Policy Agent Pack Guide

Sun™ ONE Identity Server 5.1

Version 1.1

816-5428-10
November 2002
Third Edition

Contents

About This Guide

This *Policy Agent Pack Guide* offers an introduction to Sun™ ONE Identity Server Policy Agent and describes how to install URL policy agents on Web and Proxy Servers.

This preface contains the following sections:

- What You Are Expected to Know
- Sun ONE Identity Server Documentation Set
- What's in This Guide
- Documentation Conventions Used in This Manual
- Related Information

What You Are Expected to Know

This book is considered to be an auxiliary manual in the documentation series provided with Sun ONE Identity Server 5.1 (formerly known as iPlanet Directory Server Access Management Edition or DSAME). It is essential that you understand directory technologies and have some experience with Java and XML programming languages. You will get the most out of this guide if you are familiar with directory servers and Lightweight Directory Access Protocol (LDAP). Particularly, you should be familiar with Sun ONE Directory Server and the documentation provided with that product.

This guide is intended for use by IT professionals who manage access to their network through Sun ONE servers and services. The functionality contained in Sun ONE Identity Server allows you to manage user data and enforce access policies throughout your enterprise.

As you try to understand the concepts described in this guide, you should reference the *Sun ONE Identity Server Installation and Configuration Guide* and the *Sun ONE Identity Server Programmer's Guide.*

Sun ONE Identity Server Documentation Set

This book is considered an auxiliary manual in the documentation series provided with Sun ONE Identity Server. The Sun ONE Identity Server documentation set contains the following titles:

- *Installation and Configuration Guide* describes Sun ONE Identity Server and provides details on how to plan and install Sun ONE Identity Server on Solaris and Windows 2000 platforms.
- *Administration Guide* documents how to manage user and service data in an Sun ONE Identity Server system once it has been installed.
- *Programmer's Guide* documents how to customize DSAME interfaces.
- *Sun ONE Identity Server Policy Agent Pack Guide (*this guide) documents how to install Sun ONE Identity Server Policy Agent on Web and Proxy Servers.
- The *Release Notes* file gathers an assortment of information, including a description of what is new in this release, last minute installation notes, known problems and limitations, and how to report problems.

NOTE Be sure to check the Sun ONE Identity Server documentation web site for updates to the release notes and for revisions to the guides.

`http://docs.sun.com/db/coll/S1_s1IdServ_51`

What's in This Guide

The following table lists all the Agents documented in this Guide.

Table 1 Agents Documented in this Guide

Agents	Platforms
iPlanet Web Server 6.0 SP*x*	Solaris 8
iPlanet Web Server 4.1 SP8	Solaris 8
iPlanet Proxy Server 3.6	Solaris 8

Table 1 Agents Documented in this Guide

Agents	Platforms
Microsoft IIS 5.0	Windows 2000
iPlanet Web Server 6.0 SP2	Windows 2000
Microsoft IIS 4.0	Windows NT 4.0
Apache 1.3.22 from Red Hat	Linux 7.2
Apache 1.3.26	Solaris 8 and 9
Lotus Domino 5.0.10	Windows 2000
Sun ONE Web Server 6.0 SP*x*	Solaris 9
IBM HTTP Server 4.0.3 AE	Solaris 8

Documentation Conventions Used in This Manual

In this guide, there are certain typographic and terminology conventions used to simplify discussion and to help you better understand the material. These conventions are described below.

Typographic Conventions

This book uses the following typographic conventions:

- *Italic type* is used within text for book titles, new terminology, emphasis, and words used in the literal sense.
- `Monospace font` is used for sample code and code listings, API and language elements (such as function names and class names), filenames, pathnames, directory names, HTML tags, and any text that must be typed on the screen.
- *Italic serif font* is used within code and code fragments to indicate variable placeholders. For example, the following command uses *filename* as a variable placeholder for an argument to the gunzip command:

  `gunzip -d` *filename*`.tar.gz`

Terminology

Below is a list of the general terms that are used in the Sun ONE Identity Server documentation set:

- *DSAME* refers to Sun ONE Identity Server and any installed instances of the Sun ONE Identity Server software.
- *Policy and Management Services* refers to the collective set of Sun ONE Identity Server components and software you have installed and running a dedicated web server. The dedicated web server is installed for you automatically when you install the Policy and Management Services.
- *Web server that runs Sun ONE Identity Server services* refers to the dedicated web server where the Policy and Management Servers are installed.
- *Directory Server* refers to an installed instance of Sun ONE Directory Server.
- *Agent_Install_Dir* is a variable placeholder for the directory where you have installed the URL Policy Agent.
- *Web_Server_root* is a variable placeholder for the home directory where you have installed Web Server.
- *DSAME_Install_Dir* is a variable placeholder for the home directory where you have installed Sun ONE Identity Server.

Related Information

In addition to the documentation provided with DSAME, you should be familiar with several other sets of documentation that can be used with this book. Of particular interest are Sun ONE Web Server and Sun ONE Proxy Server documentation sets. You can access these on the Internet at the following URLs:

Sun ONE Web Server Documentation

You can find the Sun ONE Web Server documentation at the following web site:

`http://docs.sun.com/db/prod/s1websrv`

Sun ONE Proxy Server Documentation

You can find the Sun ONE Proxy Server documentation at the following web site:

`http://docs.sun.com/prod/s1.webproxys`

Other Sun ONE Product Documentation

Documentation for all Sun ONE servers and technologies can be found at the following web site:

`http://docs.sun.com`

Chapter 1

Read This First

This chapter provides a brief overview of Policy Agents, as well as some concepts you will need to understand before proceeding with the Installation program.

Topics include:

- How Policy Agents Work
- Supported Servers
- Before You Begin Installation

How Policy Agents Work

Sun ONE Identity Server Policy Agents protect content on your web servers and Proxy Servers from unauthorized intrusions. They control access to services and web resources based on the policies configured by an administrator.

Uses for Policy Agents

Policy agents are installed on web servers for a variety of reasons. Here are three examples:

- An agent on a Human Resources server prevents non-Human Resources personnel from viewing confidential salary information and other sensitive data.
- An agent on an Operations web server allows only network administrators to view network status reports or to modify network administration records.

- An agent on an Engineering web server allows authorized personnel from many internal segments of a company to publish and share research and development information. At the same time, the agent restricts external partners from gaining access to the proprietary information.

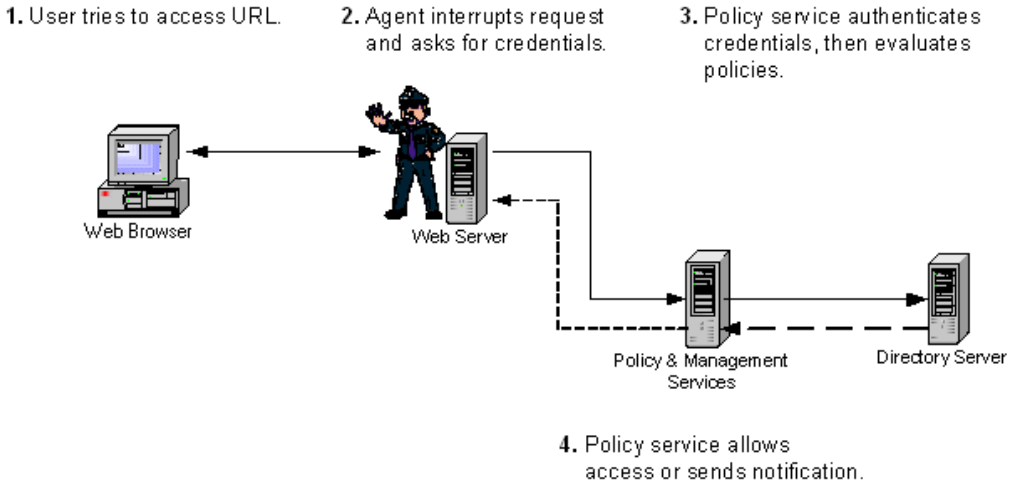
In each of these situations, a system administrator must set up policies that allow or deny users access to content on a web server. For information on setting policies and for assigning roles and policies to users, see the *Sun ONE Identity Server Administration Guide.*

How an Agent Interacts with Identity Server

Figure 1-1 illustrates how a Policy Agent installed on a remote web server interacts with Sun ONE Identity Server. When a user points a browser to a particular URL on a protected web server, the following interactions take place:

1. The agent intercepts the request and validates the existing authentication credentials. If the existing authentication level is insufficient, the appropriate Identity Server authentication service will present a login page. The login page prompts the user for credentials such as username and password.
2. The authentication service verifies that the user credentials are valid. For example, the default LDAP authentication service verifies that the username and password are stored in Sun ONE Directory Server. You might use other authentication modules such as RADIUS or Certificate modules. In such cases, credentials are not verified by Directory Server but are verified by the appropriate authentication module.
3. If the user's credentials are properly authenticated, the Policy Agent examines all the roles assigned to the user.
4. Based on the aggregate of all policies assigned to the user, the individual is either allowed or denied access to the URL.

Figure 1-1 An agent's interaction with Identity Server Policy and Management Services.



Supported Servers

Policy Agent Pack 1.1 supports the following servers running on the Solaris 8 platform:

- iPlanet Web Server 6.0 SPx
- iPlanet Web Server 4.1 SP8
- iPlanet Proxy Server 3.6
- Apache 1.3.12

Policy Agent Pack 1.1 supports the following servers running on the Windows 2000 platform:

- Microsoft IIS 5.0
- iPlanet Web Server 6.0 SP2

Policy Agent Pack 1.1 supports the following servers running on the Windows NT platform:

- Microsoft IIS 4.0

Policy Agent Pack 1.1 supports the following servers running on the Solaris 9 platform:

- iPlanet Web Server 6.0 SPx
- Apache 1.3.22

Other independent agents are:

- Apache 1.3.22 from Red Hat on Linux 7.2 platform
- Apache 1.3.26 on Solaris 8 and 9 platforms
- Lotus Domino 5.0.10 on Windows 2000 platform
- IBM HTTP Server 1.3.19 on Solaris 8 platform

Before You Begin Installation

The following are issues or concepts that you should be familiar with before you start the Installation program:

- Java Runtime Environment (JRE) 1.3.1_04 Requirement
- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Installing Multiple Web Server Agents on the Same Computer System
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache
- Global Not-Enforced List
- The AMAgent.properties File
- Verifying a Successful Installation

Java Runtime Environment (JRE) 1.3.1_04 Requirement

You must have the Java Runtime Environment (JRE) 1.3.1_04 or higher version installed or available on a shared file system in order to run the graphical user interface (GUI) version of the Agent Installation program.

If you are using the Solaris operating system, and JRE 1.3.1_04 is not available, you can use the command-line version of the Agent Installation program.

If you are running the Windows operation system, the Installation program will install JRE 1.3.1_04 if it is not detected.

The Web Server that Runs Identity Server Services vs. Remote Web Servers

You can use the Installation program install a Policy Agent on the web server where Identity Server is installed. In Sun ONE documentation, this server is referred to as the *web server that runs the Identity Server services*.You can also use the Installation program to install additional Policy Agents on remote web servers in your enterprise. A *remote* web server in a Identity Server deployment is any web server other than the one that runs Sun ONE Identity Server policy and management services. It is “remote” relative to the Identity Server-dedicated web server.

Installing Multiple Web Server Agents on the Same Computer System

If you have multiple web servers or Proxy servers installed on one computer system, you can install a different agent for each server or server instance. Note that since only one instance of Microsoft IIS server can be installed per computer system, you cannot install multiple Microsoft IIS agents on the same computer system.

For more information, see “Installing Multiple Web Server Agents on the Same Solaris Computer System” on page 38.

Providing Failover Protection for Identity Server Agents

When you install a Policy agent, you can specify a *failover* or backup web server for running the Sun ONE Identity Server Policy and Management services. This is essentially a high availability option. It ensures that if the web server the runs Identity Server service becomes unavailable, the agent can still process access requests through the secondary or failover web server running Identity Server service.

To set up failover protection for the Policy Agent, you must first install two different instances of Identity Server on two separate web servers. See the detailed instructions in the *Sun ONE Identity Server Installation and Configuration Guide*. Then follow the instructions in the subsequent sections of this manual to install the appropriate Agent. The agent Installation program will prompt you for the host name and port number of the failover web server you configured to work with Identity Server.

NOTE The protocol (for example, http or https) must be the same for both primary web server and the failover web server.

Updating the Agent Cache

Each agent maintains a cache that stores the policies for each user session. The cache can be updated by either a polling mechanism or a notification mechanism. By default the polling mechanism is enabled.

NOTE The iPlanet Proxy server agent does not maintain any cache.

Polling Cache Updates

In the *polling* mode, the agent sends a request (polls) to the Identity Server for any session and policy changes after a specified interval of time. The agent then updates the cache with the information received from the poll.

The agent uses the polling mechanism to update the cache when the property `com.iplanet.am.policy.cAPI.notification.enable` is set to `FALSE` in the `AMAgent.properties` file.

The following two properties are activated in the `AMAgent.properties` file when the agent is in polling mode:

`com.iplanet.am.policy.cAPI.cacheUpdateInterval`

`com.iplanet.am.policy.cAPI.cacheEntryLifeTime`

The `com.iplanet.am.policy.cAPI.cacheUpdateInterval` property specifies the interval, in minutes, after which the agent performs a cleanup operation to remove all the stale entries in the cache. By default, this property is set to a polling interval of 120 minutes.

The com.iplanet.am.policy.cAPI.cacheEntryLifeTime property determines the amount of time an entry remains valid after it has been added to the cache. The value of the property represents the number of minutes the entry remains valid. After this time has elapsed, this entry in the cache will be ignored and re-fetched from the Identity Server. The default value for this property is 3 minutes.

Notification Cache Updates

In the *notification* mode, the agent gets notified by the Identity Server session service about session changes. Session changes include events such as a session log-out or a session time-out. When notified of a session change, the agent updates the corresponding entry in the cache.

The agent uses the notification mechanism to update the cache when the property com.iplanet.am.policy.cAPI.notification.enable is set to TRUE in the AMAgent.properties file.

Restrictions due firewalls, as well as the type of web server in use, may not allow notifications to work in certain situations. In such cases, polling is the only way an agent can update its cache.

NOTE The notification support is not available in the following instances:

- If IIS 4.0 or IIS 5.0 is using HTTPS
- If both the Apache 1.3.12 server and the Identity Server are using HTTPS
- If you are using iPlanet Proxy Server

Global Not-Enforced List

The *global not-enforced list* defines the resources that should not have any policies (either allow or deny) associated with them.

By default, a policy agent denies access to all resources for the web server that it protects. However, various resources available through a web server (such as a web site or application) might not need to have any policy enforced. Common examples of such resources include the HTML pages and .gif images found in the Welcome menu for a web site. The user should be able to browse such pages without authenticating. These resources need to be on the global not-enforced list. Only one of the following two properties in AMAgent.properties file will be used for this purpose:

com.iplanet.am.policy.agents.url.notenforcedlist.local

com.iplanet.am.policy.agents.url.notenforcedlist.remote

The property you use depends on where the agent is installed relative to the Identity Server.

Using com.iplanet.am.policy.agents.url.notenforcedlist.local

If the Identity Server and Policy agent are running on the same web server, use the `com.iplanet.am.policy.agents.url.notenforcedlist.local` property to read the list of resources that has no policy enforced on them. The default value in the list defines a set of resources that are used by the Identity Server services. Add to this list by separating additional items with commas. Wild cards can be used in the expressions that are used in global not-enforced list.

