Sun Federated Access Manager Policy Agent 3.0 Guide for Sun Java System Web Server 7.0

Beta

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

Part No: 820–4579–05
July 15, 2008

080715@20490

Sun Federated Access Manager Policy Agent 3.0 Guide for Sun Java System Web Server 7.0

Early Access (EA) release. Last revised July 15, 2008

The Sun Java™ System Web Server 7.0 policy agent is a version 3.0 web agent that functions with Java System Federated Access Manager to protect applications and resources on web servers and web proxy servers deployed on Web Server 7.0.

This agent supports Web Server 7.0, Web Server 7.0 Update 1, and Web Server 7.0 Update 2. A version 2.2 web agent also exists for Web Server 7.0. However, to use the new version 3.0 features described in "What's New in Version 3.0 Web Agents" on page 4, you must deploy the version 3.0 Web Server 7.0 agent.

This guide provides specific information about the Web Server 7.0 agent, including:

What's New in Version 3.0 Web Agents

Sun is developing version 3.0 web agents in conjunction with Federated Access Manager 8.0. The version 3.0 web agents have the following new features and improvements over the version 2.2 web agents:

- Centralized agent configuration

  The centralized agent configuration feature moves most of the agent configuration properties from the `AMAgent.properties` file to the Federated Access Manager centralized data repository.

  An agent administrator can then manage the multiple agent configurations from a central server location, using either the Federated Access Manager Administration Console or the `famadm` command-line utility.

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

  - The properties required for the agent to start up and initialize itself are stored in the `FAMAgentBootstrap.properties` file locally on the server where the agent is installed. For example, the agent profile name and password used to access the Federated Access Manager server are stored in the bootstrap file.
  - The rest of the agent properties are stored either centrally in the Federated Access Manager data repository (centralized configuration option) or locally in the `FAMAgentConfiguration.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 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).

- Hot-swappable agent configuration properties

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

- One-level wildcard support in URL policy and not enforced URLs

  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 agent installation option with minimal questions asked during the installation

  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.
- Option to create the agent profile during installation

  The 3.0 agent installer supports an option to create the agent profile in the Federated Access Manager server during the agent installation so you don't have to create the profile manually using the Federated Access Manager Console or CLI.
- Property name changes

  Version 3.0 web agent property names have been changed to correspond to J2EE agent property names. The same names are now used for properties that are common to both web and J2EE agents.
- 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 Web Server 7.0 Agent

Supported Platforms for the Web Server 7.0 Agent

The Web Server 7.0 agent is supported on these platforms:

- Solaris OS on SPARC platforms, versions 9 and 10 (32–bit/64–bit)
- Solaris OS on x86 platforms, versions 9 and 10 (32–bit/64–bit)

- Red Hat Enterprise Linux Advanced Server 4.0 and 5.0 (32–bit/64–bit)
- Windows 2003, Enterprise Edition (32–bit/64–bit)
- Windows 2003, Standard Edition (32–bit/64–bit)

Note: Web Server 7.0 runs as a 32-bit application on Windows and Linux systems.

Supported Deployment Containers for the Web Server 7.0 Agent

You can deploy the Web Server 7.0 agent on the following deployment containers. The links are to the Web Server documentation collections.

- Sun Java System Web Server 7.0: `http://docs.sun.com/coll/1308.3`
- Sun Java System Web Server 7.0 Update 1: `http://docs.sun.com/coll/1653.1`
- Sun Java System Web Server 7.0 Update 2: `http://docs.sun.com/coll/1653.2`

Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4

Access Manager 7.1 and Access Manager 7 2005Q4 are compatible with version 3.0 policy agents. However, because Access Manager does not support centralized agent configuration, a version 3.0 agent deployed with Access Manager must store its configuration data locally in the `FAMAgentBootstrap.properties` and `FAMAgentConfiguration.properties` files.

The `com.sun.am.policy.agents.config.repository.location` property in the Federated Access Manager server Agent Service schema (`AgentService.xml` file) specifies where the agent configuration data is stored:

- `local`: Configuration data is stored locally in the `FAMAgentConfiguration.properties` file on the server where the agent is deployed.
- `centralized`: Configuration data is stored remotely in the Federated Access Manager central data repository.

