Sun Federated Access Manager Policy Agent 3.0 Guide for Sun Java System Application Server 8.1/8.2/9.0/9.1

Beta

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

Part No: 820–4578–05
June 25, 2008

080625@20490

Sun Federated Access Manager Policy Agent 3.0 Guide for Sun Java System Application Server 8.1/8.2/9.0/9.1

Early Access (EA) release. Last revised June 25, 2008

The Sun Java™ System Application Server 8.1/8.2/9.0/9.1 policy agent is a version 3.0 J2EE agent that functions with Sun™ Federated Access Manager to protect applications and resources such as HTML files, servlets, JSPs, and EJBs deployed on Application Server, as well as on Glassfish, the open source application server.

This agent supports Application Server 8.1, 8.2, 9.0, and 9.1. Version 2.2 agents also exist for Application Server 8.1 and Application Server 8.2/9.0/9.1. However, to use the new version 3.0 features described in "What's New in Version 3.0 Policy Agents" on page 4, you must deploy the version 3.0 Application Server 8.1/8.2/9.0/9.1 agent.

This guide provides specific information about the Application Server 8.1/8.2/9.0/9.1 agent, including:

What's New in Version 3.0 Policy Agents

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

- Centralized agent configuration

  The centralized agent configuration feature moves most of the agent configuration properties from the `AMAgent.properties` file to the Federated Access Manager central 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 agent administrator no longer needs to edit an agent's `AMAgent.properties` file.

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

  - The 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).

- More hot-swappable agent configuration properties

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

- One-level wildcard support in URL policy

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

- Default J2EE 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 in the server 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 `famadm` utility.

- Automated migration support

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

Supported Platforms, Compatibility, and Coexistence for the Application Server 8.1/8.2/9.0/9.1 Agent

Supported Platforms for the Application Server 8.1/8.2/9.0/9.1 Agent

The Application Server 8.1/8.2/9.0/9.1 agent is supported on these platforms:

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

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

Supported Deployment Containers for the Application Server 8.1/8.2/9.0/9.1 Agent

You can deploy the Application Server 8.1/8.2/9.0/9.1 agent on these deployment containers:

- Sun Java System Application Server 8.1, 8.2, 9.0, and 9.1. For documentation, see:
  - Application Server 8.1: `http://docs.sun.com/coll/1343.1`
  - Application Server 8.2: `http://docs.sun.com/coll/1343.2`
  - Application Server 9.0: `http://docs.sun.com/coll/1343.3`
  - Application Server 9.1: `http://docs.sun.com/coll/1343.4`
- Glassfish, the Open Source Application Server for the Java Enterprise Edition (EE) 5 platform. For information, see:
  - Glassfish project: `http://glassfish.dev.java.net`

Compatibility With Access Manager 7.1 and Access Manager 7 2005Q4

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

The `com.sun.identity.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 in the Federated Access Manager centralized 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 Application Server 8.1/8.2/9.0/9.1 Agent

Setting Your `JAVA_HOME` Environment Variable

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

Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File

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

1. **Login into the server where you want to install the agent.**
2. **Create a directory to unzip the `appserver_v9_agent.zip` distribution file.**
3. **Download and unzip the `appserver_v9_agent.zip` distribution file from the OpenSSO project site:**

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

The following table shows the layout after you unzip the `appserver_v9_agent.zip` file. *PolicyAgent-base* is where you unzipped the distribution file.

File or Directory *PolicyAgent-base*`/j2ee_agents/appserver_v9_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`	Agent application (`agentapp.war`) For information, see "Deploying the Agent Application" on page 20.
`/lib`	Required JAR files
`/locale`	Required properties files
`/logs`	Log files
`/sampleapp`	Policy agent sample application. For information, see "Deploying the Policy Agent Sample Application" on page 24.

Creating a Password File

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

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

▼ To Create a Password File

1. **Create an ASCII text file for the agent profile. For example:** `/tmp/as91agentpw`
2. **If you want the** `agentadmin` **program to automatically create the agent profile in 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.

Creating an Agent Profile

The Application Server 8.1/8.2/9.0/9.1 agent uses an agent profile to communicate with Federated Access Manager server. You can create an agent profile using any of these methods:

- Create the agent profile during installation when you run the agentadmin program with the --custom-install option. The program prompts you for this information:
  - Agent profile name and path to the agent profile password file
  - Agent administrator name and path to the agent administrator password file
- Use the Federated Access Manager Console, as described in "Creating an Agent Profile" on page 10.
- Use the famadm command-line utility with the create-agent subcommand. For more information about the famadm command, see the *Sun Federated Access Manager 8.0 Administration Reference*.