NOTE This list is used only in the following instances:

- When an iPlanet Web Server 6.0 agent is installed on the Identity Server.
- When you are using an iPlanet Proxy Server 3.6 agent

Using com.iplanet.am.policy.agents.url.notenforcedlist.remote

If the agent and Sun ONE Identity Server are running on different web servers, use the `com.iplanet.am.policy.agents.url.notenforcedlist.remote` property to maintain the global not-enforced list. Additions to this list must be separated by commas. Wild cards can be used in the expressions that are used in global not-enforced list.

NOTE You cannot use this list in the following instances:

- When an iPlanet Web Server 6.0 agent is installed on the Identity Server.
- When you are using an iPlanet Proxy Server 3.6 agent.

The AMAgent.properties File

The `AMAgent.properties` file stores configuration parameters used by the Policy Agent. From time to time, you may need to make changes to the default parameters in this file. For example, when you want to specify a different failover web server for running Identity Server services, or when you want to enable validation by agent on client IP addresses.

The `AMAgent.properties` file includes information for the following configurations:

- debugging

- policy agent
- Identity Server services
- policy API
- service and agent deployment descriptors
- session failover

The `AMAgent.properties` file also contains configuration information on advanced features, such as forwarding LDAP user attributes via `HTTP` headers, client IP address validation, and so on. The `AMAgent.properties` file has comments before each property; refer to the file for more details.

Table 1-1 provides the default location for `AMAgent.properties` on the various supported servers.

Table 1-1 Locating AMAgent.properties on different platforms

Server	Location
All Supported UNIX web servers	`/etc/opt/SUNWam/conf/`*WebServer*`/_`*PathInstanceName*`/config/` Here, *WebServer* can be: •`iWS60` •`iWS41` •`Proxy` •`APACHE`
iPlanet Web Server 6.0 Windows 2000	`\`*Agent_Install_Dir*`\Agents\iws60\web-apps\agent\WEB-INF\config\`
Microsoft IIS 5.0 Windows 2000	`\`*Agent_Install_Dir*`\Agents\iis50\config\`
Microsoft IIS 4.0 Windows NT	`\`*Agent_Install_Dir*`\Agents\iis40\config\`
Apache 1.3.22 from Red Hat	`/`*Agent_Install_Dir*`/apagent/conf`
Apache 1.3.26	`/etc/opt/SUNWam/conf/APACHE/_`*PathInstanceName*`/`
Lotus Domino 5.0.10	`\`*Agent_Install_Dir*`\Agents\domino\config`
IBM HTTP Server 1.3.19	`/etc/opt/SUNWam/conf/IBMHTTP/_opt_IBMHTTPD_conf/`

Changing that `AMAgent.properties` file can have serious and far-reaching effects. Remember that you can safely change many of the properties in this file by simply re-installing the agent. However, if you must make manual changes, keep the following in mind:

- Make a backup copy of this file before you make changes.
- Trailing spaces are significant; use them judiciously.
- Use forward-slash (/) to separate directories, not back-slash (\). This holds true even on Windows systems.
- Spaces in the Windows file names are allowed.

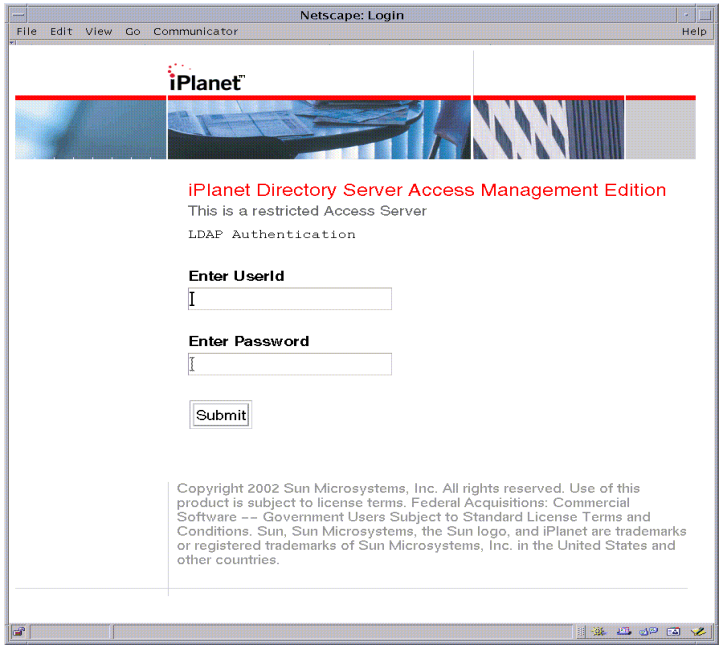
NOTE If you make changes to the `AMAgent.properties` file, you must restart the web server to make your changes take effect.

Verifying a Successful Installation

After installing a Policy Agent, it is good practice to make sure that the agent was installed successfully and works as you expect it to work. There are two things you can check to verify a successful agent installation.

First, try to access some web content on the web server where the agent is installed. If the agent is installed correctly, you should see the Identity Server login page. Figure 1-2 is an example of a Identity Server login page that uses LDAP authentication. Secondly, check the `AMAgent.properties` file. Make sure that each property is set properly.

Figure 1-2 The Sun ONE Identity Server Login page



Chapter 2

Policy Agent Pack 1.1 on Solaris 8

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server (also referred as DSAME) to grant or deny user access to web servers in an enterprise. The Policy Agent Pack 1.1 provides a set of policy agents for use with various web and proxy servers. This chapter explains how to install and configure the policy agents for servers running on the Solaris 8 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Installing Multiple Web Server Agents on the Same Solaris Computer System
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses

Before You Begin

Be sure that you are familiar with the concepts presented in Chapter 1, “Read This First.” The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement

- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Installing Multiple Web Server Agents on the Same Computer System
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache
- Global Not-Enforced List
- The AMAgent.properties File

Supported Solaris Web Servers

Policy Agent Pack 1.1 supports the following servers running on the Solaris 8 operating system:

- iPlanet Web Server 6.0 SP*x*
- iPlanet Web Server 4.1 SP8
- iPlanet Proxy Server 3.6
- Apache 1.3.12

Patch Cluster for Solaris

- When running Apache 1.3.12 Web Server on Solaris 8 operating system, you must ensure that the recommended patch cluster 109234-09 is installed. You can download this patch from: `http://sunsolve.sun.com`.

Using the Graphical User Interface (GUI) Version of the Installation Program

The GUI version of the Installation program allows you to install only one policy agent at a time.

Installing a Web Server Policy Agent

Use these instructions for installing agents on the following servers using the Solaris 8 operating system:

- iPlanet Web Server 4.1

- iPlanet Web Server 6.0
- Apache web server 1.3.12

To Install a Web Server Policy Agent

You must have root permissions when you run the agent Installation program.

1. Unpack the product binaries file using the following command:

   ```
   # gunzip -dc agents-RTM
   Candidate-domestic-us.sparc-sun-solaris2.8.tar.gz | tar -xvof -
   ```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

   ```
   # ./setup
   ```

3. In the Welcome page, click Next.
4. Read the License Agreement. Click Yes to agree to the license terms.
5. When prompted, provide the following information about the web server this agent will protect:

   Install DSAME agent in this directory: Enter the full path to the directory where you want this agent to be installed, and then click Next.

   Select the desired component: Mark the check box of the agent you want to install, and then click Next.

NOTE Only one agent can be installed at a time.

   Host Name: Enter the fully qualified domain name of the machine where the web server is installed. For example, `mycomputer.siroe.com`.

   Web Server Instance Directory: This prompt displays only if you have selected an iPlanet Web Server agent. Specify the web server instance that this agent will protect. Enter the full path to the directory where the web server instance is located. Example:

Web_Server_root/`https-mycomputer.siroe.com`

Apache Config File Location: This prompt displays only if you've selected the Apache web server agent. Specify the web server that this agent will protect. Enter the full path to the directory where the `httpd.conf` file is located.

Web Server Port: Enter the port number for the web server that will be protected by the agent.

Web Server Protocol: If the web server has been configured for SSL, choose HTTPS; otherwise choose HTTP.

Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`.

The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

When all the information is entered correctly, click Next.

6. Enter information about the web server that runs DSAME policy and management services. The Policy Agent will connect to this server.

   DSAME Services Host: Enter the fully qualified domain name of the system where the primary web server that runs DSAME services is installed. For example, `myserver.siroe.com`.

   DSAME Services Port: Enter the port number for the web server that runs DSAME services.

   DSAME Services Protocol: If the web server that runs DSAME services is SSL-enabled, select HTTPS; otherwise select HTTP.

   DSAME Services Deployment URI: Enter the location that was specified when DSAME was installed. The default Universal Resource Identifier (URI) for DSAME is `/amserver`.

   Failover Server Host: Enter the fully qualified name for the secondary web server that will run DSAME services if the primary web server becomes unavailable. If no failover host exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that runs DSAME services. If no failover host exists, then leave this field blank.

   When all the information is entered correctly, click Next.

7. Review the Installation Summary to be sure that the information you've entered is correct. If you want to make changes, click Back. If all the information is correct, click Next.
8. In the Ready to Install page, click Install Now.
9. When the installation is complete, you can click Details to view details about the installation, or click Exit to end the Installation program.
10. You must restart your iPlanet Web Server or Apache web server for the installation to be complete.

Installing a Proxy Server Policy Agent

Use these instructions for installing a Policy Agent on iPlanet Proxy Server 3.6 on the Solaris 8 operating system.

To Install a Proxy Server Policy Agent

You must have root permissions when you run the agent Installation program.

1. Unpack the product binaries file using the following command:

```
# gunzip -dc agents-RTM
Candidate-domestic-us.sparc-sun-solaris2.8.tar.gz | tar -xvof -
```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You will find the program in the directory where you untarred the binaries file. At the command line, enter the following:

```
# ./setup
```

3. In the Welcome page, click Next.
4. Read the License Agreement. Click Yes to agree to the license terms.
5. To search for the directory where you would like to install the agent, click Browse. To accept the default, click Next.
6. Select the component DSAME Agent for iPlanet Proxy Server 3.6, and then click Next.

NOTE Only one component can be installed at a time.

7. When prompted, provide the following information about the web server where this agent will be installed:

   Host Name: Enter the fully qualified domain name of the system where the remote web server is installed. For example, `mycomputer.siroe.com`.

   Proxy Server Instance Directory: Enter the full path to the directory where the iPlanet Proxy Server instance is located. For example:

proxy_server_root_dir/proxy-*mycomputer*-proxy

Proxy Server Port: Enter the port number for the Proxy server instance. If you login to Proxy Server on the local machine as admin, you can click on the Proxy Server instance and check the port number.

Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is /amagent.

The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

When all the information is entered correctly, click Next.

8. When prompted, provide the following information about the web server that runs DSAME services.

   DSAME Services Host: Enter the fully qualified domain name of the system where the primary web server that runs DSAME services is installed. For example, myserver.siroe.com.

   DSAME Services Port: Enter the port number for the primary web server that runs DSAME services.

   DSAME Services Protocol: If the web server that runs DSAME services has been configured for SSL select HTTPS; otherwise select HTTP.

   DSAME Services Deployment URI: Enter the location that was specified when DSAME was installed. The default Universal Resource Identifier (URI) for DSAME is /amserver.

   Failover Server Host: Enter the fully qualified name for the secondary web server that will run DSAME services if the primary web server becomes unavailable. If no failover host exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that will run DSAME services. If no failover host exists, then leave this field blank.

   When all the information is entered correctly, click Next.

9. Click Install Now.

10. When the installation is complete you may review the details or click Exit.

11. Restart the Proxy Server.

Uninstalling a Policy Agent

To uninstall an agent, you must run the Uninstallation program. Follow the steps below:

1. In the directory where the agent is installed, at the command line, enter the following command:

   ```
   # ./uninstall_agent
   ```

2. Click Next on Welcome Panel.
3. On Type of Install Panel, select Full.
4. Click Uninstall Now.
5. Click Exit after uninstallation is complete.

In the directory where the product binary file is unpacked (and where the installation program was invoked), there is another uninstallation program named `uninstall`. The `uninstall` program can be used to detect and uninstall all agents that were previously installed using the `setup` program; even agents that were installed on a remote machine. Invoke `uninstall` using the following command:

```
# ./uninstall
```

On the other hand, `uninstall_agent` will uninstall only the agent (or agents) that were previously installed with the `setup` program in the current directory.

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

To Install an Agent Using the Command Line

1. In the directory where you unpacked the binaries file, at the command line, enter the following:

   ```
   # setup -nodisplay
   ```

2. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement? Enter yes.

   Install DSAME Agent in this directory: Enter the full path to the directory in which you want to install the policy agent.

   The following text displays:

```
 [ ]  1  DSAME Agent for iPlanet Web Server 6.0 SPx
 [ ]  2  DSAME Agent for iPlanet Web Server 4.1 SP8
 [ ]  3  DSAME Agent for iPlanet Proxy Server 3.6
 [ ]  4  DSAME Agent for Apache 1.3.12
DSAME Agent components showing a checked box will be installed.
Only one agentmay be installed at a time.
```

   To check a particular component, enter its number, or 0 when you are finished: Enter the number that corresponds to the policy agent you want to install. The following message displays, with a checkmark beside the server your specified.

```
[X]  1  DSAME Agent for iPlanet Web Server 6.0 SPx
[ ]  2  DSAME Agent for iPlanet Web Server 4.1 SP8
[ ]  3  DSAME Agent for iPlanet Proxy Server 3.6
[ ]  4  DSAME Agent for Apache 1.3.12
```

   To check a particular component, enter its number, or 0 when you are finished: Enter 0 to continue.

3. Provide the following information about the iPlanet Web Server this agent will protect:

   - `Hose Name`
   - `Web Server Port`
   - `Web Server Protocol`

- `iPlanet Web Server Instance Directory`

For more information on each of these items, see “Installing a Web Server Policy Agent,” on page 28.

4. Provide the following information about the web server that runs DSAME Services:
   - `Host Name`
   - `Port Number`
   - `Protocol`
   - `Deployment URI`
   - `Failover Host`
   - `Failover Port`
   - `amAdmin Password`

   For more information on each of these items, see “Installing a Web Server Policy Agent,” on page 28.
5. The following text displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation
```

When prompted, **What would you like to do?**, enter 1 to start the installation.

To Uninstall an Agent Using the Command Line

1. From the directory where the agent is installed, enter the following command at the command line:

   ```
   # ./uninstall_agent -nodisplay
   ```

NOTE You can also use the `uninstall` command from the directory where the product was originally installed (this is the directory from where you ran the `setup` command). To uninstall an agent from the original installation directory, enter the following command:

```
# ./uninstall -nodisplay
```

If you have used the `uninstall_agent -nodisplay` command, the following text displays:

```
Please select the type of uninstall to perform from the following
choices:
1. Full
2. Partial
```

If you have used the `uninstall` command from the installation directory, a list of agents is displayed. From this list, select the agent that you wish to uninstall.

To remove the product and all of the components from your system, enter 1 for Full. To remove some, but not all, product components, enter 2 for Partial.

2. The following text displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
```

When prompted, **What would you like to do**? enter 1 to begin uninstallation.

3. The following text displays:

```
Product           Result     More Info
1. DSAME Agent    Full       Available
2. Done
```

To see log information on the agent, enter 1. To exit the Installation program, enter 2.