For both configurations, the `FAMAgentBootstrap.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

Federated Access Manager 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, Federated Access Manager 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 Web Server 7.0 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:**
   - Solaris SPARC systems (32–bit): `sjsws_v70_SunOS_sparc_agent_3.zip`
   - Solaris SPARC systems (64–bit): `sjsws_v70_SunOS_x86_64_agent_3.zip`
   - Solaris x86 systems (32–bit): `sjsws_v70_SunOS_x86_agent_3.zip`
   - Solaris x86 systems (64–bit): `sjsws_v70_SunOS_x86_64_agent_3.zip`
   - Linux systems: `ssjsws_v70_Linux_agent_3.zip`
   - Windows systems: `sjsws_v70_WINNT_agent_3.zip`

   These distribution files are available from the OpenSSO project site:

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

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

File or Directory *PolicyAgent-base*/web_agents/sjsws_agent	Description
README.txt and license.txt	Readme and license files
/bin	agentadmin and agentadmin.bat programs
/config	Template, properties, and XML files
/data	license.log file. Do not edit this file.
/etc	Empty
/lib	Required library and JAR files
/locale	Required properties files
/logs	Log files

Creating an Agent Profile

A web agent uses an agent profile to communicate with Federated Access Manager server. A version 2.2 web agent could use the default agent profile (UrlAccessAgent). A version 3.0 agent, however, must create an agent profile using any of these methods:

- Use the Federated Access Manager Console, as described in "Creating an Agent Profile" on page 8.
- Use the famadm command-line utility with the create-agent subcommand. For more information about the famadm command, see the *Federated Access Manager 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 Federated Access Manager Console

1. **Login into the Federated Access Manager 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 `FAMAgentConfiguration.properties` file on the server where the agent is installed.
   - `Centralized`: In the Federated Access Manager server central configuration data repository.

7. **In the `Server URL` field, enter the Federated Access Manager server URL.**

   For example: `http://fam.example.com:8080/fam`

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 `famadm` command-line utility to edit the agent profile. For more information, see the *Federated Access Manager 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 Web Server 7.0 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 Federated Access Manager server during the installation.

▼ To Create a Password File

1. **Create an ASCII text file for the agent profile. For example:** `ws7agentpw`

2. **If you want the `agentadmin` program to automatically create the agent profile in Federated Access Manager 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 Federated Access Manager, including:

- **Agent management**: Use the agent administrator to manage agents either in the Federated Access Manager Console or by executing the `famadm` 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 Federated Access Manager 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 Federated Access Manager 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 Federated Access Manager 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 Web Server 7.0 Agent

Gathering Information to Install the Web Server 7.0 Agent

The following table describes the information you will need to provide when you run the `agentadmin` program to install Web Server 7.0 agent. For some `agentadmin` prompts, you can accept the default value displayed by the program, if you prefer.

TABLE 1 Information Required to Install the Web Server 7.0 Agent

Prompt Request	Description
Sun Java System Web Server Config Directory Path	Complete path to the directory used by Web Server to store its configuration files. For example: `/opt/sun/webserver7/https-agenthost/config`
Federated Access Manager URL	For example: `http://fam.example.com:8080/fam`
Agent URL	For example: `http://agent.example.com:8090`
Encryption Key	Key used to encrypt the agent profile password. The encryption key must be at least 7 characters long. You can accept the default key or create a new key using the `agentadmin --getEncryptKey` command. Applies only to the custom installation option.
Agent Profile Name	A policy agent communicates with Federated Access Manager server using the name and password in the agent profile. For information, see "Creating an Agent Profile" on page 8. For example: `WS7Agent`
Agent Profile Password File	ASCII text file with only one line specifying the agent profile password. You create the agent profile password file as a pre-installation step. For information, see "Creating a Password File" on page 9.
Option to create the agent profile The `agentadmin` program displays the following prompt if the agent profile previously specified for the Agent Profile Name prompt does not already exist in Federated Access Manager: `Enter true if the Agent Profile is being created into Federated Access Manager 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 Federated Access Manager and must have agent administrative privileges. For information see, "Creating an Agent Administrator" on page 10. If you prefer, you can also specify `amadmin` as this user. ■ Path to the agent administrator password file. For information, see "Creating a Password File" on page 9.

Installing the Web Server 7.0 Agent Using the `agentadmin` Program

Before you install the Web Server 7.0 agent:

- A Federated Access Manager server instance must be installed.
- The Web Server 7.0 instance must be installed and configured on the server where you plan to install the agent.
- You have downloaded and unzipped the agent distribution file, as described in "Downloading and Unzipping the Agent Distribution File" on page 7.

