents.config.user.mapping.mode[]`
- `com.sun.identity.agents.config.user.attribute.name`
- `com.sun.identity.agents.config.user.principal`
- `com.sun.identity.agents.config.user.token`

All of the user mapping properties are hot-swappable.

## Verifying Users in the WebLogic Portal 10 User Repository

To further enforce security, configure the agent to verify users in the WebLogic Portal 10 user repository.

Configure a custom verification handler using either the OpenSSO Enterprise Console or the `ssoadm` utility.

To configure a custom verification handler in the OpenSSO Enterprise Console:

1. Login to the Console as `amadmin`.
2. Under Access Control, *realm-name*, Agents, and J2EE, click the name of the agent profile you want to update.

The Console displays the Edit page for the agent profile.

3. Click Application, and then set the **Custom Verification Handler**, which specifies an application specific verification handler to validate the user credentials with the local repository. The corresponding property is `com.sun.identity.agents.config.verification.handler`.
4. Click Save.

To use the `ssoadm` utility, set the `com.sun.identity.agents.config.verification.handler` property. For example:

```
com.sun.identity.agents.config.verification.handler[groupspace] =  
com.sun.identity.agents.weblogic.v10.AmWLPortalVerificationHandler
```

This property is hot-swappable.

## Testing the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

### ▼ To Test the WebLogic Server/Portal 10 Agent on WebLogic Portal 10

- 1 Create a user with the user ID of `sean` in both the WebLogic Portal Administration Console and OpenSSO Enterprise Console.
- 2 If the agent filter mode (`com.sun.identity.agents.config.filter.mode` property) is set to ALL, create the appropriate OpenSSO Enterprise policies for the portal URLs where `sean` is the user.



- 3 **Using a browser, specify the URL of the sample portal. For example:**  
`http://agent.example.com:7041/groupspace/groupspace.jsp`
- 4 **Login with the user ID of sean.**  
The sample portal home page should appear.
- 5 **Click GS Example Community.**  
The portal web page appears.
- 6 **Click Logout.**

## Migrating a Version 2.2 WebLogic Server/Portal 10 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 features, described in [“What's New in Version 3.0 Policy Agents” on page 4](#).

The migration process migrates the agent's binary files, updates the agent's 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 WebLogic Server/Portal 10 agent, download the version 3.0 WebLogic Server/Portal 10 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 `WL10v3Agent` 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 27](#).

## ▼ 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 container files and directories.

### 2 Stop the WebLogic Server/Portal 10 container 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 OpenSSO project site:

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

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

For example, if you downloaded and unzipped the version 3.0 WebLogic Server/Portal 10 agent in the `v30agent` directory:

```
cd /v30agent/j2ee_agents/weblogic_v10_agent/bin
```

### 6 Run the version 3.0 `agentadmin` program with the `--migrate` option. For example:

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

### 7 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/weblogic_v10_agent
...
```

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

The `agentadmin` program migrates the version 2.2 agent.

### 8 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 = WL10v3Agent
```

- 9 **Copy the Agent\_ddd/config/OpenSSOAgentConfiguration.properties file to the /bin directory where ssoadm is installed on the OpenSSO Enterprise server.**
- 10 **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
```
- 11 **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
- 12 **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 -b WL10v3Agent -t J2EEAgent -u amadmin
-f /tmp/amadminpw -D ./OpenSSOAgentConfiguration.properties
```

In this example:

- tools\_zip\_root is the directory where you unzipped ssoAdminTools.zip.
- WL10v3Agent is the version 3.0 agent configuration name.
- J2EEAgent is the agent type for J2EE agents.
- /tmp/amadminpw is the path to the amadmin password 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.

- 13 **Restart the WebLogic Server/Portal 10 container 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 WebLogic Server/Portal 10 Agent” on page 30](#).

# Third-Party Web Site References

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

**Note** – Sun is not responsible for the availability of third-party web sites mentioned in this document. Sun does not endorse and is not responsible or liable for any content, advertising, products, or other materials that are available on or through such sites or resources. Sun will not be responsible or liable for any actual or alleged damage or loss caused or alleged to be caused by or in connection with use of or reliance on any such content, goods, or services that are available on or through such sites or resources.

# Revision History

Part Number	Date	Description
820–4580	October 3, 2008	In-progress RR review draft
820-4580–05	June 25, 2008	Early Access (EA) release draft

# 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 BEA WebLogic Server/Portal 10*, and the part number is 820-4580.