Installing Multiple Web Server Agents on the Same Solaris Computer System

To install multiple web server agents on a single computer system, use the graphical user interface (GUI) version of the Agent Installation program to install y the first agent. After the first agent is installed, you can then install successive agents using the `config` script. This script must be run from the command line as described in the next section.

To Install Multiple Web Server Agents on the Same Computer System

Once you have installed a agent on a system, you can install successive agents on that system using a script that copied to the system during the agent installation. The two scripts, `config` and `unconfig`, located in the following directory:

Agent_Install_Dir`/SUNWam/`*agent_directory*`/bin`

To install additional agents on a system after the original agent has been installed, run the `config` script from the `bin` directory using the following command:

```
# ./config
```

Follow the prompts to install the additional agents. For information on each of the prompts, see “Installing a Web Server Policy Agent,” on page 28. In general, information needs to be entered for both the protected web server instance and the DSAME server(s). The following text shows an example run:

```
# ./config
Enter the Web Server Instance Directory:
[/Web_Server_root/https-server_instance]
Enter the Local Hostname: [mycomputer.siroe.com]
Enter the Agent Web Server Port: [80]
Select Agent Web Server Protocol: [1] http [2] https-->[1]
Enter the Agent Deployment URI: [/amagent]
Enter the DSAME Service Host: [mycomputer.siroe.com]
Enter the DSAME Service Port: [58080]
Select DSAME Service Protocol: 1. http 2. https-->[1]
Enter the DSAME Deployment URI: [/amserver]
Enter the DSAME Failover Server Host: []
```

```
Enter the DSAME Failover Server Port: []
Configuring webserver ... Webserver version:  6.0
The directory /var/opt/SUNWam/agents/_opt_iws6a_https-server_instance
does not exist.
Creating it.
Deploying  web application
Loading  new configuration
Web application deploy successful

done
```

Using the config Script for Silent Installations

The `config` script can also be used to do silent, non-interactive agent installations. For details on its usage, use the `config -h` command to display details on the `config` command:

```
# ./config -h
Usage: config [ -r response_file | -R | -h ]
        -r specifies a response file.
        -R prints out the response file template.
        -h prints out this message.
```

In order to perform a silent installation, you must supply a *response file* for each of the agents you want to install. The command `config -R` indicates the fields which you must supply in the response file. This text file needs to be prepared before you begin the silent installation.

```
# ./config -R
Response file contains:
AGENT_HOST        # agent hostname
WS_INSTANCE_DIR   # iWS instance directory
AGENT_PORT        # agent server port
AGENT_PROTOCOL    # agent protocol: http|https
AGENT_DEPLOY_URI  # agent deploy URI
SERVER_HOST       # dsame server name
SERVER_PORT       # dsame server port
SERVER_PROTO      # dsame server protocol: http|https
SERVER_DEPLOY_URI # dsame server deploy URI
FAILOVER_S_HOST   # dsame fail over server name
FAILOVER_S_PORT   # dsame fail over server port
```

Here is an example response file, named `response.iws60`:

```
AGENT_HOST=mycomputer.siroe.com
WS_INSTANCE_DIR=
AGENT_PORT=80
AGENT_PROTOCOL=http
AGENT_DEPLOY_URI=/amagent
SERVER_HOST=mycomputer.siroe.com
SERVER_PORT=http
SERVER_PROTO=58080
SERVER_DEPLOY_URI=/amserver
FAILOVER_S_HOST=
FAILOVER_S_PORT=
```

Below is an example showing how the `config` script is used in conjunction with the `response.iws60` response file to complete a silent installation:

```
# ./config -r ./response.iws60
Configuring webserver ... Webserver version:  60
The directory /var/opt/SUNWam/agents/_opt_iws6a_https-server_instance
does not exist.
Creating it.
Deploying  web application
Loading  new configuration
Web application deploy successful

done
```

NOTE Be sure to use the `unconfig` script to uninstall any agent that was installed using the `config` script—you cannot use the GUI installation program to uninstall agents that were installed via the command line.

Removing an Agent Using the unconfig Script

To remove an agent that was installed from the command line using the `config` script, use the script `unconfig`. The `unconfig` script is located in the following directory:

Agent_Install_Dir`/SUNWam/`*agent_directory*`/bin`

Here is an example run of the `unconfig` script:

```
# ./unconfig /opt/iws6a/https-mycomputer.siroe.com
Unconfiguring webserver ... Deleting web application
Loading  new configuration
Web application delete successful
done.
```

Using Secure Sockets Layer (SSL) with an Agent

During installation, if you choose the HTTPS protocol, the agent is automatically configured and ready to communicate over SSL.

NOTE Before proceeding with the following steps, you should have a solid understanding of SSL concepts and the security certificates required to enable communication over the HTTPS protocol. See the documentation that comes with your web server. If you're using iPlanet Web Server, you can access the following documentation on the Internet:

`http://docs.sun.com/source/816-5691-10/esecurty.htm`

The Agent's Default Trust Behavior

By default, a policy agent is installed on a iPlanet Web Server 6.0 or Apache Server 1.3.12 that will trust any server certificate presented over SSL by the web server that runs DSAME services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs DSAME services is SSL-enabled, and you want the URL policy agent to perform certificate-checking, you must do two things:

1. Disable the agent's default trust behavior.
2. Install a CA certificate on the remote web server (where the agent is installed). The CA certificate must the be same one that is installed on the web server that runs DSAME service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default, it is set to `true`:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the web server must be the same one that is installed on the web server that runs DSAME services.

To Install the CA Certificate on iPlanet Web Server

See the instructions for installing a CA Certificate in the documentation that comes with the web server. In general, you install a CA Certificate through the web server's Administration console.

You can access the documentation for iPlanet Web Server 6.0 on the Internet at the following URL:

```
http://docs.sun.com/source/816-5691-10/esecurty.htm
```

To Install the CA Certificate on Apache 1.3.12

You can use the `certutil` program to install the CA Certificate on Apache 1.3.12.

1. In C shell, at the command line, enter the following commands:

   ```
   # cd /Agent_Install_Dir/SUNWam/apache1.3.12/cert
   # setenv LD_LIBRARY_PATH /Agent_Install_Dir/SUNWam/apache1.3.12/lib
   # export LD_LIBRARY_PATH
   # ./certutil -A -n cert-name -t "C,C,C" -d . -i cert-file
   ```

   In the commands above, the variables represent the following:

   - *cert-name* can be any name for this certificate.

- *cert-dir* is directory where the certificate-related files are located.
- *cert-file* is the base-64 encoded root certificate file.

For more information on the `certutil` utility, enter `certutil -H` for online Help.

2. To verify that the certificate is properly installed, at the command line, enter the following:

```
# ./certutil -L -d .
```

Trust database information will display including the name of the root CA certificate you installed. Example:

```
Certificate Name Trust Attrubutes

rootCAcert

p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

Setting the REMOTE_USER Server Variable

The `REMOTE_USER` server environment variable can be set to a DSAME authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

`REMOTE_USER` will be set while accessing allowed URLs.

To enable the `REMOTE_USER` setting for globally not-enforced URLs as specified in the `AMAgent.properties` file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the `AMAgent.properties` file to `TRUE` (by default, this value is set to `FALSE`):

`com.iplanet.am.policy.agents.anonRemoteUser.enable`

When you set this property value to TRUE, the value of REMOTE_USER will be set to the value contained in the following property in the AMAgent.properties file (by default, this value is set to anonymous):

com.iplanet.am.policy.agents.unauthenticatedUser

NOTE This feature is not available for the iPlanet Proxy Server Agent.

Forwarding LDAP User Attributes via HTTP Headers

DSAME agents has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of DSAME. A DSAME agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in AMAgent.properties file. To turn this feature on and off, use the following AMAgent.properties file property:

com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable

By default, this property is set to false, and the feature off. To turn on attribute forwarding, set this property to true. To configure the attributes that are to be forwarded in the HTTP headers, use the AMAgent.properties file property com.iplanet.am.policy.agents.ldapattr.

Below is an example section in the AMAgent.properties file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web
servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case
letters,
#       and any _ will become -
# NOTE: for IIS and Apache agents, "http_header_name" will be
prefixed
#       by HTTP_, and all lower case letters will become upper
case,
```

```
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organiza
tion-unit,o|organization,
c|country,mail|email,employeenumber|employee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the DSAME server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either DSAME User attributes or DSAME Dynamic attributes (for explanation of these two types of user attributes, refer to the DSAME *Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

Note that each web server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each property in the AMAgents.properties file.

NOTE This feature is not available for the iPlanet Proxy Server Agent.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or “hijacking” of SSO tokens.

The AMAgent.properties file contains a property titled com.iplanet.am.policy.agents.client_ip_validation.enable, which by default is set to false.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

This feature should not be used, however, if the client browser uses a web proxy or if there is a load-balancing application somewhere between the client browser and the agent-protected web server. In such cases, the IP address appearing in the request will not reflect the real IP address on which the client browser runs.

NOTE This feature is not available for the iPlanet Proxy Server Agent.

Chapter 3

Policy Agent Pack 1.1 on Windows 2000

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server (also referred as DSAME) to grant or deny user access to web servers in an enterprise. The Policy Agent Pack 1.1 provides a set of policy agents for use with various web and proxy servers. This chapter explains how to install and configure the policy agents for servers running on the Windows 2000 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses
- Troubleshooting the IIS Policy Agent

Before You Begin

Be sure that your are familiar with the concepts presented in Chapter 1, “Read This First.” The chapter includes brief but important information on the following topics:

- How Policy Agents Work

- Java Runtime Environment (JRE) 1.3.1_04 Requirement
- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Installing Multiple Web Server Agents on the Same Computer System
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache
- Global Not-Enforced List
- The AMAgent.properties File

Supported Windows Web Servers

The Agent Pack supports the following web servers on the Windows 2000 Server operating system:

- Microsoft IIS 5.0
- iPlanet Web Server 6.0 SP2

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version of the Installation program to install one agent at a time.

Installing the Policy Agent for Microsoft IIS

The IIS agent enforces policy on URL access for Microsoft's Internet Information Services (IIS) web server. The agent is an IIS ISAPI filter installed at the IIS web service level that will enforce policy on all IIS web sites. Technical considerations prevent the agent from being installed at the web site level.

Prior to installation, be sure that the entry for the system where the agent will be installed has a domain name set. If the web server that runs DSAME services is running on a separate system, make sure the server is also in the DNS query list.

To Install the Policy Agent on Microsoft IIS

You must have administrator privileges to run the installation program.

1. Unzip the product binaries file.
2. Run the Installation program by double-clicking `setup.exe`.
3. In the Welcome window, click Next.
4. Read the License Agreement. Click Yes to accept the license agreement.
5. Select the directory where you would like to install the agent by clicking Browse, or click Next to accept the default.
6. Select the component "DSAME Agent for IIS" and click Next.

NOTE Only one component can be installed at a time.

7. Enter the information about the web server where this agent will be installed:

   Host Name: Enter the fully qualified domain name of the system where the agent web server is installed. For example, `mycomputer.siroe.com`.

   Web Server Document Root: Enter the document root directory. This directory needs to accessible by the web server root `w3svc`.

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

   Web Server Protocol: If your web server has been configured for SSL, then select HTTPS; otherwise select HTTP.

   Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`.

The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an “Access denied” message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

When all the information is entered correctly, click Next.

8. Provide the following information about the web server that runs DSAME services:

   DSAME Services Host: Enter the fully qualified domain name of the system where the primary web server that runs DSAME services is installed. For example, `myserver.siroe.com`.

   DSAME Services Port: Enter the port number for the primary web server that runs DSAME services.

   DSAME Services Protocol: If the web server that runs DSAME services has been configured for SSL, then select HTTPS; otherwise select HTTP.

   DSAME Services Deployment URI: Enter the location that was specified when DSAME was installed. The default Universal Resource Identifier (URI) for DSAME is `/amserver`.

   Failover Server Host: Enter the fully qualified domain name for the secondary web server that will run DSAME services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that will run DSAME services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

9. If all the information entered is correct click Next.

10. Review your selections in the Summary panel and click Install Now.

11. When the installation is complete you may review the details, and then click Exit.

12. The installation modifies the system path by appending to it the location of the Agent libraries. In order for the change to take effect and for the Agent to work properly, you must reboot your computer. If you would like to reboot your computer immediately click Reboot Now in the popup window.

NOTE If the IIS 5.0 agent was previously installed and uninstalled on your machine, you do not need to reboot if you are installing the same IIS 5.0 agent in the same directory.

Installing the Policy Agent for iPlanet Web Server

You must have administrator privileges to run the Installation program.

To Install the Policy Agent on iPlanet Web Server

1. Unzip the product binaries file.
2. Run the Installation program by double-clicking `setup.exe`.
3. In the Welcome window, click Next.
4. Read the License Agreement. Click Yes to agree to the license terms.
5. Select the directory where you would like to install the agent by clicking Browse, or click Next to accept the default.
6. Select the component "DSAME Agent for iWS 6.0" and click Next.

NOTE Only one component can be installed at a time.

7. Provide the following information about the web server where this agent will be installed:

   Host Name: Enter the fully qualified domain name of the system where the agent web server is installed. For example, `mycomputer.siroe.com`.

   iPlanet Web Server Instance Directory: Enter the full path to the directory where the iPlanet Web Server instance is located. This is the web server instance that the agent will protect. For example, */Web_Server_root/*`https-mycomputer.siroe.com`.

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

Web Server Protocol: If the web server has been configured for SSL, then select HTTPS; otherwise select HTTP.

Agent Deployment URI: Enter a directory name. The default URI for the policy agent is `/amagent`.

The Universal Resource Identifier (URI) prefix tells the web server where to look for HTML pages the agent needs to display. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory denoted by this URI, will be created in the web server Document Root you supplied.

If all the information entered is correct, click Next.

8. Enter the information about the web server that runs DSAME services.

   DSAME Services Host: Enter the fully qualified domain name of the system where the primary web server that runs DSAME services is installed. For example, `myserver.siroe.com`.

   DSAME Services Port: Enter the port number for the primary web server that runs DSAME services.

   DSAME Services Protocol: If the web server that runs DSAME services has been configured for SSL, then select HTTPS; otherwise select HTTP.

   DSAME Services Deployment URI: Enter the location that was specified when DSAME was installed. The default Universal Resource Identifier (URI) for DSAME is `/amserver`.

   Failover Server Host: Enter the fully qualified domain name for the secondary web server that will run DSAME services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that will run DSAME services. If no failover server exists, then leave this field blank.

9. If all the information entered is correct click Next.

10. Click Install Now.

11. When the installation is complete you may review the details, and then click Exit.

12. You must restart your iPlanet Web Server for the installation to be complete.

Uninstalling and Disabling Policy Agents

Use the following procedure to uninstall a Policy Agent:

1. From the Start Menu, open Settings > Control Panel.
2. In the Control Panel, open Add / Remove Programs.
3. In the Add/Remove Programs window, choose iPlanet Directory Services Access Management Edition Agent 1.1.
4. Click Change/Remove.
5. Click Next on Welcome Panel.
6. On Type of Install Panel, select Full.
7. Click Uninstall Now.
8. Click Exit after uninstallation is complete.

Disabling a Policy Agent Installed on Microsoft IIS

Use the following steps to disable an agent on Microsoft IIS:

1. Launch Internet Services Manager.
   a. In the Start Menu, click Programs > Administrative Tools > Internet Services Manager.
2. Check the filter status.
   a. Open properties for the host computer in the Tree Pane of the Internet Services Manager window which is titled “Internet Information Services.”
   b. The host computer name should appear in the tree underneath the Internet Information Services root.
   c. Click Edit in the Master Properties section of the Internet Information Services tab.
   d. Select the ISAPI Filters tab in the WWW Service Master Properties dialog that appears.
   e. Highlight the filter named "DSAME IIS Agent.”

      You can click Edit to view the filter name and executable path. You’ll need this information when you want to re-enable the agent. Click Cancel to return to the program.
   f. Click Remove.

g. Click Apply and exit from the WWW Service Master Properties dialog.

h. Restart Microsoft IIS.

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

To Install an Agent Using the Command Line

1. In the directory where you unzipped the binaries file, at the command line, enter the following command:

   ```
   setup.bat -nodisplay
   ```

2. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement?

   Install DSAME Agent in this directory: Specify the directory where you want the agent to be installed. To accept the default directory that is displayed in brackets, press Enter. Otherwise, enter a full path.

3. The following text displays:

```
DSAME Agent components showing a checked box will be installed.
Only one agent may be installed at a time.
[ ]  1  DSAME Agent for IIS 5.0
[ ]  2  DSAME Agent for iPlanet Web Server 6.0 SP2
```

   First, do one of the following:

   - To install the agent for Microsoft IIS 5.0, enter 1.
   - To install the agent for iPlanet Web Server 6.0 SP2, enter 2.

   When a check mark appears beside your choice, enter 0 to continue.

4. When prompted, provide the following information about the web server instance this Agent will protect:

   - Host Name
   - Web Server Port
   - Web Server Protocol
   - iPlanet Web Server Instance Directory
   - Agent Deployment URI

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 48.

5. When prompted, provide the following information about the web server that runs DSAME Services:

   - Host Name
   - Port Number
   - Protocol
   - Deployment URI
   - Failover Host
   - Failover Port
   - amAdmin Password

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 48.

6. When displayed, review the summary of installation information you’ve specified. Press Enter to continue, or enter and exclamation point (!) to exit the program.

7. The following message displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation

What would you like to do
```

To continue with installation, enter 1.