▼ To Create an Agent Profile in the Federated Access Manager Console

1. **Login into the Federated Access Manager Administration Console as** `amAdmin`**.**
2. **Under** `Access Control`**,** *realm-name*`,` `Agents`**, and** `J2EE`**, click** `New`**.**
3. **In the** `Name` **field, enter the name for the new agent profile. For example:** `AS9Agent`
4. **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.
5. **In the** `Server URL` **field, enter the Federated Access Manager server URL.**

   For example: `http://famhost.example.com:8080/fam`
6. **In the** `Agent URL` **field, enter the URL for the agent application (**`agentapp`**).**

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

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

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

   If you prefer, you can also use the `famadm` command-line utility to edit the agent profile. For more information, see the *Sun Federated Access Manager 8.0 Administration Reference*.

Installing the Application Server 8.1/8.2/9.0/9.1 Agent

Gathering Information to Install the Application Server 8.1/8.2/9.0/9.1 Agent

The following table describes the information you will need to provide when you run the `agentadmin` program to install the Application Server 8.1/8.2/9.0/9.1 agent. For some `agentadmin` prompts, you can accept the default value displayed by the program, if you prefer.

TABLE 1 Information Required to Install the Application Server 8.1/8.2/9.0/9.1 Agent

Prompt Request	Description
Application Server Configuration Directory	Path to the directory used by Application Server to store its configuration files. Applies to both default and custom installation options. Default: `/var/opt/SUNWappserver/domains/domain1/config`
Application Server Instance Name	Name of the Application Server instance secured by this agent. Applies only to the custom installation option. Default: `server`
Access Manager URL	URL where Federated Access Manager is running. Applies to both default and custom installation options. For example: `http://famhost.example.com:8080/fam`
Is the agent installed on the DAS host for a remote instance?	Default: `false` See "Installing the Agent on the Domain Administration Server (DAS)" on page 19. Applies only to the custom installation option.
Agent URL	Applies to both default and custom installation options. Agent protected Application Server URL For example: `http://agenthost.example.com:8090/agentapp` **Note**: The version 3.0 `agentadmin` program does not prompt you for the deployment URI for the agent application, because `/agentapp` is combined with this URL.
Encryption Key	Key used to encrypt the agent profile password. The encryption key should be at least 12 characters long. You can accept the default key or create a new key using the `agentadmin --getEncryptKey` command. Applies only to the custom installation option.

TABLE 1 Information Required to Install the Application Server 8.1/8.2/9.0/9.1 Agent *(Continued)*

Prompt Request	Description
Agent Profile Name	A policy agent communicates with Federated Access Manager using the name and password in the agent profile. Applies to both default and custom installation options. For information, see "Creating an Agent Profile" on page 10.
Agent profile password file	ASCII text file with only one line specifying the agent profile password. You create the agent profile password file as a pre-installation step. Applies to both default and custom installation options. For information, see "Creating a Password File" on page 8.
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 9. 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 8. Applies only to the custom installation option.

Installing the Application Server 8.1/8.2/9.0/9.1 Agent Using the `agentadmin` Program

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

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

or

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

Before you install the Application Server 8.1/8.2/9.0/9.1 agent:

- A Federated Access Manager server instance must be installed and running.
- The Application Server deployment container must be installed and configured on the server where you plan to install the agent.
- You must have downloaded and unzipped the distribution file, as described in "Downloading and Unzipping the `appserver_v9_agent.zip` Distribution File" on page 7.

▼ To Install the Application Server 8.1/8.2/9.0/9.1 Agent Using the `agentadmin` Program

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

Important: To install the agent, you must have write permission to the Application Server agent deployment container files and directories.

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

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

3 Change to the following directory:

PolicyAgent-base`/j2ee_agents/appserver_v9_agent/bin`

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

```
# chmod 755 agentadmin
```

5 Stop the Application Server deployment container.

6 Start the agent installation:

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

or

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

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

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

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

```
-----------------------------------------------
SUMMARY OF YOUR RESPONSES
-----------------------------------------------
Application Server Config Directory :
/opt/SUNWappserver/domains/domain1/config
Application Server Instance name : server
Federated Access Manager URL : http://famhost.example.com:8080/fam

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

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

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

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

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

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

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

PolicyAgent-base/j2ee_agents/appserver_v9_agent/logs/audit

10 **Restart the Application Server deployment container.**

Note – After you install the Application Server 8.1/8.2/9.0/9.1 agent for a specific domain, you cannot use that same agent on the same host for a different domain. To use the Application Server 8.1/8.2/9.0/9.1 agent for another domain on the same host, you must install the agent specifically for that domain.

Example 1 Sample agentadmin Program Installation for the Application Server 8.1/8.2/9.0/9.1 Agent

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

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

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

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

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

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

```
Agent URL: http://agenthost.example.com:8090/agentapp

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

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

Enter the path to a file that contains the password to be used for identifying
the Agent.
[ ? : Help, < : Back, ! : Exit ]
Enter the path to the password file: as91agentpw

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

---------------------------------------------
SUMMARY OF YOUR RESPONSES
---------------------------------------------
Application Server Config Directory :
/opt/SUNWappserver/domains/domain1/config
Application Server Instance name : server
Federated Access Manager URL : http://famhost.example.com:8080/fam

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

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

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

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

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

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

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

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

Generating audit log file name ...DONE.

