Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Apache HTTP Server 2.0.x

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

Part No: 820–7584–12
December 22, 2009

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^{TM} 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.

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.

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

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

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

Les produits qui font l'objet de cette publication et les informations qu'il contient sont régis par la legislation 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 legislation américaine en matière de contrôle des exportations et la liste de ressortissants spécifiquement designés, 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 Apache HTTP Server 2.0.x

Last updated December 22, 2009

The Apache HTTP Server 2.0.x policy agent is a version 3.0 web agent that functions with Sun OpenSSO Enterprise to protect resources on Apache HTTP Server 2.0.x.

Contents

For general information about web policy agents, including the new features for version 3.0 agents, see *Sun OpenSSO Enterprise Policy Agent 3.0 User's Guide for Web Agents*.

Note – A version 2.2 web agent also exists for Apache HTTP Server 2.0.x. However, to use the new version 3.0 agent features, you must deploy the version 3.0 agent described in this guide.

Supported Platforms, Compatibility, and Coexistence for the Apache HTTP Server 2.0.x Agent

Supported Platforms for the Apache HTTP Server 2.0.x Agent

TABLE 1 Supported Platforms for the Apache HTTP Server 2.0.x Agent

Agent For	Support Platforms
▪ Apache HTTP Server 2.0.x ▪ Oracle HTTP Server 10.1.x based on Apache HTTP Server 2.0.x ▪ IBM HTTP Server 6.0 and 6.1 based on Apache HTTP Server 2.0.x	▪ Solaris OS on SPARC and x86 platforms, versions 9 and 10, 32–bit and 64–bit ▪ Red Hat Enterprise Linux Advanced Server 4.0 and 5.0, 32–bit and 64–bit ▪ Windows Server 2003 and 2008, 32–bit only ▪ Ubuntu 8.x Server Edition, 32-bit and 64-bit ▪ SuSE Linux 9.x, 32-bit and 64-bit ▪ Debian 4.x, 32-bit and 64-bit
▪ Apache HTTP Server 2.0.x on IBM AIX® systems ▪ IBM HTTP Server 6.0 and 6.1 based on Apache HTTP Server 2.0.x	▪ IBM AIX 5.x and 6.1, 32–bit only
▪ Apache HTTP Server 2.0.x	▪ HP-UX 11i v1 or later, 32–bit, with the integrated (built-in) Apache 2.0.x server only **Note**. The Apache HTTP Server 2.0.x agent is **not** supported on the Apache 2.0.x server manually installed on HP-UX.
▪ Minor versions of the Apache HTTP Server 2.0.x web container, Oracle HTTP Server, and IBM HTTP Server are supported. ▪ Minor versions of the supported platforms, including updates, service packs, and patches, are also supported.	

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

Coexistence With Version 2.2 Policy Agents

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

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

Unsupported OpenSSO Enterprise Features

The Apache HTTP Server 2.0.x agent does not support the following features:

- "Log File Rotation" on page 5
- "Notifications" on page 5
- "POST Data Preservation" on page 6

Log File Rotation

The Apache HTTP Server 2.0.x agent does not support log file rotation, because the multi-process environment impairs the agent's capability to obtain the correct size of the log file. Without the correct log file size, the agent cannot rotate the file as intended.

Therefore, do not enable log rotation for the Apache HTTP Server 2.0.x agent, either in the OpenSSO Administration Console or by setting the `com.sun.am.policy.agents.config.local.log.rotate` property to `true`. Enabling log rotation can cause inconsistent and unpredictable results for the agent.

Notifications

The Apache HTTP Server 2.0.x agent does not support notifications, so maintaining the agent's SSO, policy, and configuration caches through a notification mechanism is not available.

Therefore, do not enable notifications for the Apache HTTP Server 2.0.x agent, either in the OpenSSO Administration Console or by setting the `com.sun.identity.agents.config.notification.enable property` to `true`. Enabling notifications can cause unpredictable behavior for the agent.

POST Data Preservation

The Apache HTTP Server 2.0.x agent does not support POST data preservation, where POST data is submitted to the server through HTML forms before users log in to OpenSSO Enterprise.