8. When installation is complete, you must restart the web server.

To Uninstall an Agent Using the Command Line

1. In the *Agent_Install_Dir* directory, at the command line, enter the following command:

   ```
   java uninstall_DSAME_Agent -nodisplay
   ```

2. When prompted, provide the following information:

   Please select the type of uninstall to perform from the following choices: To remove the product and all of the components, enter. To select some, but not all, product components to removed, enter Partial.

3. The following message displays:

```
1. Uninstall Now
2. Start Over
3. Exit Uninstallation
What would you like to do?
```

   To begin uninstalling the agent, enter 1.

4. When the Installation program is finished, you must reboot the system.

   If you want to see more details of the uninstallation, a log file is written in the following location:

   ```
   %TEMP%\DSAME_Agent_uninstall.*
   ```

Using Secure Sockets Layer (SSL) with an Agent

During installation, if you specify the HTTPS protocol for the web server that runs DSAME services, the agent is automatically configured to communicate over SSL.

NOTE Before proceeding with the following steps, you should have a solid understanding of SSL concepts and the security certificates required to enable communication over the HTTPS protocol. See the documentation that comes with your web server. If you're using iPlanet Web Server, you can access the following documentation on the Internet:

`http://docs.sun.com/source/816-5691-10/esecurty.htm`

The Agent's Default Trust Behavior

By default, a policy agent is installed on a iPlanet Web Server 6.0 or Microsoft IIS 5.0 that will trust any server certificate presented over SSL by the web server that runs DSAME services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs DSAME services is SSL-enabled, and you want the policy agent to perform certificate-checking, you must do two things:

1. Disable the agent's default trust behavior.
2. Install CA certificate on the web server where the agent is installed. The CA certificate must the be same one that is installed on the web server that runs DSAME service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to true:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the web server must be the same one that is installed on the web server that runs DSAME services.

To Install the CA Certificate on Microsoft IIS Server

See the instructions for installing a CA Certificate in the documentation that comes with the web server. Generally, this is done through the web server's Administration console.

1. Go to the following directory:

   Agent_Install_Dir\Agents\iis50\utils

2. Add the same certificate that is installed on the web server that runs DSAME services into the existing certificate database. At the command line, enter the following command:

   `certutil -A -n` *cert-name* `-t "C,C,C" -d` *cert-dir* `-i` *cert-file*

   using the following variables:

   - *cert-name* can be any name for this certificate.
   - *cert-dir* is directory where the certificate-related files are located. On Windows the locations is:

     Agent_Install_Dir\Agents\iis50\cert

   - *cert-file* is the base-64 encoded certificate file.
   - For more information on `certutil`, type `certutil -H`.

3. Restart IIS.

Setting the REMOTE_USER Server Variable

The `REMOTE_USER` server environment variable can be set to a DSAME authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

For an iPlanet Web Server agent, the feature is enabled all the time. To enable the `REMOTE_USER` feature for an IIS 5.0 agent, perform the following steps:

1. In the Windows Start menu, choose Programs > Administrative Tools > Internet Services Manager.

   This will launch the Internet Information Services console.

2. On the web site that you want the DSAME agent to protect, select Properties.

3. Select the Directory Security tab.
4. In the Anonymous Access and Authentication Control section, click Edit.
5. In the dialog that displays, select Anonymous Access and Basic Authentication, then deselect Integrated Windows Authentication.

   Performing these steps will set `REMOTE_USER` for allowed URLs.

To enable the `REMOTE_USER` setting for globally not-enforced URLs as specified in the `AMAgent.properties` file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the `AMAgent.properties` file to `TRUE` (by default, this value is set to `FALSE`):

```
com.iplanet.am.policy.agents.anonRemoteUser.enable
```

When you set this property value to `TRUE`, the value of `REMOTE_USER` will be set to the value contained in the following property in the `AMAgent.properties` file (by default, this value is set to `anonymous`):

```
com.iplanet.am.policy.agents.unauthenticatedUser
```

Forwarding LDAP User Attributes via HTTP Headers

DSAME agents has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of DSAME. A DSAME agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in `AMAgent.properties` file. To turn this feature on and off, use the following `AMAgent.properties` file property:

```
com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable
```

By default, this property is set to `false`, and the feature off. To turn on attribute forwarding, set this property to `true`. To configure the attributes that are to be forwarded in the HTTP headers, use the `AMAgent.properties` file property `com.iplanet.am.policy.agents.ldapattr`

Below is an example section in the `AMAgent.properties` file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web
servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case
letters,
#       and any _ will become -
# NOTE: for IIS and Apache agents, "http_header_name" will be
prefixed
#       by HTTP_, and all lower case letters will become upper
case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organiza
tion-unit,o|organization,c|country,mail|email,employeenumber|emp
loyee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the DSAME server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either DSAME User attributes or DSAME Dynamic attributes (for explanation of these two types of user attributes, refer to the DSAME *Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

NOTE Each web server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each property in the AMAgents.properties file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or “hijacking” of SSO tokens.

The `AMAgent.properties` file contains a property titled `com.iplanet.am.policy.agents.client_ip_validation.enable`, which by default is set to `false`.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

This feature should not be used, however, if the client browser uses a web proxy or if there is a load-balancing application somewhere between the client browser and the agent-protected web server. In such cases, the IP address appearing in the request will not reflect the real IP address on which the client browser runs.

Troubleshooting the IIS Policy Agent

If you are experiencing problems with your installation try the following:

- Check the installation log file for errors:

  `%TEMP%\DSAME_install.`*nnnn*

- Re-install by uninstalling and then installing.
- Verify agent loading in IIS:

  a. Launch Internet Services Manager.

  b. Start > Programs > Administrative Tools > Internet Services Manager.

  c. Open the properties for the host computer in the Tree Pane of the Internet Services Manager window that is titled Internet Information Services.

  d. The host computer name should appear in the tree underneath the Internet Information Services root.

  e. Click Edit in the Master Properties section of the Internet Information Services tab.

  f. Select the ISAPI Filters tab in the WWW Service Master Properties dialog that appears.

g. Look for the filter name "DSAME agent."

If the Filter name "DSAME agent" does not appear at all, then check that the installer was run, and look for any errors during installation. The install log is located at:

`%TEMP%\DSAME_install.`*nnnn*

A green arrow pointing up in the Status column to the right of the "DSAME agent" indicates the agent loaded successfully into IIS. A red arrow pointing down indicates that the filter failed to load. The most likely cause of the filter not loading successfully (red arrow) is that it cannot locate the required dll files.

h. Check your system path to ensure that the following directory is present:

Agent_Install_Dir`\Agents\iis50\lib`

i. If the filter did not load successfully check the following:

- Check the path of the Agent DLL by clicking "DSAME agent" and then Edit. Ensure that the path in the text box labeled Executable is valid.
- The agent also needs several DLL files. Check that the following exist in the directory `Agents\iis50\lib`:

  `libamPolicy.dll`

  `libnspr4.dll`

  `libplc4.dll`

  `libplds4.dll`

  `nss3.dll`

  `ssl3.dll`

j. If the libraries are in your system path try rebooting the system.

- IIS logs filter loading errors in the System Event Log. To check the event log:

  a. Start > Programs > Administrative Tools > Event Viewer

  b. Select the System Log

  c. Check for Error messages with Source W3SVC.

- If the agent loads but returns HTTP 500 Internal Server Error for all URL requests to the IIS web server.

This indicates that the agent has loaded but did not properly initialize. Returning HTTP 500 Internal Server Error for all HTTP requests is a fail-safe to protect URL resources when the Agent cannot initialize. The most likely cause is a DSAME agent or server misconfiguration or unavailability.

- Check the agent debug log.

  The log is located by default at the *Agent_Install_Dir* directory. This is the best source of debug information for resolving initialization and agent operation issues. The log file directory is specified by the property: `com.iplanet.services.debug.directory` in the `AMAgent.properties` file located in the directory:

  Agent_Install_Dir`\Agents\iis50\config`

  The property `com.iplanet.services.debug.level` controls the verbosity of the log information. Setting this property to “`message`” yields the most debug information. The value "message" should not be used in production environments since it reduces performance and quickly generates large debug outputs to the file.

- Check that the agent can locate the `AMAgent.properties` configuration file.

  The agent uses the registry key `HKEY_LOCAL_MACHINE\Software\iPlanet\DSAME IIS Agent\5.0` to locate the `AMAgent.properties` file. The `AMAgent.properties` file is located at:

  Agent_Install_Dir`\Agents\iis50\config`

- The agent uses the Application Event Log to log errors that occur before the debug log file specified in `AMAgent.properties` is started.

  a. Start > Programs > Administrative Tools > Event Viewer.

  b. Select the Application Log.

  c. Check for Error messages with Source DSAME IIS Agent.

Chapter 4

Policy Agent Pack 1.1 on Windows NT

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server (also referred as DSAME) to grant or deny user access to web servers in an enterprise. The Policy Agent Pack 1.1 provides a set of policy agents for use with various web and proxy servers. This chapter explains how URL access agents can be configured for IIS 4.0 running on the Windows NT operating system, version 4.0, with Service Pack 6.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Installing Multiple Policy Agents on the Same Windows Computer System
- Using Secure Sockets Layer (SSL) With an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses
- Troubleshooting the IIS 4.0 Policy Agent
- Known Issues

Before You Begin

Be sure you're familiar with the concepts presented in Chapter 1, "Read This First." The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement
- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Installing Multiple Web Server Agents on the Same Computer System
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache
- Global Not-Enforced List
- The AMAgent.properties File

Supported Windows Web Server

The Agent Pack supports the following web server on the Windows NT Server 4.0 SP6 operating system:

- Microsoft IIS 4.0

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version of the Installation program to install one agent at a time.

Installing the Policy Agent for Microsoft IIS 4.0

The IIS agent enforces policy on URL access for Microsoft's Internet Information Services (IIS 4.0) web server. The agent is an IIS ISAPI filter installed at the IIS web service level that will enforce policy on all IIS web sites. Technical considerations prevent the agent from being installed at the web site level.

Prior to installation, be sure that the entry for the system where the agent will be installed has a domain name set. If the web server that runs DSAME services is running on a separate system, make sure the server is also in the DNS query list.

To Install the Policy Agent on Microsoft IIS 4.0

You must have administrator privileges to run the installation program.

1. Unzip the product binaries file.
2. Run the Installation program by double-clicking `setup.exe`.
3. In the Welcome window, click Next.
4. Read the License Agreement. Click Yes to accept the license agreement.
5. Select the directory where you would like to install the agent by clicking Browse, or click Next to accept the default.
6. Select the component "DSAME Agent for IIS 4.0" and click Next.
7. Enter the information about the web server where this agent will be installed:

   Host Name: Enter the fully qualified domain name of the system where the Agent web server is installed. For example, `mycomputer.siroe.com`.

   Web Server Document Root: Enter the document root directory. This directory needs to be accessible by the web server root `w3svc`.

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

   Web Server Protocol: If your web server has been configured for SSL, then select HTTPS; otherwise select HTTP.

   Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`.

   The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

   When all the information is entered correctly, click Next.

8. Provide the following information about web server that runs DSAME services:

   DSAME Services Host: Enter the fully qualified domain name of the system where the primary web server that runs DSAME services is installed. For example, `myserver.siroe.com`.

   DSAME Services Port: Enter the port number for the primary web server that runs DSAME services.

   DSAME Services Protocol: If the web server that runs DSAME services has been configured for SSL, then select HTTPS; otherwise select HTTP.

   DSAME Services Deployment URI: Enter the location that was specified when DSAME was installed. The default Universal Resource Identifier (URI) for DSAME is `/amserver`.

   Failover Server Host: Enter the fully qualified domain name for the secondary web server that will run DSAME services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that will run DSAME services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

9. If all the information entered is correct, click Next.

10. Review your selections in the Summary panel and click Install Now.

11. When the installation is complete you may review the details, and then click Exit.

12. The installation modifies the system path by appending to it the location of the Agent libraries. In order for the change to take effect and for the Agent to work properly, you must reboot your computer. If you would like to reboot your computer immediately click Reboot Now in the popup window.

NOTE If the IIS 4.0 agent was previously installed and uninstalled on your machine, you do not need to reboot if you are installing the same IIS 4.0 agent in the same directory.

Uninstalling and Disabling Policy Agents

When you no longer require the policy agent, you can uninstall it or disable it.

Uninstalling a Policy Agent

1. In the Start Menu, open Settings > Control Panel.
2. In the Control Panel, open Add / Remove Programs.
3. In the Add / Remove Programs window, choose iPlanet Directory Services Access Management Edition Agent 1.1.
4. Click Change / Remove.
5. Click Next on the Welcome panel.
6. On the Type of Install panel, select Full.
7. Click Uninstall Now.
8. Click Exit after uninstallation is complete.

Disabling a Policy Agent Installed on Microsoft IIS 4.0

1. Launch Internet Services Manager.
   - In the Start Menu, click Programs > Windows NT 4.0 Options Pack > Microsoft Internet Information Server: Internet Services Manager.
2. Check the status of the filter.
   a. In the left side of the window, right click on the hostname of the computer and select Properties.
   b. In the Master Properties section, select WWW Service, and click Edit.
   c. Select the ISAPI Filters tab in the WWW Service Master Properties dialog that appears.
   d. Highlight the filter named “DSAME Agent.”