▼ To Install the Web Server 7.0 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 Web Server 7.0 instance.

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

   PolicyAgent-base`/web_agents/sjsws_agent/bin`

3. **Stop the Web Server 7.0 instance.**

4. **Start the agent installation:**

   ```
   # ./agentadmin --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
   ---------------------------------------------
   Sun Java System Web Server Config Directory :
   /opt/SUNWwbsvr7/https-agenthost/config
   Access Manager URL : http://famhost.example.com:8080/fam
   Agent URL : http://agenthost.example.com:8090
   Encryption Key : Cj6ThCocoqGAwy5V4Zsjjd8/cZ7KcZdd
   Agent Profile name : WS7Agent
   Agent Profile Password file name : /tmp/ws7agentpw
   Agent Profile will be created right now by agent installer : true
   Agent Administrator : amadmin
   ```

```
Agent Administrator's password file name : /tmp/amadminpw

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]:
```

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/Agents30/web_agents/sjsws_agent/Agent_001/config/FAMAgentBootstrap.properties
Agent Configuration Tag file location
/opt/Agents30/web_agents/sjsws_agent/Agent_001/config/FAMAgentConfiguration.properties
Agent Audit directory location:
/opt/Agents30/web_agents/sjsws_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/Agents30/web_agents/sjsws_agent/Agent_001/logs/debug

Install log file location:
/opt/Agents30/web_agents/sjsws_agent/installer-logs/audit/custom.log

Thank you for using Sun Federated Access Manager Policy Agent. INSTALL NOTE:
Installer modifies obj.conf file in the config directory you specified. To
make agent changes effective do Pull and deploy configuration using Web
Server Admin Console or CLI. If there are multiple obj.conf files already
present, then manually add agent settings to the required obj.conf files.
UNINSTALL NOTE: Uninstall removes agent settings from obj.conf file in the
config directory you specified. If there are multiple obj.conf files
configured manually in the same config directory, then please remove them
manually. For more information, please refer agent documentation.
```

All files are under the *PolicyAgent-base*/web_agents/sjsws_agent/ directory, where *PolicyAgent-base* is where you unzipped the agent distribution file.

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

PolicyAgent-base/web_agents/sjsws_agent/logs/audit

8 Restart the Web Server 7.0 instance that is being protected by the policy agent.

Note – After you install the Web Server 7.0 agent for a specific domain, you cannot use that same agent on the same host for a different domain. To use the Web Server 7.0 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 Web Server 7.0 Agent

```
***************************************************************************
Welcome to the Sun Federated Access Manager Policy Agent for Sun Java System
Web Server.
***************************************************************************

Enter the complete path to the directory which is used by Sun Java System Web
Server to store its configuration Files. This directory uniquely
identifies the Sun Java System Web Server instance that is secured by this
Agent.
[ ? : Help, ! : Exit ]
Enter the Sun Java System Web Server Config Directory Path
[/var/opt/SUNWwbsvr7/https-agenthost.example.com/config]:
/opt/SUNWwbsvr7/https-agenthost/config

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

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

Enter a valid Encryption Key.
[ ? : Help, < : Back, ! : Exit ]
Enter the Encryption Key [Cj6ThCocoqGAwy5V4Zsjjd8/cZ7KcZdd]:

Enter the Agent profile name
[ ? : Help, < : Back, ! : Exit ]
Enter the Agent Profile name: WS7Agent

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/ws7agentpw

WARNING:
Agent profile/User: WS7Agent does not exist in Federated Access
Manager! 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 Federated Access Manager after
installation".