Pre-Installation Tasks for the Apache HTTP Server 2.0.x Agent

Setting Your `JAVA_HOME` Environment Variable

The agent installation program requires the Java Runtime Environment (JRE) 1.5 or later. Before you install the agent , set your `JAVA_HOME` environment variable to point to the JDK installation directory for the JDK version you are using. If you have not set this variable (or if you set it incorrectly), the program will prompt you for the correct path.

Downloading and Unzipping the Agent Distribution File

▼ To Download and Unzip the Agent Distribution File

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

2 **Create a directory to unzip the agent distribution file.**

3 **Download and unzip the agent distribution file, depending on your platform:**

Platform	Distribution File
Solaris SPARC systems, 64–bit	`apache_v20_SunOS_sparc_64_agent_3.zip`
Solaris SPARC systems, 32–bit	`apache_v20_SunOS_sparc_agent_3.zip`
Solaris x86 systems, 64–bit	`apache_v20_SunOS_x86_64_agent_3.zip`
Solaris x86 systems, 32–bit	`apache_v20_SunOS_x86_agent_3.zip`
Linux systems, 64–bit	`apache_v20_Linux_64_agent_3.zip`
Linux systems, 32–bit	`apache_v20_Linux_agent_3.zip`
Windows systems	`apache_v20_WINNT_agent_3.zip`
IBM AIX systems	`apache_v20_AIX_agent_3.zip`
HP-UX systems	`apache_v20_HP-UX_agent_3.zip`

These distribution files are available from the following sites:

- Sun Downloads under View by Category, Identity Management, and Policy Agents: `http://www.sun.com/download/index.jsp`
- OpenSSO project: `https://opensso.dev.java.net/public/use/index.html`

The following table shows the files and directories after you unzip the agent distribution file. These files are in the following directory:

AgentHome`/web_agents/apache_agent`, where *AgentHome* is where you unzipped the agent distribution file.

For example: `/opt/web_agents/apache_agent`

File or Directory	Description
`README.txt`, `README_NOTES`, and `license.txt`	Readme and license files
`/bin`	■ UNIX, Linux, and AIX systems: `agentadmin`, `certutil`, and `crypt_util` ■ Windows systems: `agentadmin.bat`, `certutil.exe`, and `cryptit.exe`
`/config`	Template, properties, and XML files
`/data`	`license.log` file (Do not edit this file)
`/etc`	`dsame.template` file
`/lib`	Library and JAR files
`/locale`	Properties files

File or Directory	Description
`/installer-logs`	Log files after you install the agent

Creating an Agent Profile

A web agent uses an agent profile to communicate with OpenSSO Enterprise server. A version 2.2 web agent can use the default agent profile (`UrlAccessAgent`). For a version 3.0 agent, however, you must create an agent profile using any of these three methods:

- Use the OpenSSO Enterprise Console, as described in "Creating an Agent Profile" on page 8.
- 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*.
- Choose the "Option to create the agent profile in the server during installation" when you run the `agentadmin` program.

▼ To Create an Agent Profile in the OpenSSO Enterprise Console

1. **Login into the OpenSSO Enterprise Administration Console as `amAdmin`.**

2. **Click `Access Control`, *realm-name*, `Agents`, and `Web`.**

3. **Under `Agent`, click `New`.**

4. **In the `Name` field, enter the name for the new agent profile.**

5. **Enter and confirm the `Password`.**

   Important: This password must be the same password that you enter in the agent profile password file that you specify when you run the `agentadmin` program to install the agent.

6. **In the `Configuration` field, check the location where the agent configuration properties are stored:**

   - `Local`: In the `OpenSSOAgentConfiguration.properties` file on the server where the agent is installed.
   - `Centralized`: In the OpenSSO Enterprise server central configuration data repository.

7. **In the `Server URL` field, enter the OpenSSO Enterprise server URL.**

   For example: `http://openssohost.example.com:8080/opensso`

8. **In the `Agent URL` field, enter the URL for the agent.**

   For example: `http://agenthost.example.com:8090/`

9 **Click `Create`.**

The console creates the agent profile and displays the `WebAgent` 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.