      You can click Edit to view the filter name and executable path. You will need this information when you want to re-enable the agent. Click Cancel to return to the program.
   e. Click Remove
   f. Click Apply and exit from the WWW Service Master Properties dialog.
3. Restart Microsoft IIS 4.0 by stopping `iisadmin`, and then staring `iisadmin` and `w3csvc`.

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

To Install an Agent Using the Command Line

1. In the directory where you unzipped the binaries file, at the command line, enter the following command:

   ```
   setup.bat -nodisplay
   ```

2. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement?

   Install DSAME Agent in this directory: Specify the directory where you want the agent o be installed. To accept the default directory that is displayed in brackets, press Enter. Otherwise, enter a full path.

3. The following text displays:

   ```
   DSAME Agent components showing a checked box will be installed.
   Only one agent may be installed at a time.
   [ ]  1  DSAME Agent for IIS 4.0
   ```

   First, do one of the following:

   - To install the agent for Microsoft IIS 4.0, enter 1.

   Then, when a check mark appears beside your choice, enter 0 to continue.

4. When prompted, provide the following information about the web server instance this Agent will protect:

   - `Host Name`
   - `Web Server Port`

- Web Server Protocol
- Web Server Doocument Root
- Agent Deployment URI

For information about these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 66.

5. When prompted, provide the following information about the web server that runs DSAME Services:

   - Host Name
   - Port Number
   - Protocol
   - Deployment URI
   - Failover Host
   - Failover Port

   For information about these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 66.

6. When displayed, review the summary of installation information you’ve specified. Press Enter to continue, or enter and exclamation point (!) to exit the program.

7. The following message displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation

What would you like to do
```

   To continue with installation, enter 1.

8. When installation is complete, you must restart IIS 4.0.

To Uninstall an Agent Using the Command Line

1. In the *Agent_Install_Dir* directory, at the command line, enter the following command:

   ```
   java uninstall_DSAME_Agent -nodisplay
   ```

2. When prompted, provide the following information:

   Please select the type of uninstall to perform from the following choices: To remove the product and all of the components, enter. To select some, but not all, product components to removed, enter Partial.

3. The following message displays:

```
1. Uninstall Now
2. Start Over
3. Exit Uninstallation
What would you like to do?
```

   To begin uninstalling the agent, enter 1.

4. When the Installation program is finished, you must reboot the system.

If you want to see more details of the uninstallation, a log file is written in the following location:

```
%TEMP%\DSAME_Agent_uninstall.*
```

Installing Multiple Policy Agents on the Same Windows Computer System

You can install only one instance of IIS per computer system and you can install only one global agent per IIS. The global agent protects all websites on the server.

Using Secure Sockets Layer (SSL) With an Agent

During Installation, if you specify the HTTPS protocol for the web server that runs DSAME services, the agent is automatically configured to communicate over SSL with DSAME services.

The Agent's Default Trust Behavior

By default, a policy agent installed on a Microsoft IIS 4.0 that will trust any server certificate presented over SSL by the web server that runs DSAME services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs DSAME services is SSL-enabled, and you want the policy agent to perform certificate-checking, you must do two things:

1. Disable the agent's default trust behavior.
2. Install CA certificate on the web server where the agent is installed. The CA certificate must the be same one that is installed on the web server that runs DSAME service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to true:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the web server must be the same one that is installed on the web server that runs DSAME services.

To Install the CA certificate on Microsoft IIS

1. Navigate to the following directory:

   Agent_Install_Dir\Agents\iis40\utils

2. Add the same root certificate, which is installed on the web server that runs DSAME services, into the existing certificate database. At the command line, enter the following command:

   `certutil -A -n` *cert-name* `-t "C,C,C" -d` *cert-dir* `-i` *cert-file*

   use the following variables:

   - *cert-name* can be any name for this root certificate.
   - *cert-dir* is directory where the certificate-related files are located. On Windows the locations is:

     Agent_Install_Dir\Agents\iis40\cert

   - *cert-file* is the base-64 encoded root certificate file.
   - For more information on `certutil`, type `certutil -H`

3. Restart IIS.

Setting the REMOTE_USER Server Variable

The `REMOTE_USER` server environment variable can be set to a DSAME authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

To enable the `REMOTE_USER` feature, perform the following steps:

1. In the Windows Start menu, select Programs > Windows NT Option Pack > Microsoft Internet Information Server > Internet Services Manager.

   This will launch the Microsoft Management Console.

2. On the web site that you want the DSAME agent to protect, select Properties.
3. Select the Directory Security tab.

4. In the Anonymous Access and Authentication Control section, click Edit, and select Allow Anonymous Access (selected by default), Basic Authentication (not selected by default), and deselect Challenge / Response (selected by default).

REMOTE_USER will be set while accessing allowed URLs.

To enable the REMOTE_USER setting for a globally not-enforced list by unauthenticated users, the com.iplanet.am.policy.agents.anonRemoteUser.enable property must be set to true (by default, it is set to false). This property can be found in the AMAgent.properties file located in *Agent_Install_Dir*\Agents\iis40\config.

The com.iplanet.am.policy.agents.unauthenticatedUser property will be used for the value of the REMOTE_USER setting. By default, it is set to anonymous.

Forwarding LDAP User Attributes via HTTP Headers

DSAME agents has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of DSAME. A DSAME agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in AMAgent.properties file. To turn this feature on and off, use the following AMAgent.properties file property:

com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable

By default, this property is set to false, and the feature off. To turn on attribute forwarding, set this property to true. To configure the attributes that are to be forwarded in the HTTP headers, use the AMAgent.properties file property com.iplanet.am.policy.agents.ldapattr.

Below is an example section in the AMAgent.properties file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web
servers
```

```
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case
letters,
#       and any _ will become -
# NOTE: for IIS and Apache agents, "http_header_name" will be
prefixed
#       by HTTP_, and all lower case letters will become upper
case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organiza
tion-unit,o|organization,c|country,mail|email,employeenumber|emp
loyee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the DSAME server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either DSAME User attributes or DSAME Dynamic attributes (for explanation of these two types of user attributes, refer to the DSAME *Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

NOTE Each web server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each property in the AMAgents.properties file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or “hijacking” of SSO tokens.

The `AMAgent.properties` file contains a property titled `com.iplanet.am.policy.agents.client_ip_validation.enable`, which by default is set to `false`.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

This feature should not be used, however, if the client browser uses a web proxy or if there is a load-balancing application somewhere between the client browser and the agent-protected web server. In such cases, the IP address appearing in the request will not reflect the real IP address on which the client browser runs.

Troubleshooting the IIS 4.0 Policy Agent

If you are experiencing problems with your installation try the following:

- Check the installation log file for errors:

  `%TEMP%\DSAME_install.`*nnnn*

- Re-install by uninstalling and then installing.
- Verify agent loading in IIS:

  a. Launch Internet Services Manager.

  b. Start > Programs > Windows NT Option Pack > Microsoft Internet Information Server > Internet Services Manager.

  This will launch the Microsoft Management Console.

  c. In the left window, right click on the hostname of the computer and select Properties.

  d. In the Master Properties section, select WWW Service and click Edit.

  e. Select the ISAPI Filters tab in the WWW Service Master Properties dialog that appears.

f. Look for the filter name "DSAME agent."

If the Filter name "DSAME agent" does not appear at all, then check that the installer was run, and look for any errors during installation. The install log is located at:

`%TEMP%\DSAME_install.`*nnnn*

A green arrow pointing up in the Status column to the right of the "DSAME agent" indicates the agent loaded successfully into IIS. A red arrow pointing down indicates that the filter failed to load. The most likely cause of the filter not loading successfully (red arrow) is that it cannot locate the required dll files.

g. Check your system path to ensure that the following directory is present:

Agent_Install_Dir`\Agents\iis40\lib`

h. If the filter did not load successfully check the following:

- Check the path of the Agent DLL by clicking "DSAME agent" and then Edit. Ensure that the path in the text box labeled Executable is valid.
- The agent also needs several DLL files. Check that the following files exist in the `Agents\iis40\lib` directory:

  `libamUrlAccessAgentIis40.dll`

  `libamPolicy.dll`

  `libnspr4.dll`

  `libplc4.dll`

  `libplds4.dll`

  `nss3.dll`

  `ssl3.dll`

  `smime3.dll`

i. If the libraries are in your system path, try rebooting the system.

- IIS logs filter loading errors in the System Event Log. To check the event log:

  a. Start > Programs > Administrative Tools > Event Viewer.

  b. Select the System Log.

  c. Check for Error messages with Source W3SVC.

- If the agent loads, but returns HTTP 500 Internal Server Error for all URL requests to the IIS web server, it indicates that the agent has loaded, but did not properly initialize. Returning HTTP 500 Internal Server Error for all HTTP requests is a fail-safe to protect URL resources when the Agent cannot initialize. The most likely cause is a DSAME agent or server misconfiguration or unavailability.
- Check the agent debug log.

  The log is located by default at the *Agent_Install_Dir* directory. This is the best source of debug information for resolving initialization and agent operation issues. The log file directory is specified by the property: `com.iplanet.services.debug.directory` in the `AMAgent.properties` file located in the directory:

  Agent_Install_Dir`\Agents\iis40\config`

  The property `com.iplanet.services.debug.level` controls the verbosity of the log information. Setting this property to “`message`” yields the most debug information. The value "message" should not be used in production environments since it reduces performance and quickly generates large debug outputs to the file.
- Check that the agent can locate the `AMAgent.properties` configuration file.

  The agent uses the registry key `HKEY_LOCAL_MACHINE\Software\iPlanet\DSAME IIS Agent\4.0` to locate the `AMAgent.properties` file. The `AMAgent.properties` file is located at:

  Agent_Install_Dir`\Agents\iis40\config`
- The agent uses the Application Event Log to log errors that occur before the debug log file specified in `AMAgent.properties` is started.

  a. Choose Start > Programs > Administrative Tools > Event Viewer.

  b. Select the Application Log.

  c. Check Error messages with Source DSAME IIS Agent.

Known Issues

Issue

Internet services hang when you attempt to shutdown individual websites.

Workaround

It is highly recommended that you do not shut down your websites individually. Instead, you should shut them down collectively by stopping the IIS Admin Service, restarting the IIS Admin Service, and then restarting the individually managed services.

1. To stop the IIS Admin Service, issue the following command from the command line:

   ```
   c:\>net stop iisadmin /y
   ```

   Alternatively, you can shutdown the IIS Admin Service from the Services menu:

   a. Under the Start menu, select Control Panel.

   b. Click on Services.

   c. Select IIS Admin Service.

   d. Click Stop.

   This will shutdown all internet services managed by the `iisadmin` process, including FTP services, WWW services and SMTP services.

2. To restart the ISS Admin Service, issue the following command from the command line:

   ```
   c:\>net start iisadmin
   ```

   Alternatively, you can restart the services from the Services menu:

   a. Under the Start menu, select Control Panel.

   b. Click on Services.

   c. Select IIS Admin Service.

   d. Click Start.

3. To restart the individual services, issue the following command from the command line:

   ```
   c:\>net start w3svc
   ```

   Alternatively, you can restart the individual services from the Services menu:

   a. Under the Start menu, select Control Panel.

   b. Click on Services.

   c. Select World Wide Web Publishing.

d. Click Start.

Chapter 5

Policy Agent for Apache 1.3.22 From Red Hat

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server to grant or deny user access to web servers in an enterprise. This chapter explains how to install the Sun ONE Identity Server Policy Agent for Apache 1.3.22 server running on the Red Hat Linux 7.2 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses
- Troubleshooting Information

Before You Begin

Be sure you're familiar with the concepts presented in Chapter 1, "Read This First." The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement

- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Providing Failover Protection for Identity Server Agents
- Global Not-Enforced List
- The AMAgent.properties File

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version of the Installation program to install agent.

Installing the Policy Agent

You must have root permissions when you run the agent installation program.

4. Unpack the product binaries using the following command:

   ```
   # gunzip -dc agents-1.1-domestic-us.i686-intel-linux.tar.gz | tar
   -xvof -
   ```

5. Run the `setup` program. You'll find the program in the directory where you untarred the binaries. At the command line, enter the following:

   ```
   # ./setup_linux
   ```

6. In the Welcome page, click Next.
7. Read the License Agreement. Click Yes to agree to the license terms.
8. In the Select Installation Directory window, provide the following information:

   Install Sun ONE Identity Server Policy Agent in this directory: Enter the full path to the directory where you want this agent to be installed, and then click Next.

9. By default, Sun ONE Identity Server Policy Agent for Apache 1.3.22 is selected, click Next.
10. In the Agent Web Server Information window, provide the following information about the Apache web server this agent will protect:

    Host Name: Enter the fully qualified domain name of the machine where the Apache 1.3.22 server is installed. For example, `mycomputer.siroe.com`.

Apache config File Location: Enter the full path to the directory where the `httpd.conf` file is located.

Web Server Port: Enter the port number for the web server that will be protected by the agent.

Web Server Protocol: If the web server has been configured for SSL, choose HTTPS; otherwise choose HTTP.

Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`

The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

When all the information is entered correctly, click Next.

11. In the Identity Server Information window, provide information about the web server that runs Identity Server policy and management services.

    Identity Server Host: Enter the fully qualified domain name of the system where the primary web server that runs Identity Server Services is installed. For example, `myserver.siroe.com`.

    Identity Server Port: Enter the port number for the web server that runs Identity Server services.

    Identity Server Protocol: If the web server that runs Identity Server is SSL-enabled, select HTTPS; otherwise select HTTP.

    Identity Server Deployment URI: Enter the location that was specified when Identity Server was installed. The default Universal Resource Identifier (URI) for Identity Server is `/amserver`.

    Failover Server Host: If you have configured a failover web server to run Identity Server services, enter the host name of the failover system. Examples: `backup.siroe.com`. If there is no failover server, then leave this field blank.

    Failover Server Port: If you have configured a failover web server to run Identity Server services, enter the web server port number. If there is no failover host server, then leave this field blank.

12. Review the Installation Summary to be sure that the information you've entered is correct. If you want to make changes, click Back. If all the information is correct, click Next.

13. In the Ready to Install page, click Install Now.
14. When the installation is complete, you can click Details to view details about the installation, or click Exit to end the Installation program.
15. You must restart your Apache web server for the installation to be complete. At the command line enter the following:

    ```
    /etc/init.d/httpd restart
    ```

Uninstalling and Disabling Policy Agent

When you no longer require the policy agent, you can uninstall it or disable it.

Uninstalling the Policy Agent

Follow the steps below:

1. In the directory where the agent is installed, at the command line, enter the following command:

    ```
    # java uninstall_Identity_Server_Policy_Agent
    ```

2. Click Next on Welcome panel.
3. On Type of Install panel, select Full.

NOTE Since there is only one component, it is recommended that you select Full uninstallation.The Partial uninstallation is not supported.

4. Click Uninstall Now.
5. Click Exit after uninstallation is complete.

Disabling a Policy Agent

Follow the steps below:

1. In the file `httpd.conf` remove or comment out the following line:

    ```
    # include /Agent_Install_Dir/apagent/conf/dsame.conf
    ```

2. Restart the server.

    ```
    /etc/init.d/httpd restart
    ```

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

Installing the Policy Agent

You must have root permissions when you run the agent installation program.

1. Unzip the Solaris tar file using the following command:

   ```
   # gunzip -dc agents-1.1-domestic-us.i686-intel-linux.tar.gz | tar
   -xvof -
   ```

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

   ```
   # ./setup_linux -nodisplay
   ```

3. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement? Enter yes.

   License Agreement? Enter yes.

   Install Sun ONE Identity Server Policy Agent in this directory: Enter the full path to the directory in which you want to install the policy agent.

   The following text displays:

```
Sun ONE Identity Server Policy Agent components showing a checked
box will be installed. Only one agent may be installed at a time.
[ ]  1 Sun[tm] ONE Identity Server Policy Agent for Apache 1.3.22
```

To check a particular component, enter its number, or 0 when you are finished: Enter the number that corresponds to the policy agent you want to install. The following message displays, with a cross mark beside the server you specified.