Enter true if the Agent Profile is being created into Federated Access
Manager by the installer. Enter false if it will be not be created by
installer.
[ ? : Help, < : Back, ! : Exit ]
This Agent Profile does not exist in Federated Access Manager, 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: amadmin

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/amadminpw

---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
Sun Java System Web Server Config Directory :
/opt/SUNWwbsvr7/https-agenthost/config
Access Manager URL : http://famhost.example.com:8080/fam
Agent URL : http://agenthost.example.com:8090
Encryption Key : Cj6ThCocoqGAwy5V4Zsjjd8/cZ7KcZdd
Agent Profile name : WS7Agent
Agent Profile Password file name : /tmp/ws7agentpw
Agent Profile will be created right now by agent installer : true
Agent Administrator : amadmin
Agent Administrator's password file name : /tmp/amadminpw

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

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

```
Reading data from file /tmp/ws7agentpw and encrypting it ...DONE.

Generating audit log file name ...DONE.

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

Creating the Agent Profile WS7Agent ...DONE.

Creating a backup for file
/opt/SUNWwbsvr7/https-agenthost/config/obj.conf ...DONE.

Creating a backup for file
/opt/SUNWwbsvr7/https-agenthost/config/magnus.conf ...DONE.

Adding Agent parameters to
/opt/SUNWwbsvr7/https-agenthost/config/magnus.conf file ...DONE.

Adding Agent parameters to
/opt/SUNWwbsvr7/https-agenthost/config/obj.conf file ...DONE.

SUMMARY OF AGENT INSTALLATION
-----------------------------
Agent instance name: Agent_001
Agent Bootstrap file location:
/opt/Agents30/web_agents/sjsws_agent/Agent_001/config/FAMAgentBootstrap.properties
Agent Configuration Tag file location
/opt/Agents30/web_agents/sjsws_agent/Agent_001/config/FAMAgentConfiguration.properties
Agent Audit directory location:
/opt/Agents30/web_agents/sjsws_agent/Agent_001/logs/audit
Agent Debug directory location:
/opt/Agents30/web_agents/sjsws_agent/Agent_001/logs/debug

Install log file location:
/opt/Agents30/web_agents/sjsws_agent/installer-logs/audit/custom.log

Thank you for using Sun Federated Access Manager Policy Agent. INSTALL NOTE:
Installer modifies obj.conf file in the config directory you specified. To
make agent changes effective do Pull and deploy configuration using Web
Server Admin Console or CLI. If there are multiple obj.conf files already
present, then manually add agent settings to the required obj.conf files.
UNINSTALL NOTE: Uninstall removes agent settings from obj.conf file in the
config directory you specified. If there are multiple obj.conf files
configured manually in the same config directory, then please remove them
manually. For more information, please refer agent documentation.
```

After You Finish the Install

Agent Instance Directory: The installation program creates the following directory for each Web Server 7.0 agent instance:

PolicyAgent-base/web_agents/sjsws_agent/Agent_*nnn*

where:

- *PolicyAgent-base* is where you unzipped the agent distribution 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 FAMAgentBootstrap.properties and FAMAgentConfiguration.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 Web Server 7.0 Agent

Installing the Web Server 7.0 Agent on Multiple Web Server 7.0 Instances

After you install the Web Server 7.0 agent for a specific Web Server 7.0 instance, you can install the agent on another Web Server 7.0 instance by executing the agentadmin program again for that instance.

Installing Web Server 7.0 Agent on the Federated Access Manager Host Server

Installing the Web Server 7.0 agent on the Federated Access Manager host server is not recommended in a production deployment because performance can be degraded.

However, if you do install the agent on the Federated Access Manager host server on the same Web Server 7.0 instance, add the URLs related to Federated Access Manager to the not enforced URL list. If you are installing the agent on a different Web Server 7.0 instance, configuration of the not enforced URL list is not required.

▼ To Configure the Not Enforced URL List

1. **Login into the Administration Console as** `amAdmin`**.**
2. **Under** `Access Control`**,** *realm-name*`,` `Agents`**, and** `Web`**, click the name of the agent you want to configure.**

   The Console displays the `Edit` page for the agent.
3. **Under** `Non Enforcement`**, add the URLs related to Federated Access Manager to the** `Not Enforced URL List .`
4. **Click** `Save`**.**

Post-Installation Tasks for the Web Server 7.0 Agent

Changing the Password for an Agent Profile

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

▼ To Change the Password for an Agent Profile

1. **On the Federated Access Manager server:**
   a. **Login into the Administration Console as** `amAdmin`**.**
   b. **Under** `Access Control`**,** *realm-name*`,` `Agents`**, and** `Web`**, click 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 Web Server 7.0 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*`/web_agents/sjsws_agent/bin` **directory.**

      PolicyAgent-base is where you unzipped the agent distribution file.