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

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 Apache HTTP Server 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 if you use the custom installation option and have the `agentadmin` program automatically create the agent profile in OpenSSO Enterprise server during the installation. If you prefer, you can use `amadmin` as the agent administrator

▼ To Create a Password File

1 **Create an ASCII text file for the password file. For example:** `/tmp/apache2agentpw`

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.**

Setting the IBM JDK/JRE for IBM AIX Systems

Perform this task only if you are installing the Apache HTTP Server 2.0.x agent on an IBM AIX system and you are using the IBM JDK/JRE.

▼ To Set the IBM JDK/JRE for IBM AIX Systems

1. **After you download and unzip the Apache HTTP Server 2.0.x agent distribution file for AIX, locate the** `agentadmin` **script in the following directory:**

   AgentHome`/web_agents/apache_agent/bin`, where *AgentHome* is where you unzipped the agent distribution file.

2. **In the** `agentadmin` **script, comment out the following line, which sets the regular JDK/JRE** `classpath`**:**

   ```
   $JAVA_VM -classpath "$AGENT_CLASSPATH"
   com.sun.identity.install.tools.launch.AdminToolLauncher $*
   ```

3. **In the** `agentadmin` **script, uncomment the following line at the end of the file, which sets the IBM JDK/JRE** `classpath`**:**

   ```
   #$JAVA_VM -DamKeyGenDescriptor.provider=IBMJCE -DamCryptoDescriptor.provider=IBMJCE
   -DamRandomGenProvider=IBMJCE -classpath "$AGENT_CLASSPATH"
   com.sun.identity.install.tools.launch.AdminToolLauncher $*
   ```

4. **Save your changes.**

Creating an Agent Administrator (Optional)

Creating an agent administrator is optional. An agent administrator can manage agents in OpenSSO Enterprise, including:

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

▼ To Create an Agent Administrator

1. **Login to OpenSSO Enterprise Console as** `amadmin`**.**

2. **Create a new agents administrator group:**

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

   b. **Click** `New`**.**

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

d. **Click** `OK`**.**

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

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

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

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

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

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

c. **Click** `OK`**.**

d. **Click the new agent administrator name.**

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

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

g. **Click** `Save`**.**

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

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

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

c. **Click** `Save`**.**

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

Installing the Apache HTTP Server 2.0.x Agent

Gathering Information to Install the Apache HTTP Server 2.0.x Agent

The following table describes the information you will need to provide when you run the `agentadmin` program to install Apache HTTP Server 2.0.x agent. For some `agentadmin` prompts, you can accept the default value displayed by the program, if you prefer.

TABLE 2 Information Required to Install the Apache HTTP Server 2.0.x Agent

Prompt Request	Description
Apache Server Config Directory Path	Path to the configuration directory used by the Apache HTTP Server instance. For example: `/opt/apache-2.0.63/conf`
OpenSSO server URL	URL for OpenSSO Enterprise server. For example: `http://openssohost.example.com:8080/opensso`
Agent URL	URL for the Apache HTTP Server 2.0.x agent. For example: `http://agenthost.example.com:8090`
Agent Profile Name	Name of the agent profile. For example: `Apache2Agent` For information, see "Creating an Agent Profile" on page 8.
Agent Profile Password File	Path to the agent profile password file. For example: `/tmp/apache2agentpw` For information, see "Creating a Password File" on page 9.

TABLE 2 Information Required to Install the Apache HTTP Server 2.0.x Agent *(Continued)*

Prompt Request	Description
Option for the installer to create the agent profile The `agentadmin` program displays the following prompt if the agent profile previously specified for the Agent Profile Name prompt does not already exist in OpenSSO Enterprise: `Enter true if the Agent Profile is being created into OpenSSO server by the installer. Enter false if it will be not be created by installer.`	To have the installation program create the agent profile, enter `true`. The program then prompts you for: ■ Agent administrator who can create, update, or delete the agent profile. For example: `agentadmin` **Important**: To use this option, the agent administrator must already exist in OpenSSO Enterprise server and must have agent administrative privileges. If you prefer, you can specify `amadmin` as this user. For information see, "Creating an Agent Administrator (Optional)" on page 10. ■ Path to the agent administrator password file. For example: `/tmp/agentadminpw` For information, see "Creating a Password File" on page 9.