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

Creating the Agent Profile AS91Agent ...DONE.

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

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


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

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

Thank you for using Sun Federated Access Manager Policy Agent 3.0.
```

After You Finish the Install

Agent Instance Directory

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

PolicyAgent-base/j2ee_agents/appserver_v9_agent/Agent_*nnn*

where:

- *PolicyAgent-base* is where you unzipped the appserver_v9_agent.zip file.
- *nnn* identifies the agent instance as Agent_001, Agent_002, and so on for each additional agent instance.

Each agent instance directory contains the following subdirectories:

- /config contains the configuration files for the agent instance, including 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 Sun Java System Application Server 8.1/8.2/9.0/9.1 Agent

Installing the Agent on the Domain Administration Server (DAS)

The Domain Administration Server (DAS) is a specific Sun Java System Application Server instance that has administration capabilities for a specific domain. Each domain has its own DAS instance with a unique port number. The default administrative domain is named domain1, and the default port number is 4848.

The DAS authenticates the administrator, accepts console and command-line requests from administrator, and then communicates with server instances in the domain to carry out the requests. The DAS is sometimes referred to as the admin server or the default server. It is called the default server because it is the only server instance that gets created during an Application Server installation.

Note – Deploy the Application Server 8.1/8.2/9.0/9.1 agent on the DAS instance only for evaluation or prototype deployments. In a production environment, it is recommended that you create a separate Application Server instance to deploy the agent and the resources you want to protect.

For more information about the DAS, see the *Application Server 9.1 Administration Guide* in the following documentation collection: `http://docs.sun.com/coll/1343.4`.

Post-Installation Tasks for the Application Server 8.1/8.2/9.0/9.1 Agent

Required Post-Installation Tasks for the Application Server 8.1/8.2/9.0/9.1 Policy Agent

Deploying the Agent Application

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

▼ To Deploy the Agent Application

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

PolicyAgent-base`/j2ee_agents/appserver_v9_agent/etc/agentapp.war`

where *PolicyAgent-base* is where you unzipped the `appserver_v9_agent.zip` distribution file.

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

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

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

Installing the Agent Filter for the Application Server 8.1/8.2/9.0/9.1Agent

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

▼ To Install the Agent Filter

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

If the application is deployed, undeploy it before continuing.

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

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

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

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

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

Note: Application Server 8.1/8.2/9.0/9.1 supports the Java Servlet specification version 2.4. Version 2.4 is fully backward compatible with version 2.3. Therefore, all existing servlets should work without modification or recompilation.

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

Specify the `<filter>`, `<filter-mapping>`, and `<dispatcher>` elements immediately after the `<web-app>` element. For example:

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

```
        <dispatcher>INCLUDE</dispatcher>
        <dispatcher>FORWARD</dispatcher>
        <dispatcher>ERROR</dispatcher>
    </filter-mapping>
...
</web-app>
```

4 **Deploy (or redeploy) the application on Application Server 8.1/8.2/9.0/9.1.**

The agent filter is added to the application.

Next Steps You can also protect an application with J2EE declarative security. To learn more about protecting your application with J2EE declarative security, consider deploying the sample application. For information, see "Deploying the Policy Agent Sample Application" on page 24.

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

Optional Post-Installation Tasks for the Application Server 8.1/8.2/9.0/9.1 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** `J2EE`**, click the name of the agent profile you want to update.**

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

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

d. Click `Save`**.**

2 On the server where the Application Server 8.1/8.2/9.0/9.1 agent is installed:

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

b. Change to the *PolicyAgent-base*`/j2ee_agents/appserver_v9_agent/bin` **directory.**

where *PolicyAgent-base* is where you unzipped the `appserver_v9_agent.zip` distribution file.

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

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

For example:

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

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