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

```
#./agentadmin --encrypt Agent_002 /tmp/ws7agentpw
```

`Agent_002` 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/FAMAgentBootstrap.properties` file, set the following property to the new encrypted password from the previous step. For example:**

```
com.sun.am.policy.am.password=/54GwN432q+MEnfh/AHLMA==
```

e. **Restart the Web Server 7.0 instance that is being protected by the policy agent.**

Using SSL With the Web Server 7.0 Agent

During the agent installation, if you specify the `HTTPS` protocol, the Web Server 7.0 agent is automatically configured and ready to communicate over Secure Sockets Layer (SSL). Before continuing with the tasks in this section, ensure that the Web Server 7.0 instance is configured for SSL. For information, see `http://docs.sun.com/doc/820-2202/gbthq?a=view`.

The SSL related tasks in this section include:

- "To Install the Federated Access Manager Root CA Certificate on a Remote Web Server 7.0 Instance" on page 20
- "To Configure Notifications For the Web Server 7.0 Agent" on page 20
- "To Disable the Trust Behavior of the Web Server 7.0 Agent" on page 21

▼ To Install the Federated Access Manager Root CA Certificate on a Remote Web Server 7.0 Instance

- **The root CA certificate that you install on the remote Web Server 7.0 instance must be the same certificate that is installed on the Federated Access Manager server.**

  To install the Federated Access Manager root CA certificate on Web Server 7.0, see the Web Server 7.0 documentation: `http://docs.sun.com/doc/820-2202/gbrtm?l=ru[amp ]a;=view`

▼ To Configure Notifications For the Web Server 7.0 Agent

1 **Add the Web Server 7.0 root CA certificate to the Federated Access Manager certificate database.**

2. **Mark the root CA certificate as trusted to enable Federated Access Manager to successfully send notifications to the Web Server 7.0 agent.**

▼ To Disable the Trust Behavior of the Web Server 7.0 Agent

By default, an agent installed on a remote Web Server 7.0 instance trusts any server certificate presented over SSL by the Federated Access Manager host. The web agent does not check the root CA certificate. If the Federated Access Manager host is SSL-enabled and you want the Web Server 7.0 agent to perform certificate checking, you can disable this behavior.

- **In the Web Server 7.0 agent's `FAMAgentBootstrap.properties` file, set the following properties, depending on the requirements for your deployment.**

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

  - Disable the option to trust server certificate sent over SSL by the Federated Access Manager host:

    ```
    com.sun.identity.agents.config.trust.server.certs = false
    ```

  - Set the certificate database directory. For example:

    ```
    com.sun.identity.agents.config.sslcert.dir =
    /var/opt/SUNWwbsvr7/https-agent-host.example.com/config
    ```

  - 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 =
    https-agent-host.example.com.host-
    ```

  - Set the certificate database password:

    ```
    com.sun.identity.agents.config.certdb.password = password
    ```

  - Set the certificate database alias:

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

Preserving POST Data For Web Server 7.0

Only the Web Server 7.0 agent supports POST data preservation. Other web agents do not support this feature. POST data is submitted to Web Server 7.0 through HTML forms before users log into Federated Access Manager. An HTML page containing the HTML form should be in the not enforced list. By default, POST data preservation is disabled.

▼ To Enable POST Data Preservation for the Web Server 7.0 Agent

1. **Login to the Federated Access Manager Console as `amadmin`.**

2. **Under** `Access Control`, *realm-name*, `Agents`, **and** `Web`, **click the name of the agent you want to configure.**

3. **Click** `Advanced`, **and then** `Post Processing`.

4. **On the** `Edit` **agent page:**

   a. **For** `POST Data Preservation`, **check** `Enabled`.

   b. **For** `POST Data Entries Cache Period`, **specify a value in minutes, if you want a value other than the default value of 10.**

      This value determines the time in minutes that POST data is valid in the Web Server 7.0 cache.

   c. **Click** `Save`.

Both values are hot-swappable, which means you don't have to restart Web Server 7.0 after you set them.

Managing the Web Server 7.0 Agent

Federated Access Manager 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:

- Federated Access Manager Administration Console

  You can manage both version 3.0 J2EE and web agents from the Federated Access Manager 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.

- `famadmn` command-line utility

  The `famadmn` utility is available on the Federated Access Manager server after you install the tools and utilities in the `famAdminTools.zip` file. The `famadm` 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 `famadm` utility, including the syntax for each subcommand, see the *Federated Access Manager 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 are deploying the agent with Access Manager 7.1 or Access Manager 7 2005Q4, which do not support centralized agent configuration.