Installing the Apache HTTP Server 2.0.x Agent Using the `agentadmin` Program

Before you install the Apache HTTP Server 2.0.x agent, your deployment must meet these requirements:

- An Apache HTTP Server 2.0.x instance must be installed and configured on the platform where you plan to install the agent.
- An OpenSSO Enterprise server instance must be installed and accessible to the Apache HTTP Server 2.0.x instance.
- You must have downloaded and unzipped the agent distribution file, as described in "Downloading and Unzipping the Agent Distribution File" on page 6.

▼ To Install the Apache HTTP Server 2.0.x Agent Using the `agentadmin` Program

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

Important: To install the agent, you must have write permission to the files and directories for the Apache HTTP Server instance.

2 **Stop the Apache HTTP Server instance.**

3 **Change to the *PolicyAgent-base*/`bin` directory. For example:**

```
# cd /opt/web_agents/apache_agent/bin
```

4 **Start the agent installation. For example:**

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

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

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

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

```
-----------------------------------------------
SUMMARY OF YOUR RESPONSES
-----------------------------------------------
Apache Server Config Directory : /opt/apache-2.0.63/conf
OpenSSO server URL : http://opensshost.example.com:8080/opensso
Agent URL : http://agenthost.example.com:8090
Agent Profile name : Apache2Agent
Agent Profile Password file name : /tmp/apache2agentpw
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]: 1
```

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

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

```
SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/web_agents/apache_agent/Agent_001/config/OpenSSOAgentBootstrap.properties
Agent Configuration Tag file location
/opt/web_agents/apache_agent/Agent_001/config/OpenSSOAgentConfiguration.propertie
s
Agent Audit directory location:
/opt/web_agents/apache_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/web_agents/apache_agent/Agent_001/logs/debug
Install log file location:
/opt/web_agents/apache_agent/installer-logs/audit/install.log
```

7 **After the installation finishes successfully, if you wish, check the installation log file in the `/installer-logs/audit` directory**

8 **Restart the Apache HTTP Server instance for the agent.**

Agent Installation Program Functions

The agent installation program performs these functions:

- Creates the `OpenSSOAgentBootstrap.properties` and `OpenSSOAgentConfiguration.properties` configuration files from the respective template files.
- Creates the file `dsame.conf` file from the template file.
- Modifies the `httpd.conf` file to include the path for the `dsame.conf` file.
- Creates the **agent instance directory** as *PolicyAgent-base*`/Agent_`*nnn*, where *nnn* identifies the agent instance as `Agent_001`, `Agent_002`, and so on for each additional agent instance.

  For example: `/opt/web_agents/apache_agent/Agent_001`

  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 Apache HTTP Server 2.0.x Agent

- “Installing the Apache HTTP Server 2.0.x Agent on Multiple Apache HTTP Server Instances” on page 15
- “Installing Apache HTTP Server 2.0.x Agent on the OpenSSO Enterprise Host Server” on page 16

Installing the Apache HTTP Server 2.0.x Agent on Multiple Apache HTTP Server Instances

After you install the Apache HTTP Server 2.0.x agent on a specific Apache HTTP Server instance, you can install the agent on another Apache HTTP Server instance by executing the `agentadmin` program again for that instance.

Installing Apache HTTP Server 2.0.x Agent on the OpenSSO Enterprise Host Server

OpenSSO Enterprise is not supported on the Apache HTTP Server 2.0.x web container. Therefore, installing the Apache HTTP Server 2.0.x agent and OpenSSO Enterprise on the same server instance is not supported.

Post-Installation Tasks for the Apache HTTP Server 2.0.x Agent

- "Using SSL With the Apache HTTP Server 2.0.x Agent (Optional)" on page 16
- "Changing the Password for an Agent Profile (Optional)" on page 18
- "Configuring the Apache HTTP Server 2.0.x Agent on IBM AIX Systems" on page 19
- "Setting the `SHLIB_PATH` Environment Variable on HP-UX Systems" on page 20

Using SSL With the Apache HTTP Server 2.0.x Agent (Optional)

If you specify the `HTTPS` protocol during the Apache HTTP Server 2.0.x agent installation, the agent is automatically configured and ready to communicate over Secure Sockets Layer (SSL). Before continuing with the tasks in this section, however, ensure that the Apache HTTP Server instance is configured for SSL. For information, see the Apache HTTP Server 2.0 documentation:`http://httpd.apache.org/docs/2.0/`.