```
[X]  1 Sun[tm] ONE Identity Server Policy Agent for Apache 1.3.22
```

To check a particular component, enter its number, or 0 when you are finished: Enter `0` to continue.

4. Provide the following information about the Apache web server this agent will protect.
   - `Host Name`
   - `Apache config File Location`
   - `Web Server Port`
   - `Web Server Protocol`
   - `Agent Deployment URI`

   For details on these items, refer to "Using the Graphical User Interface (GUI) Version of the Installation Program" on page 84.

5. Provide the following information about the web server that runs Identity Server services. The following fields refer to the system where Identity Server is installed.
   - `Identity Server Host Name`
   - `Identity Server Port Number`
   - `Identity Server Protocol`
   - `Identity Server Deployment URI`
   - `Failover Server Host`
   - `Failover Server Port`

   For details on these items, refer to "Using the Graphical User Interface (GUI) Version of the Installation Program" on page 84.

6. The following text displays:

```
Ready to Install
1. Install Now
2. Start Over
3. Exit Installation
```

When prompted, **What would you like to do?**, enter `1` to start the installation.

7. The following text displays:

```
Product                                  Result    More Info
1.Sun ONE Identity Server Policy Agent Installed Available
2.Done
```

To see log information, enter `1`. To exit the Installation program, enter `2`.

Uninstalling the Policy Agent

1. In the directory where you unpacked the binaries file, at the command line, enter the following command at the command line:

```
# java uninstall_Identity_Server_Policy_Agent -nodisplay
```

2. The following text displays:

```
Please select the type of uninstall to perform from the following
choices:
1. Full
2. Partial
```

To remove the product and all of the components from your system, enter `1` for Full. To remove some, but not all, product components, enter `2` for Partial.

NOTE Since there is only one component, it is recommended that you enter `1` for Full uninstallation.The Partial uninstallation is not supported.

3. The following text displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
```

When prompted, **What would you like to do**? enter `1` to begin uninstallation.

4. The following text displays:

```
Product                                  Result More Info
1. Sun ONE Identity Server Policy Agent Full   Available
2. Done
```

To see log information on the agent, enter `1`. To exit the Installation program, enter `2`.

Using Secure Sockets Layer (SSL) with an Agent

During Installation, if you specify the HTTPS protocol for the web server that runs Sun ONE Identity Server services, the agent is automatically configured to communicate over SSL with Sun ONE Identity Server services.

The Agent's Default Trust Behavior

By default, a policy agent is installed on a web server that will trust any server certificate presented over SSL by the web server that runs Identity Server services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs Identity Server services is SSL-enabled, and you want the policy agent to perform certificate-checking, you must do the following:

1. Disable the agent's default trust behavior.
2. Install a CA certificate on the Apache web server (where the agent is installed). The CA certificate must be the same one that is installed on the web server that runs Sun ONE Identity Server service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to `true`:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the Apache web server must be the same one that is installed on the web server that runs Identity Server services.

To Install the CA Certificate on Apache Web Server

You can use the `certutil` program to install the CA Certificate on Apache web server.

1. In C shell, at the command line, enter the following commands:

   ```
   # cd /Agent_Install_Dir/SUNWam/apagent/cert
   # setenv LD_LIBRARY_PATH /Agent_Install_Dir/SUNWam/apagent/lib
   # export LD_LIBRARY_PATH
   # ./certutil -A -n cert-name -t "C,C,C" -d . -i cert-file
   ```

   In the commands above, the variables represent the following:

   - *cert-name* can be any name for this certificate.
   - *cert-dir* is directory where the certificate-related files are located.
   - *cert-file* is the base-64 encoded certificate file.

   For more information on the `certutil` utility, enter `certutil -H` for on-line Help.

2. To verify that the certificate is properly installed, at the command line, enter the following:

   ```
   # ./certutil -L -d .
   ```

   Trust database information will display including the name of the CA certificate you installed. Example:

```
Certificate Name Trust Attrubutes

rootCAcert

p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

Setting the REMOTE_USER Server Variable

The REMOTE_USER server environment variable can be set to Identity Server authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

REMOTE_USER will be set while accessing allowed URLs.

To enable the REMOTE_USER setting for globally not-enforced URLs as specified in the AMAgent.properties file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the AMAgent.properties file to TRUE (by default, this value is set to FALSE):

com.iplanet.am.policy.agents.anonRemoteUser.enable

When you set this property value to TRUE, the value of REMOTE_USER will be set to the value contained in the following property in the AMAgent.properties file (by default, this value is set to anonymous):

com.iplanet.am.policy.agents.unauthenticatedUser

Forwarding LDAP User Attributes via HTTP Headers

Identity Server agent has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of Identity Server. An Identity Server agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in AMAgent.properties file. To turn this feature on and off, use the following AMAgent.properties file property:

com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable

By default, this property is set to false, and the feature off. To turn on attribute forwarding, set this property to true. To configure the attributes that are to be forwarded in the HTTP headers, use the AMAgent.properties file property com.iplanet.am.policy.agents.ldapattr.

Below is an example section in the AMAgent.properties file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case letters,
#       and any _ will become _
# NOTE: for IIS and Apache agents, "http_header_name" will be prefixed
#       by HTTP_, and all lower case letters will become upper case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organization-unit
,o|organization,c|country,mail|email,employeenumber|employee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the Identity Server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either Identity Server User attributes or Identity Server Dynamic attributes (for explanation of these two types of user attributes, refer to the *Sun ONE Identity Server Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the Apache web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

NOTE Each Apache web server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each property in the AMAgents.properties file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or *hijacking* of SSO tokens.

The `AMAgent.properties` file contains a property titled `com.iplanet.am.policy.agents.client_ip_validation.enable`, which by default is set to `false`.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

Troubleshooting Information

If you are experiencing problems with your installation try the following:

- Check the `httpd.conf` file in the `config` directory in the Apache Server has a fully qualified domain name for the `ServerName` variable.
- Ensure that you have set your machine with a fully qualified domain name.
- Check the `debug.directory` in the `AMAgent.properties` file. The log file directory is specified by the property: `com.iplanet.services.debug.directory` in the `AMAgent.properties` file located in the directory */Agent_Install_Dir/*`apagent/conf`. Verify whether this directory is created with proper permissions.
- Verify the following in */Agent_Install_Dir/*`apagent/conf/dsame.conf`:
  - The first line should be:

    `LoadModule dsame_module` */Agent_Install_Dir/*`apagent/lib/mod_dsame.so`
  - `Agent_Config_file` should point to the location of `AMAgent.properties`
  - `Shared_Lib_Dir` should be *Agent_Install_Dir/*`apagent/lib`
- Check the following Identity Server variables are set properly in the `AMAgent.properties` file.

  `com.iplanet.am.server.protocol`

  `com.iplanet.am.server.port`

`com.iplanet.am.server.host`

`com.iplanet.am.naming.url`

`com.iplanet.am.policy.agents.url.authLoginUrl`

- Check the following properties are set with correct values when failover server is enabled.

  `com.iplanet.am.policy.agents.url.failover.server.host`

  `com.iplanet.am.policy.agents.url.failover.server.port`

  `com.iplanet.am.policy.agents.url.failoverAuthLoginUrl`

Policy Agent for Apache 1.3.26

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server to grant or deny user access to web servers in an enterprise. This chapter explains how to install the Sun ONE Identity Server Policy Agent for Apache 1.3.26 server running on Solaris 8 or 9 operating systems.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses

Before You Begin

Be sure you're familiar with the concepts presented in Chapter 1, "Read This First." The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement
- Providing Failover Protection for Identity Server Agents
- Global Not-Enforced List
- The AMAgent.properties File

Patch Clusters for Solaris

When running Apache 1.3.26 Web Server on platforms Solaris 8 and 9, you must ensure that the recommended patches 109234-09 and 113146-01are installed. You can download this patch from `http://sunsolve.siroe.com`

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version of the Installation program to install agent.

Installing the Policy Agent Using GUI

You must have root permissions when you run the agent installation program.

1. Unpack the product binaries file using the following command:

   ```
   # gunzip -dc Apache_1.3.26_agent_1.2_sparc-sun-solaris2.8.tar.gz
   | tar -xvof -
   ```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

   ```
   # ./setup
   ```

3. Set your `JAVA_HOME` environment variable to JDK version 1.3.1_04 or higher. The installation requires that you setup your `JAVA_HOME` variable correctly. However, in case you have incorrectly set the `JAVA_HOME` variable, the `setup` script will prompt you for supplying the correct `JAVA_HOME` value:

   ```
   Please enter path to pick up java:
   ```

   Enter the full path where JDK is located to launch the installer.

4. In the Welcome page, click Next.

5. Read the License Agreement. Click Yes to agree to the license terms.

6. In the Select Installation Directory window, provide the following information:

   Install Sun ONE Identity Server Policy Agent for Apache 1.3.26 in this directory: Enter the full path to the directory where you want this agent to be installed, and then click Next.

7. By default, Sun ONE Identity Server Policy Agent for Apache 1.3.26 is selected, click Next.

8. In the Agent Web Server Information window, provide the following information about the Apache web server this agent will protect:

   Host Name: Enter the fully qualified domain name of the machine where the Apache 1.3.26 server is installed. For example, `mycomputer.siroe.com`.

   Apache config File Location: Enter the full path to the directory where the `httpd.conf` file is located.

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

   Web Server Protocol: If the web server has been configured for SSL, choose HTTPS; otherwise choose HTTP.

   Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`

   The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an “Access denied” message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

   When all the information is entered correctly, click Next.

9. In the Identity Server Information window, provide information about the web server that runs Identity Server policy and management services.

   Identity Server Host: Enter the fully qualified domain name of the system where the primary web server that runs Identity Server services is installed. For example, `myserver.siroe.com`.

   Identity Server Port: Enter the port number for the web server that runs Identity Server services.

   Identity Server Protocol: If the web server that runs Identity Server is SSL-enabled, select HTTPS; otherwise select HTTP.

   Identity Server Deployment URI: Enter the location that was specified when Identity Server was installed. The default Universal Resource Identifier (URI) for Identity Server is `/amserver`.

   Failover Server Host: If you have configured a failover web server to run Identity Services, enter the host name of the failover system. Examples: `blue.madisonparc.com`. If there is no failover server, then leave this field blank.

   Failover Server Port: If you have configured a failover web server to run Identity Services, enter the web server port number. If there is no failover host server, then leave this field blank.

10. Review the Installation Summary to be sure that the information you've entered is correct. If you want to make changes, click Back. If all the information is correct, click Next.

11. In the Ready to Install page, click Install Now.

12. When the installation is complete, you can click Details to view details about the installation, or click Exit to end the Installation program.

13. You must restart your Apache server for the installation to be complete. At the command line enter the following:

    ```
    /etc/init.d/httpd restart
    ```

Uninstalling and Disabling the Policy Agent

When you no longer require the policy agent, you can uninstall it or disable it.

Uninstalling a Policy Agent

Use the following steps to uninstall the Policy Agent.

1. In the directory where the agent is installed, at the command line, enter the following command:

   ```
   # ./uninstall_Apache1326_agent
   ```

2. Click Next on Welcome panel.
3. On Select Type of Uninstall panel, select Full and click Next.

NOTE Since there is only one component, it is recommended that you select Full uninstallation.The Partial uninstallation is not supported.

4. Click Uninstall Now.
5. Click Exit after uninstallation is complete.

Disabling a Policy Agent

Use the following steps to disable a Policy Agent.

1. In the file `httpd.conf` remove or comment out the following line:

   ```
   # include
   /etc/opt/SUNWam/conf/APACHE/_usr_local_apache_conf/dsame.conf
   ```

2. Restart the server.

   ```
   /etc/init.d/httpd restart
   ```

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

Installing an Agent Using the Command Line

You must have root permissions when you run the agent installation program.

1. Unpack the product binaries file using the following command:

```
# gunzip -dc
agent-Apache1326-1.1-domestic-us.sparc-sun-solaris2.8.tar.gz |
tar -xvof -
```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

```
# ./setup -nodisplay
```

3. Set your `JAVA_HOME` environment variable to JDK version 1.3.1_04 or higher. The installation requires that you setup your `JAVA_HOME` variable correctly. However, in case you have incorrectly set the `JAVA_HOME` variable, the setup script will prompt you for supplying the correct `JAVA_HOME` value:

```
Please enter path to pick up java:
```

Enter the full path where JDK is located to launch the installer.

4. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement? Enter yes.

   Install Sun ONE Identity Server Policy Agent for Apache1326 in this directory: Enter the full path to the directory in which you want to install the policy agent.

   The following text displays:

```
Sun ONE Identity Server Policy Agent for Apache1326 components
showing a checked box will be installed. Only one agent may be
installed at a time.
[ ]  1 Sun[tm] ONE Identity Server Policy Agent for Apache 1.3.26
```

   To check a particular component, enter its number, or 0 when you are finished: Enter the number that corresponds to the policy agent you want to install. The following message displays, with a cross mark beside the server you specified.

```
[X]  1 Sun[tm] ONE Identity Server Policy Agent for Apache 1.3.26
```

   To check a particular component, enter its number, or 0 when you are finished: Enter `0` to continue.

5. Provide the following information about the Apache web server this agent will protect.

   - `Host Name`
   - `Apache config File Location`
   - `Web Server Port`
   - `Web Server Protocol`
   - `Agent Deployment URI`

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 98.

6. Provide the following information about the web server that runs Identity Server services. The following fields refer to the system where Identity Server is installed.

   - Identity Server Host
   - Identity Server Port
   - Identity Server Protocol
   - Identity Server Deployment URI
   - Failover Server Host
   - Failover Server Port

   For details on these, refer to "Using the Graphical User Interface (GUI) Version of the Installation Program" on page 98.

7. The following text displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation
```

   When prompted, **What would you like to do?**, enter `1` to start the installation.

8. The following text displays:

```
Product                                          Result    More Info
1. SunONE Identity Server Policy Agent for Apache1326  Installed  Available
2. Done
```

   To see log information, enter `1`. To exit the Installation program, enter `2`.

Uninstalling an Agent Using the Command Line

1. In the directory where you unpacked the binaries file, at the command line, enter the following command at the command line:

```
# java
uninstall_SunONE_Identity_Server_Policy_Agent_for_Apache1326
-nodisplay
```

2. The following text displays:

```
Please select the type of uninstall to perform from the following
choices:
1. Full
2. Partial
```

To remove the product and all of the components from your system, enter `1` for Full. To remove some, but not all, product components, enter `2` for Partial.

NOTE Since there is only one component, it is recommended that you enter `1` for Full uninstallation. The Partial uninstallation is not supported.