The following property in the Federated Access Manager 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 `FAMAgentConfiguration.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 `FAMAgentBootstrap.properties` file. The agent uses information in the bootstrap file to start and initialize itself and to communicate with Federated Access Manager 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 Web Server 7.0 Agent

Preparing to Uninstall the Web Server 7.0 Agent

▼ To Prepare to Uninstall Web Server 7.0 Agent

1. **Undeploy any applications protected by the Web Server 7.0 agent.**
2. **Stop the Web Server 7.0 instance, if it is running.**

Uninstalling the Web Server 7.0 Agent Using the `agentadmin` Program

▼ To Uninstall the Web Server 7.0 Agent

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

   PolicyAgent-base`/web_agents/sjsws_agent/bin`

   where *PolicyAgent-base* is where you unzipped the agent distribution 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. **The `uninstall` program prompts you for the Web Server configuration directory path.**

   Default: `/var/opt/SUNWwbsvr7/https-`*agenthostname*`/config`

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

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

Example 2 Uninstallation Sample for the Web Server 7.0 Agent

```
************************************************************************
Welcome to the Federated Access Manager Policy Agent for Sun Java System Web Server If
the Policy Agent is used with Federation Manager services, User needs to
enter information relevant to Federation Manager.
************************************************************************
Enter the complete path to the directory which is used by Sun Java
System Web Server to store its configuration Files. This directory
uniquely identifies the Sun Java System Web Server instance that is
secured by this Agent.
[ ? : Help, ! : Exit ]
Enter the Sun Java System Web Server Config Directory Path
[/var/opt/SUNWwbsvr7/https-agenthost/config]:

---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
Sun Java System Web Server Config Directory :
```

```
/var/opt/SUNWwbsvr7/https-agenthost/config

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

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*`/web_agents/sjsws_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.

Migrating a Version 2.2 Web Server 7.0 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 Web Agents" on page 4.

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 `FAMAgentBootstrap.properties` and `FAMAgentConfiguration.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 Web Server 7.0 agent, download the version 3.0 Web Server 7.0 agent.

2. On the Federated Access Manager server, run the `famadm` utility to create the new version 3.0 agent configuration in the centralized agent configuration repository.

   Therefore, the `famadm` utility must be installed from the `famAdminTools.zip` file on the Federated Access Manager server. For information, see "Installing the Federated Access Manager Utilities and Scripts" in the *Sun Federated Access Manager 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 WS7v3Agent 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 19.

▼ 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 Web Server 7.0 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 Web Server 7.0 agent in the `v30agent` directory:

   ```
   cd /v30agent/web_agents/sjsws_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/web_agents/sjsws_agent
   ...
   ```

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

   The `agentadmin` program migrates the version 2.2 agent.

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

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

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

      For example:

      `com.sun.identity.agents.config.username = WS7v3Agent`

9. **Copy the `Agent_`*nnn*`/config/FAMAgentConfiguration.properties` file to the `/bin` directory where `famadm` is installed on the Federated Access Manager server.**

10. **In `FAMAgentConfiguration.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 Federated Access Manager server, create a password file for the Federated Access Manager 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 Federated Access Manager server, run `famadm` to create a new agent configuration in the Federated Access Manager centralized agent configuration repository. For example:**

```
cd tools_zip_root/fam/bin
./famadm create-agent -b WS7v3Agent -t WebAgent -u amadmin
-f /tmp/amadminpw -D ./FAMAgentConfiguration.properties
```

    In this example:

    - `tools_zip_root` is the directory where you unzipped `famAdminTools.zip`.
    - `WS7v3Agent` is the version 3.0 agent configuration name.
    - `WebAgent` is the agent type for J2EE agents.
    - `/tmp/amadminpw` is the path to the `amadmin` password file.

    Caution: After you run `famadm`, you might want to delete `FAMAgentConfiguration.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 Web Server 7.0 instance for the migrated agent.**

Next Steps After you migrate the agent, you can manage the new 3.0 agent configuration using the Federated Access Manager Administration Console or the `famadmn` utility, as described in "Managing the Web Server 7.0 Agent" on page 22.

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
820-4579-05	July 15, 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 Federated Access Manager Policy Agent 3.0 Guide for Web Server 7.0*, and the part number is 820-4579-05.