- "Disabling the Trust Behavior of the Apache HTTP Server Agent " on page 16
- "Installing the OpenSSO Enterprise Root CA Certificate on the Apache HTTP Server Instance" on page 17

Disabling the Trust Behavior of the Apache HTTP Server Agent

By default, the Apache HTTP Server 2.0.x agent installed on a remote Apache HTTP Server instance trusts any server certificate presented over SSL by the OpenSSO Enterprise host server. For the Apache HTTP Server 2.0.x agent to perform certificate checking, you must disable this behavior.

▼ To Disable the Trust Behavior of the Apache HTTP Server Agent

1 **Find the Apache HTTP Server 2.0.x agent's `OpenSSOAgentBootstrap.properties` file in the agent's `/config` directory. For example:**

```
/opt/web_agents/apache_agent/Agent_001/config/OpenSSOAgentBootstrap.properties
```

2. **In the `OpenSSOAgentBootstrap.properties` file, set the SSL-related properties, depending on your specific deployment.**

   Note: These properties have new names for version 3.0 web agents.

   - Disable the option to trust the server certificate sent over SSL by the OpenSSO Enterprise host server:

     `com.sun.identity.agents.config.trust.server.certs = false`
   - Specify the certificate database directory. For example:

     `com.sun.identity.agents.config.sslcert.dir = /opt/apache-2.0.63/conf/certdb`
   - If the certificate database directory has multiple certificate databases, set the following property to the prefix of the database you want to use. For example:

     `com.sun.identity.agents.config.certdb.prefix =` *prefix-*
   - Specify the certificate database password:

     `com.sun.identity.agents.config.certdb.password =` *password*
   - Specify the certificate database alias:

     `com.sun.identity.agents.config.certificate.alias =` *alias-name*

3. **Save the changes to the `OpenSSOAgentBootstrap.properties` file.**

   The agent uses information in the `OpenSSOAgentBootstrap.properties` file to start and initialize itself and to communicate with OpenSSO Enterprise server.

Installing the OpenSSO Enterprise Root CA Certificate on the Apache HTTP Server Instance

The root CA certificate that you install on the Apache HTTP Server instance must be the same certificate that is installed on the OpenSSO Enterprise host server.

Sun provides the Certificate Database Tool, `certutil`, in the Apache HTTP Server agent distribution file, to manage the root CA certificate and the certificate database.

For information about using `certutil`, see `http://www.mozilla.org/projects/security/pki/nss/tools/certutil.html`.

▼ To Install the OpenSSO Enterprise Root CA Certificate on the Apache HTTP Server Instance

1. **Obtain the root CA certificate file that is installed on the OpenSSO Enterprise host server.**

2. **On the Apache HTTP Server instance, locate the `certutil` utility.**

   After you unzip the Apache HTTP Server agent distribution file, `certutil` is available in the *PolicyAgent-base*`/bin` directory.

For example: `/opt/web_agents/apache_agent/bin/certutil`

3 **Before you use `certutil`, set the `LD_LIBRARY_PATH` environment variable to the location of the `certutil` library files.**

After you unzip the Apache HTTP Server agent distribution file, these library files are available in the *PolicyAgent-base*`/lib` directory.

For example: `/opt/web_agents/apache_agent/lib`

4 **If necessary, create the certificate database using `certutil`. For example:**

```
# cd /opt/web_agents/apache_agent/bin
# mkdir /opt/apache-2.0.63/conf/certdb
# ./certutil -N -d /opt/apache-2.0.63/conf/certdb
```

5 **Install the OpenSSO Enterprise root CA certificate using `certutil`. For example:**

```
# ./certutil -A -n cert-name -t "C,C,C" -d /opt/apache-2.0.63/conf/certdb -i cert-request-file
```

where:

- *cert-name* is the name of the OpenSSO Enterprise root CA certificate.
- *cert-request-file* is the binary root CA certificate request file.

6 **To verify that the root CA certificate is installed correctly, use `certutil` with the `-L` option. For example:**

```
# ./certutil -L -d /opt/apache-2.0.63/conf/certdb
```

You should see the name of the root CA certificate.