3. The following text displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
```

When prompted, **What would you like to do**? enter `1` to begin uninstallation.

4. The following text displays:

```
Product                                                Result More Info
1.SunONE Identity Server Policy Agent for Apache1326 Full   Available
2.Done
```

To see log information on the agent, enter `1`. To exit the Installation program, enter `2`.

Using Secure Sockets Layer (SSL) with an Agent

During Installation, if you specify the HTTPS protocol for the web server that runs Identity Server services, the agent is automatically configured to communicate over SSL with Identity Server services.

The Agent's Default Trust Behavior

By default, a policy agent is installed on a Apache web server that will trust any server certificate presented over SSL by the web server that runs Identity Server services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs Identity Server services is SSL-enabled, and you want the policy agent to perform certificate-checking, you must do the following:

1. Disable the agent's default trust behavior.
2. Install a CA certificate on the Apache web server (where the agent is installed). The root certificate must the be same one that is installed on the web server that runs Identity Server service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to `true`:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the Apache web server must be the same one that is installed on the web server that runs Identity Server services.

To Install the CA Certificate on Apache Web Server

You can use the `certutil` program to install the CA Certificate on Apache web server.

1. In C shell, at the command line, enter the following commands:

   `# cd /`*`Agent_Install_Dir`*`/SUNWam/apache/cert`

   `# setenv LD_LIBRARY_PATH /`*`Agent_Install_Dir`*`/SUNWam/apache/lib`

   `# export LD_LIBRARY_PATH`

   `# ./certutil -A -n` *cert-name* `-t "C,C,C" -d . -i` *cert-file*

   In the commands above, the variables represent the following:

   - *cert-name* can be any name for this certificate.
   - *cert-dir* is directory where the certificate-related files are located.
   - *cert-file* is the base-64 encoded certificate file.

   For more information on the `certutil` utility, enter `certutil -H` for on-line Help.

2. To verify that the certificate is properly installed, at the command line, enter the following:

   `# ./certutil -L -d .`

   Trust database information will display including the name of the CA certificate you installed. Example:

```
Certificate Name Trust Attrubutes

rootCAcert

p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

Setting the REMOTE_USER Server Variable

The REMOTE_USER server environment variable can be set to Identity Server authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

REMOTE_USER will be set while accessing allowed URLs.

To enable the REMOTE_USER setting for globally not-enforced URLs as specified in the AMAgent.properties file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the AMAgent.properties file to TRUE (by default, this value is set to FALSE):

```
com.iplanet.am.policy.agents.anonRemoteUser.enable=TRUE
```

When you set this property value to TRUE, the value of REMOTE_USER will be set to the value contained in the following property in the AMAgent.properties file (by default, this value is set to anonymous):

```
com.iplanet.am.policy.agents.unauthenticatedUser=anonymous
```

Forwarding LDAP User Attributes via HTTP Headers

Identity Server agent has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of Identity Server. An Identity Server agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in AMAgent.properties file. To turn this feature on and off, use the following AMAgent.properties file property:

```
com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable
```

By default, this property is set to false, and the feature off. To turn on attribute forwarding, set this property to true. To configure the attributes that are to be forwarded in the HTTP headers, use the AMAgent.properties file property com.iplanet.am.policy.agents.ldapattr.

Below is an example section in the AMAgent.properties file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case letters,
#       and any _ will become _
# NOTE: for IIS and Apache agents, "http_header_name" will be prefixed
#       by HTTP_, and all lower case letters will become upper case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organization-unit
,o|organization,c|country,mail|email,employeenumber|employee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the Identity Server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either Identity Server User attributes or Identity Server Dynamic attributes (for explanation of these two types of user attributes, refer to the *Sun ONE Identity Server Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the Apache web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

NOTE Each Apache web server has its own peculiarities about HTTP header name conventions. For more information on this feature, see the comments listed before each property in the AMAgents.properties file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or *hijacking* of SSO tokens.

The `AMAgent.properties` file contains a property titled `com.iplanet.am.policy.agents.client_ip_validation.enable`, which by default is set to `false`.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

```
com.iplanet.am.policy.agents.client_ip_validation.enable=true
```

Policy Agent for Lotus Domino 5.0.10

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server to grant or deny user access to web servers in an enterprise. The Sun ONE Identity Server Policy Agent for Lotus Domino 5.0.10 supports only the Single Sign-on (SSO) feature of Sun ONE Identity Server. This chapter explains how to install the Sun ONE Identity Server Policy Agent for Lotus Domino 5.0.10 server running on the Windows 2000 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Configuring the Domino DSAPI Filter
- Using Secure Sockets Layer (SSL) With an Agent
- Troubleshooting Information

Before You Begin

Be sure that you are familiar with the concepts presented in Chapter 1, “Read This First.” The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache

- Global Not-Enforced List
- The AMAgent.properties File

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version to install the Policy Agent.

Installing the Policy Agent Using GUI

You must have administrator privileges to run the Installation program.

1. Unzip the product binaries file.
2. Run the Installation program by double-clicking `setup.exe`.
3. In the Welcome panel, click Next.
4. Read the License Agreement. Click Yes to agree to the license terms.
5. In the Select Installation Directory screen, select where you would like to install the agent by clicking Browse, or click Next to accept the default.
6. Mark the check box to select the component "Sun™ ONE Identity Server Policy Agent 1.1 for Lotus Domino 5.0.10" and click Next.
7. Provide the following information about the web server where this agent will be installed:

   Host Name: Enter the fully qualified domain name of the system where the agent web server is installed. For example, `mycomputer.siroe.com`.

Domino directory: Enter the full path to the directory where the Domino Web Server instance is located. This is the web server instance that the agent will protect. For example, */Web_Server_root*/`https-mycomputer.siroe.com`.

Domino Data directory: Enter the full path to the directory where the Domino data is located.

Web Server Port: Enter the port number for the web server that will be protected by the agent.

Web Server Protocol: If the web server has been configured for SSL, then select HTTPS; otherwise select HTTP.

Agent Deployment URI: Enter a directory name. The default URI for the policy agent is `/amagent`.

The Universal Resource Identifier (URI) prefix tells the web server where to look for HTML pages the agent needs to display. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an "Access denied" message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory denoted by this URI, will be created in the web server Document Root you supplied.

If all the information entered is correct, click Next.

8. Provide the following information about the web server that runs Identity Server services.

Identity Server Services Host: Enter the fully qualified domain name of the system where the primary web server that runs Identity Server services is installed. For example, `myserver.siroe.com`.

Identity Server Services Port: Enter the port number for the primary web server that runs Identity Server services.

Identity Server Services Protocol: If the web server that runs Identity Server services has been configured for SSL, then select HTTPS; otherwise select HTTP.

Identity Server Services Deployment URI: Enter the location that was specified when Identity Server was installed. The default Universal Resource Identifier (URI) for Identity Server is `/amserver`.

Failover Server Host: Enter the fully qualified domain name for the secondary web server that will run Identity Server services if the primary server becomes unavailable. If no failover server exists, then leave this field blank.

Failover Server Port: Enter the port number of the secondary web server that will run Identity Server services. If no failover server exists, then leave this field blank.

9. If all the information entered is correct click Next.
10. Click Install Now.
11. When the installation is complete you may review the details, and then click Exit.

After the agent is installed successfully, configure the Domino DSAPI filter. See "Configuring the Domino DSAPI Filter," on page 118.

Uninstalling the Policy Agent

1. Invoke Lotus Notes, choose File > Preferences > Local Preferences.
2. Click Internet Protocols > HTTP tab.
3. Remove the DSAPI filter file name and leave this field blank.
4. Click the Save and Close button to save the changes.
5. Open Domino console and restart the server by entering the following commands:

   ```
   tell http quit
   ```

   ```
   load http
   ```

6. From the Start Menu, choose Settings > Control Panel.
7. In the Control Panel, double-click Add / Remove Programs.
8. In the Add/Remove Programs window, choose iPlanet Directory Services Access Management Edition Agent 1.1 for Lotus Domino 5.0.10 and then click Change/Remove.
9. In the Welcome Panel, click Next.
10. In the Type of Uninstall Panel, select Full.

NOTE Since there is only one component, it is recommended that you select Full uninstallation.The Partial uninstallation is not supported.

11. Click Uninstall Now.

12. Click Exit after uninstallation is complete.

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

Installing the Policy Agent Using the Command Line

1. In the directory where you unzipped the binaries file, at the command line, enter the following command:

   ```
   java agent_Domino_W2K -nodisplay
   ```

2. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement?

   Install Sun ONE Identity Server Agent in this directory: Specify the directory where you want the agent to be installed. To accept the default directory that is displayed in brackets, press Enter. Otherwise, enter a full path.

3. The following text displays:

```
Sun ONE Identity Server Agent components showing a checked box
will be installed. Only one agent may be installed at a time.
[ ]  1  Sun(TM) ONE Identity Server Policy Agent for Lotus Domino
5.0.10
```

Enter 1 to install the agent.When a check mark appears beside your choice, enter 0 to continue.

4. When prompted, provide the following information about the Domino server instance this Agent will protect:

- Host Name
- Domino directory
- Domino Data directory
- Web Server Port
- Web Server Protocol
- Agent Deployment URI

For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 112.

5. When prompted, provide the following information about the Domino Server that runs Identity Server Services:

   - Identity Server Services Host
   - Identity Server Services Port
   - Identity Server Services Protocol
   - Identity Server Services Deployment URI
   - Failover Server Host
   - Failover Server Port

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 112.

6. When displayed, review the summary of installation information you’ve specified. Press Enter to continue, or enter and exclamation point (!) to exit the program.

7. The following message displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation

What would you like to do
```

To continue with installation, enter 1.

8. After the agent is installed, configure the Domino DSAPI filter. Refer to "Configuring the Domino DSAPI Filter," on page 118

Uninstalling the Policy Agent

1. In the *Agent_Install_Dir* directory, at the command line, enter the following command:

   ```
   java uninstall_DSAME_Agent_Pack -nodisplay
   ```

2. When prompted, provide the following information:

   Please select the type of uninstall to perform from the following choices: To remove the product and all of the components, enter 1 for Full. To select some, but not all, product components to removed, enter 2 for Partial.

NOTE Since there is only one component, it is recommended that you enter 1 for Full uninstallation.The Partial uninstallation is not supported.

3. The following message displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
What would you like to do?
```

To begin uninstalling the agent, enter 1.

4. The following message displays

```
Product                 Result    More Info
1.  Domino Agent        Full      Available
2.  Done
```

To see log information, enter 1. To exit the Installation program, enter 2.

5. When the Installation program is finished, you must reboot the system.

Configuring the Domino DSAPI Filter

Use the following procedure to configure DSAPI filter.

1. Invoke Lotus Notes, choose File > Preferences > Local Preferences.
2. Click Internet Protocols > HTTP tab.
3. Enter the following for DSAPI filter file name:

   Agent_Install_Dir`\Agents\Domino\lib\amdomino.dll`
4. On Domino console restart the server by entering the following commands:

   ```
   tell http quit
   ```

   ```
   load http
   ```

Using Secure Sockets Layer (SSL) With an Agent

During Installation, if you specify the HTTPS protocol for the web server that runs Identity Server services, the agent is automatically configured to communicate over SSL.

The Agent's Default Trust Behavior

By default, a policy agent is installed on a Domino Server that will trust any server certificate presented over SSL by the web server that runs Identity Server services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs Identity Server services is SSL-enabled, and you want the policy agent to perform certificate-checking, you must do the following:

1. Disable the agent's default trust behavior.
2. Install a CA certificate on the web server where the agent is installed. The CA certificate must the be same one that is installed on the web server that runs Identity Server service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to `true`:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the Domino server must be the same one that is installed on the web server that runs Identity Server services.

To Install the CA Certificate on Domino Server

See the instructions for installing a CA Certificate in the documentation that comes with the web server. Generally, this is done through the web server's Administration console.

1. Go to the following directory:

   Agent_Install_Dir`\Agents\domino\utils`

2. Add the same certificate that is installed on the web server that runs Identity Server services into the existing certificate database. At the command line, enter the following command:

   `certutil -A -n` *cert-name* `-t "C,C,C" -d` *cert-dir* `-i` *cert-file*

   using the following variables:

   - *cert-name* can be any name for this certificate.
   - *cert-dir* is directory where the certificate-related files are located. On Windows the locations is:

     Agent_Install_Dir`\Agents\domino\cert`

   - *cert-file* is the base-64 encoded certificate file.
   - For more information on `certutil`, type `certutil -H`

3. Restart Domino Server.

Troubleshooting Information

- Installation failure

  Generate debug file by executing the following command:

  ```
  java agent_Domino_W2K -debug -debugMessage
  ```

  Check the debug messages in the debug file `agent_Domino_W2K.class`

- Unable to start Domino Server

  Check the Windows registry and verify whether the registry key `HKEY_LOCAL_MACHINE\Software\Sun ONE\IS Domino Agent` has the Install path set correctly to *Agent_Install_Dir*.

- Domino Server starts with an error message "Unable to load filter".

  Ensure that you have set the DSAPI filter correctly.

- The Sun ONE Identity Server Policy Agent uninstaller displays a blank screen and hangs when Partial uninstallation type is selected.

  To troubleshoot this problem:

  a. Close the Command Prompt window from where you executed the uninstall script.

b. Delete the `productregistry.access.tmp` file located at `C:\Winnt\system32`

c. Run the uninstall script again.

Chapter 8

Policy Agent for Sun ONE Web Server 6.0

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server to grant or deny user access to web servers in an enterprise. This chapter explains how to install and configure the Sun ONE Identity Server Policy Agent for Sun ONE Web Server 6.0 running on the Solaris 9 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Installing Multiple Web Server Agents on the Same Solaris Computer System
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses

Before You Begin

Be sure that you are familiar with the concepts presented in Chapter 1, “Read This First.” The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement

- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Installing Multiple Web Server Agents on the Same Computer System
- Providing Failover Protection for Identity Server Agents
- Updating the Agent Cache
- Global Not-Enforced List
- The AMAgent.properties File

Using the Graphical User Interface (GUI) Version of the Installation Program

The GUI version of the Installation program allows you to install only one policy agent at a time.

Installing a Web Server Policy Agent

Use these instructions for installing Agent for Sun ONE Web Server 6.0.

You must have root permissions when you run the agent installation program.

1. Unpack the product binaries file using the following command:

```
# gunzip -dc
S1WebServer_6.0_agent_1.2.sparc-sun-solaris2.8.tar.gz | tar
-xvof -
```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

```
# ./setup
```

3. In the Welcome Screen, click Next.
4. In the Software License Agreement screen, read the License Agreement. Click Yes(Accept License) to agree to the license terms.

5. In the Select Installation Directory screen, provide the following information:

   Install SunONE Webserver Agent in this directory: Enter the full path to the directory where you want this agent to be installed, and then click Next.

6. **Choose an Agent Install component**: By default, Sun(TM) ONE Identity Server Policy Agent 1.2 for Sun ONE Web Server 6.0 is selected, click Next.

7. In the Agent Web Server Information screen, provide the following information about the web server this agent will protect:

   Host Name: Enter the fully qualified domain name of the machine where the web server is installed. For example, `mycomputer.siroe.com`.

   Sun ONE Web Server Instance Directory: Specify the web server instance that this agent will protect. Enter the full path to the directory where the web server instance is located. Example:

   /Web_Server_root`/https-`*server_instance*

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

   Web Server Protocol: If the web server has been configured for SSL, choose HTTPS; otherwise choose HTTP.

   Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`.

   The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an “Access denied” message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

   When all the information is entered correctly, click Next.

8. In the Identity Server Services Information screen, enter information about the web server that runs Identity Server policy and management services. The Policy Agent will connect to this server.