```
ASEWEJIowNBJHTv1UGD324kmT==
```

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

e. Restart the Application Server deployment container.

Creating the Necessary URL Policies

If the Application Server 8.1/8.2/9.0/9.1 agent is configured to operate in the `URL_POLICY` or `ALL` filter mode, you must create the appropriate URL policies. For instance, if Application Server 8.1/8.2/9.0/9.1 is available on port 8080 using the HTTP protocol, you must create at minimum, a policy to allow access to the following resource:

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

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

If no policies are defined and the agent is configured to operate in the `URL_POLICY` or `ALL` filter mode, then no user is allowed access to the resources protected by the Application Server 8.1/8.2/9.0/9.1 agent.

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

Deploying the Policy Agent Sample Application

After you install the Application Server 8.1/8.2/9.0/9.1 agent, consider deploying the J2EE policy agent sample application to help you better understand the key features, functions, and configuration options of J2EE agents, including:

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

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

After you install the Application Server 8.1/8.2/9.0/9.1 agent, the sample application is available as:

PolicyAgent-base`/j2ee_agents/appserver_v9_agent/sampleapp/dist/agentsample.ear`

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

Managing the Application Server 8.1/8.2/9.0/9.1 Agent

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

- 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 *Sun 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 deploy 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 Application Server 8.1/8.2/9.0/9.1 Agent

Preparing to Uninstall the Application Server 8.1/8.2/9.0/9.1 Agent

▼ To Prepare to Uninstall Application Server 8.1/8.2/9.0/9.1 Agent

1. **Undeploy any applications protected by the Application Server 8.1/8.2/9.0/9.1 agent.**
2. **Restore the deployment descriptors of these applications to their original deployment descriptors. (Backup files are useful here if you have them.)**
3. **Conditionally, if you are permanently removing the Application Server 8.1/8.2/9.0/9.1 agent, undeploy the agent application.**

   However, if you plan to re-install this agent , you don't need to undeploy the agent application.

4 **Ensure that the following server instances are stopped:**

- Domain Administration Server (DAS)
- Application Server deployment container

Uninstalling the Application Server 8.1/8.2/9.0/9.1 Agent Using the `agentadmin` Program

▼ To Uninstall the Application Server 8.1/8.2/9.0/9.1 Agent

1 **Change to the following directory:**

PolicyAgent-base`/j2ee_agents/appserver_v9_agent/bin`

where *PolicyAgent-base* is where you unzipped the `appserver_v9_agent.zip` file.

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

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

or

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

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

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

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

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

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

Example 2 Uninstallation Sample for the Application Server 8.1/8.2/9.0/9.1 Agent

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

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

```
[/var/opt/SUNWappserver/domains/domain1/config]: /opt/SUNWappserver/domains/domain1/config

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

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

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

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

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

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

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

Thank you for using Sun Federated Access Manager Policy Agent 3.0.
```

After You Finish the Uninstall

- The `/config` directory is removed from the agent instance directory, but the `/logs` directory still exists.
- The `uninstall` program creates an uninstall log file in the *PolicyAgent-base*`/j2ee_agents/appserver_v9_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 Application 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 features, described in "What's New in Version 3.0 Policy Agents" on page 4.

The migration process migrates the agent's binary files, updates the agent's 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 Application Server 8.2/9.0/9.1 agent, download the version 3.0 Application Server 8.1/8.2/9.0/9.1 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 AS9v3Agent in the examples. The old version 2.2 and new version 3.0 agent profile passwords are the same. If you need to change the password for the new version 3.0 agent profile, see "Changing the Password for an Agent Profile" on page 22.

▼ To Migrate a Version 2.2 Agent:

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

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

2 Stop the Application Server deployment container for the version 2.2 agent.

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

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

   The version 3.0 agents are available from the OpenSSO project site:
   `https://opensso.dev.java.net/public/use/index.html`

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

   For example, if you downloaded and unzipped the version 3.0 Application Server 8.1/8.2/9.0/9.1 agent in the `v30agent` directory:

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

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

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

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

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

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

   The `agentadmin` program migrates the version 2.2 agent.

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 = AS9v3Agent
      ```

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 AS9v3Agent -t J2EEAgent -u amadmin
-f /tmp/amadminpw -D ./FAMAgentConfiguration.properties
```

In this example:

- `tools_zip_root` is the directory where you unzipped `famAdminTools.zip`.
- `AS9v3Agent` is the version 3.0 agent configuration name.
- `J2EEAgent` is the agent type for J2EE agents.
- `/tmp/amadminpw` is the path to the `amadmin` password file.

Caution: After you run `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 Application Server deployment container 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 Application Server 8.1/8.2/9.0/9.1 Agent" on page 24.

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
820-4578-05	June 25, 2008	Early Access (EA) release draft

Sun Welcomes Your Comments

Sun is interested in improving its documentation and welcomes your comments and suggestions. To share your comments, go to `http://docs.sun.com/` and click `Feedback`. In the online form, provide the full document title and part number. The part number is a 7-digit or 9-digit number that can be found on the title page or in the document's URL. For example, the title of this guide is *Sun Federated Access Manager Policy Agent 3.0 Guide for Application Server 8.1/8.2/9.0/9.1*, and the part number is 820-4578-05.