7 **Restart the Apache HTTP Server instance.**

Changing the Password for an Agent Profile (Optional)

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

▼ To Change the Password for an Agent Profile

1 **On the OpenSSO Enterprise server:**

a. **Login into the Administration Console.**

b. **Click Access Control, *realm-name*, Agents, Web, and then the name of the agent you want to configure.**

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 Apache HTTP Server 2.0.x agent is installed:**

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

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

```
# cd /opt/web_agents/apache_agent/bin
```

c. **Encrypt the new password using the** `agentadmin` **program. For example:**

```
#./agentadmin --encrypt Agent_001 /tmp/apache2agentpw
```

`Agent_001` is the agent instance whose password you want to encrypt.

`passwd` is the password file in the `/tmp` directory.

The `agentadmin` program returns the new encrypted password. For example:

```
The encrypted value is: /54GwN432q+MEnfh/AHLMA==
```

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.sun.identity.agents.config.password=/54GwN432q+MEnfh/AHLMA==
```

e. **Restart the Apache HTTP Server instance that is being protected by the policy agent.**

Configuring the Apache HTTP Server 2.0.x Agent on IBM AIX Systems

Perform this task only if you are installing the Apache HTTP Server 2.0.x agent on an IBM AIX system.

▼ To Configure the Apache HTTP Server 2.0.x Agent on IBM AIX Systems

1 **Set the** `LIBPATH` **variable to the agent's** `lib` **directory. For example:**

```
setenv LIBPATH /opt/web_agents/apache_agent/lib:/usr/lib:/lib
```

2. **As required, modify the `libxml2.so.2` library file to `libxml2.so` in the agent's `lib` directory, which is in the following directory:**

   AgentHome`/web_agents/apache_agent/lib`, where *AgentHome* is where you unzipped the agent distribution file.

Setting the `SHLIB_PATH` Environment Variable on HP-UX Systems

▼ To Set the `SHLIB_PATH` Environment Variable on HP-UX Systems

- **Before you start the Apache HTTP Server 2.0.x server, set the `SHLIB_PATH` environment variable to the agent's `lib` directory. For example:**

  ```
  setenv SHLIB_PATH /opt/web_agents/apache_agent/lib:/usr/lib:/lib
  ```

Managing the Apache HTTP Server 2.0.x Agent

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

- OpenSSO Enterprise Administration Console

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

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

- `ssoadm` command-line utility

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

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

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

Managing a Version 3.0 Agent With a Local Configuration

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

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

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

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

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

Uninstalling the Apache HTTP Server 2.0.x Agent

- "Preparing to Uninstall the Apache HTTP Server 2.0.x Agent" on page 21
- "Uninstalling the Apache HTTP Server 2.0.x Agent Using the `agentadmin` Program" on page 22

Preparing to Uninstall the Apache HTTP Server 2.0.x Agent

▼ To Prepare to Uninstall Apache HTTP Server 2.0.x Agent

1 **Undeploy any applications protected by the Apache HTTP Server 2.0.x agent.**

2 **Stop the Apache HTTP Server instance, if it is running.**

Uninstalling the Apache HTTP Server 2.0.x Agent Using the `agentadmin` Program

▼ To Uninstall the Apache HTTP Server 2.0.x Agent

1. **Change to the *PolicyAgent-base*/`bin` directory. For example:**

   For example: `cd /opt/web_agents/apache_agent/bin`

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

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

   or

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

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

3. **The `uninstall` program prompts you for the Apache HTTP Server configuration directory path.**

   For example: `/opt/apache-2.0.63/conf`

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

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

   The `uninstall` program uninstalls the agent (or all configured instances, if specified).

   ```
   /opt/web_agents/apache_agent/installer-logs/audit/uninstall.log
   ```

After You Finish the Uninstall

- The `/config` directory is removed from the agent instance directory, but the `/installer-logs` directory still exists.
- The `uninstall` program creates the `uninstall.log` file in the *PolicyAgent-base*/`installer-logs/audit` directory. For example:

  ```
  /opt/web_agents/apache_agent/installer-logs/audit/uninstall.log
  ```

- The agent instance directory is not automatically removed. For example, if you uninstall the agent for Agent_001, a subsequent agent installation creates the Agent_002 instance directory. To remove an agent instance directory, you must manually remove the directory.

Migrating a Version 2.2 Apache HTTP Server Policy Agent

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

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

Migrating a version 2.2 agent involves these general steps:

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

   To get the version 3.0 `agentadmin` program, you must download the version 3.0 agent that corresponds to the version 2.2 agent you are migrating. For example, if you are migrating the version 2.2 Apache HTTP Server agent, download the version 3.0 Apache HTTP Server 2.0.x 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 `openssoAdminTools.zip` file on the OpenSSO Enterprise server. For information, see Chapter 6, "Installing the OpenSSO Enterprise Utilities and Scripts," in *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 Apache2.0.xv3Agent 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 (Optional)" on page 18.

▼ To Migrate a Version 2.2 Agent:

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

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

2 **Stop the Apache HTTP Server instance for the version 2.2 agent.**

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

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

The version 3.0 agents are available from the 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 Apache HTTP Server 2.0.x agent in the `v30agent` directory:

```
cd /v30agent/web_agents/apache_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:**

```
/opt/v22/web_agents/apache_agent
```

In this example, `/opt/v22` is the directory where you downloaded and unzipped the version 2.2 agent.

The `agentadmin` program migrates the version 2.2 agent.

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

9 **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*

10 **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`

11 **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 Apache2.0.xv3Agent -t WebAgent -u amadmin
-f /tmp/amadminpw -D ./OpenSSOAgentConfiguration.properties
```

In this example:

- `tools_zip_root` is the directory where you unzipped `openssoAdminTools.zip`.
- `Apache2.0.xv3Agent` is the version 3.0 agent profile name.
- `WebAgent` is the agent type for web 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.

12 **Restart the Apache HTTP Server instance for the migrated agent.**

Next Steps After you migrate the agent, you can manage the new 3.0 agent configuration using the OpenSSO Enterprise Administration Console or the ssoadm utility, as described in “Managing the Apache HTTP Server 2.0.x Agent” on page 20.

Sun Microsystems Related Information

- “Additional Sun Resources” on page 25
- “Accessibility Features for People With Disabilities” on page 25
- “Related Third-Party Web Sites” on page 25
- “How to Report Problems and Provide Feedback” on page 26
- “Sun Welcomes Your Comments” on page 26

Additional Sun Resources

You can find additional useful information and resources at the following locations:

- Sun Services: http://www.sun.com/service/consulting/
- Sun Software Products: http://wwws.sun.com/software/
- Sun Support Resources http://sunsolve.sun.com/
- Sun Developer Network (SDN): http://developers.sun.com/
- Sun Developer Services: http://www.sun.com/developers/support/

Accessibility Features for People With Disabilities

To obtain accessibility features that have been released since the publishing of this media, consult Section 508 product assessments available from Sun upon request to determine which versions are best suited for deploying accessible solutions.

For information about Sun's commitment to accessibility, visit http://sun.com/access.

Related Third-Party Web Sites

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

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

How to Report Problems and Provide Feedback

If you have questions or issues with OpenSSO Enterprise, contact Sun as follows:

- Sun Support Resources (SunSolve) services at `http://sunsolve.sun.com/`.

  This site has links to the Knowledge Base, Online Support Center, and ProductTracker, as well as to maintenance programs and support contact numbers.
- The telephone dispatch number associated with your maintenance contract

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

If you are requesting help for a problem, please include the following information:

- Description of the problem, including when the problem occurs and its impact on your operation
- Machine type, operating system version, web container and version, JDK version, and OpenSSO Enterprise version, including any patches or other software that might be affecting the problem
- Steps to reproduce the problem
- Any error logs or core dumps

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com/` and click `Feedback`. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the title page or in the document's URL. For example, the title of this guide is *Sun OpenSSO Enterprise Policy Agent 3.0 Guide for Apache HTTP Server 2.0.x*, and the part number is 820-7584.

Revision History

Part Number	Date	Description
820-7584–12	December 22, 2009	Added support for HP-UX systems.
820-7584–11	November 10, 2009	Added support for IBM AIX systems.
820-7584–10	June 26, 2009	Initial release.