   Identity Server Services Host: Enter the fully qualified domain name of the system where the primary web server that runs Identity Server services is installed. For example, `myserver.siroe.com`.

   Identity Server Services Port: Enter the port number for the web server that runs Identity Server services.

   Identity Server Services Protocol: If the web server that runs Identity Server services is SSL-enabled, select HTTPS; otherwise select HTTP.

   Identity Server Services Deployment URI: Enter the location that was specified when Identity Server was installed. The default Universal Resource Identifier (URI) for Identity Server is `/amserver`.

   Failover Server Host: Enter the fully qualified name for the secondary web server that will run Identity Server services if the primary web server becomes unavailable. If no failover host exists, then leave this field blank.

   Failover Server Port: Enter the port number of the secondary web server that runs Identity Server services. If no failover host exists, then leave this field blank.

   When all the information is entered correctly, click Next.

9. In the Summary of all the Selections screen, review the Installation Summary to be sure that the information you've entered is correct. If you want to make changes, click Back. If all the information is correct, click Next

10. In the Ready to Install page, click Install Now.

11. When the installation is complete, you can click Details to view details about the installation, or click Exit to end the Installation program.

12. You must restart your Sun ONE Web Server for the installation to be complete.

Uninstalling a Web Server Policy Agent

To uninstall an agent, you must run the Uninstallation program. Follow the steps below:

1. In the directory where the agent is installed, at the command line, enter the following command:

   ```
   # ./uninstall_SunONE_Webserver_agent
   ```

2. Click Next on Welcome Panel.
3. In the Select Type of Uninstall screen, select Full to remove the product and all of the components from your system.
4. Click Uninstall Now.
5. Click Exit after uninstallation is complete.

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

To Install an Agent Using the Command Line

1. In the directory where you unpacked the binaries file, at the command line, enter the following:

   ```
   # ./setup -nodisplay
   ```

2. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement? Enter yes.

   Install Sun ONE Webserver Agent in this directory: Enter the full path to the directory in which you want to install the policy agent.

   The following text displays:

```
SunONE Webserver Agent components showing a checked box will be installed.
Only one agentmay be installed at a time.
[ ]  1 Sun(TM) ONE Identity Server Policy Agent for SunONE Web Server 6.0
```

To check a particular component, enter its number, or 0 when you are finished: Enter the number that corresponds to the policy agent you want to install. The following message displays, with a checkmark beside the server your specified.

```
[X]  1 Sun(TM) ONE Identity Server Policy Agent for SunONE Web Server 6.0
```

To check a particular component, enter its number, or 0 when you are finished: Enter 0 to continue.

3. Provide the following information about the iPlanet Web Server this agent will protect:
   - Host Name
   - SunONE Web Server Instance Directory
   - Web Server Port
   - Web Server Protocol
   - Agent Deployment URI

   For details on these items, refer to "Using the Graphical User Interface (GUI) Version of the Installation Program" on page 124.
4. Provide the following information about the web server that runs Identity Server Services:
   - Identity Server Services Host
   - Identity Server Services Port
   - Identity Server Services Protocol
   - Identity Server Services Deployment URI
   - Failover Server Host
   - Failover Server Port

   For details on these items, refer to "Using the Graphical User Interface (GUI) Version of the Installation Program" on page 124.
5. The Summary of all the selections you have made is displayed.
6. The following text displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation
```

When prompted, **What would you like to do?**, enter `1` to start the installation.

7. The Installation details are displayed:

```
Product                    Result       More Info
1. SunONE Webserver Agent  Installed    Available
2. Done
```

To see log information on the agent, enter 2.To exit the Installation program, enter 2.

To Uninstall an Agent Using the Command Line

1. From the directory where the agent is installed, enter the following command at the command line:

```
# ./uninstall_SunONE_Webserver_agent -nodisplay
```

2. The following text displays:

```
Please select the type of uninstall to perform from the following
choices:
1. Full
2. Partial
```

To remove the product and all of the components from your system, enter `1` for Full. To remove some, but not all, product components, enter `2` for Partial.

3. The following text displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
```

When prompted, **What would you like to do**? enter 1 to begin uninstallation.

4. The following text displays:

```
Product                        Result     More Info
1.  SunONE Webserver Agent     Full       Available
2.  Done
```

To see log information on the agent, enter 1. To exit the Uninstallation program, enter 2.

Installing Multiple Web Server Agents on the Same Solaris Computer System

To install multiple web server agents on a single computer system, use the graphical user interface (GUI) version of the Agent Installation program to install the first agent. After the first agent is installed, you can then install successive agents using the `config` script. This script must be run from the command line as described in the next section.

To Install Multiple Web Server Agents on the Same Computer System

Once you have installed an agent on a system, you can install successive agents on that system using a script that copied to the system during the agent installation. The two scripts, `config` and `unconfig` are located in the following directory:

Agent_Install_Dir/SUNWam/iws60/bin

To install additional agents on a system after the original agent has been installed, run the config script from the bin directory using the following command:

```
# ./config
```

Follow the prompts to install the additional agents. For information on each of the prompts, see "Installing a Web Server Policy Agent". In general, information needs to be entered for both the protected web server instance and the Identity Server(s). The following text shows an example run:

```
# ./config
Enter the Web Server Instance Directory:
[/Web_Server_root/https-server_instance]
Enter the Local Hostname: [mycomputer.siroe.com]
Enter the Agent Web Server Port: [80]
Select Agent Web Server Protocol: [1] http [2] https-->[1]
Enter the Agent Deployment URI: [/amagent]
Enter the DSAME Service Host: [mycomputer.siroe.com]
Enter the DSAME Service Port: [58080]
Select DSAME Service Protocol: 1. http 2. https-->[1]
Enter the DSAME Deployment URI: [/amserver]
Enter the DSAME Failover Server Host: []
Enter the DSAME Failover Server Port: []
Configuring webserver ... Webserver version:  6.0
The directory
/var/opt/SUNWam/agents/_usr_iplanet_servers_https-server_instance
does not exist. Creating it.
Deploying  web application
Loading  new configuration
Web application deploy successful

done
```

Using the config Script for Silent Installations

The config script can also be used to do silent, non-interactive agent installations. For details on its usage, use the config -h command to display details on the config command:

```
# ./config -h
Usage: config [ -r response_file | -R | -h ]
        -r specifies a response file.
        -R prints out the response file template.
        -h prints out this message.
```

In order to perform a silent installation, you must supply a *response.file* for each of the agents you want to install. The command `config -R` indicates the fields which you must supply in the *response.file*. This text file needs to be created before you begin the silent installation.

```
# ./config -R
Response file contains:
AGENT_HOST        # agent hostname
WS_INSTANCE_DIR   # iWS instance directory
AGENT_PORT        # agent server port
AGENT_PROTOCOL    # agent protocol: http|https
AGENT_DEPLOY_URI  # agent deploy URI
SERVER_HOST       # dsame server name
SERVER_PORT       # dsame server port
SERVER_PROTO      # dsame server protocol: http|https
SERVER_DEPLOY_URI # dsame server deploy URI
FAILOVER_S_HOST   # dsame fail over server name
FAILOVER_S_PORT   # dsame fail over server port
```

Here is an example *response.file*, named `response.iws60`:

```
AGENT_HOST=mycomputer.siroe.com
WS_INSTANCE_DIR=/Web_Server_root/https-server_instance
AGENT_PORT=80
AGENT_PROTOCOL=http
AGENT_DEPLOY_URI=/amagent
SERVER_HOST=mycomputer.siroe.com
SERVER_PORT=http
SERVER_PROTO=58080
SERVER_DEPLOY_URI=/amserver
FAILOVER_S_HOST=
FAILOVER_S_PORT=
```

Below is an example showing how the `config` script is used in conjunction with the `response.iws60` response file to complete a silent installation:

```
# ./config -r ./response.iws60
Configuring webserver ... Webserver version:
The directory
/var/opt/SUNWam/agents/_usr_iplanet_servers_https-server_instance
does not exist. Creating it.
Deploying  web application
Loading  new configuration
Reconfigure failure: server not running
```

```
Web application deploy successful

done
```

NOTE Be sure to use the `unconfig` script to uninstall any agent that was installed using the config script—you cannot use the GUI installation program to uninstall agents that were installed via the command line.

Removing an Agent Using the unconfig Script

To remove an agent that was installed from the command line using the `config` script, use the script `unconfig`. The `unconfig` script is located in the following directory:

Agent_Install_Dir`/SUNWam/iws60/bin`

Here is an example run of the `unconfig` script:

```
# ./unconfig /Web_Server_root/https-server_instance
Unconfiguring webserver ... Deleting web application
Loading  new configuration
Reconfigure failure: server not running

Web application delete successful
done.
```

NOTE You cannot uninstall the original agent if multiple web server agents are installed on the system. To uninstall the original agent, uninstall the agents using `unconfig` script and uninstall the original agent using command line.

Using Secure Sockets Layer (SSL) with an Agent

During installation, if you choose the HTTPS protocol, the agent is automatically configured and ready to communicate over SSL.

NOTE Before proceeding with the following steps, you should have a solid understanding of SSL concepts and the security certificates required to enable communication over the HTTPS protocol. See the documentation that comes with your web server or access from the following site:

`http://docs.sun.com/source/816-5691-10/esecurty.htm`

The Agent's Default Trust Behavior

By default, the Policy Agent installed on a Sun ONE Web Server 6.0 that will trust any server certificate presented over SSL by the web server that runs Identity Server services; the agent does not check the Certificate Authority (CA) certificate. If the web server that runs Identity Server services is SSL-enabled, and you want the URL policy agent to perform certificate-checking, you must do two things:

1. Disable the agent's default trust behavior.
2. Install CA certificate on the remote web server (where the agent is installed). The CA certificate must the be same one that is installed on the web server that runs Identity Server service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to true:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the web server must be the same one that is installed on the web server that runs Identity Server services.

To Install the CA Certificate on iPlanet Web Server

See the Web Server documentation for installing a CA Certificate.

`http://docs.sun.com/source/816-5691-10/`

Setting the REMOTE_USER Server Variable

The `REMOTE_USER` server environment variable can be set to a Identity Server authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

`REMOTE_USER` will be set while accessing allowed URLs.

To enable the `REMOTE_USER` setting for globally not-enforced URLs as specified in the `AMAgent.properties` file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the `AMAgent.properties` file to `TRUE` (by default, this value is set to `FALSE`):

```
com.iplanet.am.policy.agents.anonRemoteUser.enable=TRUE
```

When you set this property value to `TRUE`, the value of `REMOTE_USER` will be set to the value contained in the following property in the `AMAgent.properties` file (by default, this value is set to `anonymous`):

```
com.iplanet.am.policy.agents.unauthenticatedUser=anonymous
```

Forwarding LDAP User Attributes via HTTP Headers

Identity Server agents has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of Identity Server. An Identity Server agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in `AMAgent.properties` file. To turn this feature on and off, use the following `AMAgent.properties` file property:

`com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable`

By default, this property is set to `false`, and the feature off. To turn on attribute forwarding, set this property to `true`. To configure the attributes that are to be forwarded in the HTTP headers, use the `AMAgent.properties` file property `com.iplanet.am.policy.agents.ldapattr`.

Below is an example section in the `AMAgent.properties` file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web
servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case
letters,
#       and any _ will become -
# NOTE: for IIS and Apache agents, "http_header_name" will be
prefixed
#       by HTTP_, and all lower case letters will become upper
case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organiza
tion-unit,o|organization,
c|country,mail|email,employeenumber|employee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the Identity Server is installed:

DSAME_Install_Dir`/SUNWam/config/xml/amUser.xml`

The attributes in this file could be either Identity Server User attributes or Identity Server Dynamic attributes (for explanation of these two types of user attributes, refer to the *Sun ONE Identity Server Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the web server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

NOTE Each web server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each property in the `AMAgents.properties` file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or *hijacking* of SSO tokens.

The `AMAgent.properties` file contains a property titled `com.iplanet.am.policy.agents.client_ip_validation.enable`, which by default is set to `false`.

If you set this property value to `true`, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

This feature should not be used, however, if the client browser uses a web proxy or if there is a load-balancing application somewhere between the client browser and the agent-protected web server. In such cases, the IP address appearing in the request will not reflect the real IP address on which the client browser runs.

```
com.iplanet.am.policy.agents.client_ip_validation.enable=true
```

Chapter 9

URL Policy Agent for IBM HTTP Server 1.3.19

Sun ONE Identity Server Policy Agents work in tandem with Sun ONE Identity Server to grant or deny user access to web servers in an enterprise. This chapter explains how to install the Sun ONE Identity Server Policy Agent for IBM HTTP Server 1.3.19 running on Solaris 8 operating system.

Topics include:

- Before You Begin
- Using the Graphical User Interface (GUI) Version of the Installation Program
- Using the Command-Line Version of the Installation Program
- Using Secure Sockets Layer (SSL) with an Agent
- Setting the REMOTE_USER Server Variable
- Forwarding LDAP User Attributes via HTTP Headers
- Validating Client IP Addresses
- Known Issues

Before You Begin

Be sure you're familiar with the concepts presented in Chapter 1, "Read This First." The chapter includes brief but important information on the following topics:

- How Policy Agents Work
- Java Runtime Environment (JRE) 1.3.1_04 Requirement

- The Web Server that Runs Identity Server Services vs. Remote Web Servers
- Providing Failover Protection for Identity Server Agents
- The AMAgent.properties File

Using the Graphical User Interface (GUI) Version of the Installation Program

Use the GUI version of the Installation program to install agent.

Installing the Policy Agent Using GUI

You must have root permissions when you run the agent installation program.

1. Unpack the product binaries using the following command:

   ```
   # /bin/gzcat ibm_httpserver_1.3.19_agent_1.0_Solaris2.8.tar.gz |
   /bin/tar -xvf -
   ```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

   ```
   # ./setup
   ```

3. Set your `JAVA_HOME` environment variable to a JDK version 1.3.1_04 or higher. The installation requires that you setup your `JAVA_HOME` variable correctly. However, in case you have incorrectly set the `JAVA_HOME` variable, the setup script will prompt you for supplying the correct `JAVA_HOME` value:

   ```
   Please enter path to pick up java:
   ```

   Enter the full path where JDK is located to launch the installer.

4. In the Welcome page, click Next.
5. Read the License Agreement. Click Yes to agree to the license terms.

6. In the Select Installation Directory window, provide the following information:

   Install Sun ONE Identity Server Policy Agent in this directory: Enter the full path to the directory where you want this agent to be installed, and then click Next.

7. By default, Sun(TM) ONE Identity Server Policy Agent 1.0 for IBM HTTP Server 1.3.19 is selected, click Next.

8. In the Agent Web Server Information window, provide the following information about the IBM HTTP server this agent will protect:

   Host Name: Enter the fully qualified domain name of the machine where the IBM HTTP server is installed. For example, `mycomputer.siroe.com`.

   IBM HTTP Server config file: Enter the full path to the directory where the `httpd.conf` file is located.

   Web Server Port: Enter the port number for the web server that will be protected by the agent.

   Web Server Protocol: If the web server has been configured for SSL, choose HTTPS; otherwise choose HTTP.

   Agent Deployment URI: Enter a directory name. The default Universal Resource Identifier (URI) is `/amagent`

   The URI prefix tells the web server where to look for HTML pages that need to be displayed. For example, when a user attempts to access a URL, but cannot provide proper credentials, the agent must display an “Access denied” message. The URI prefix tells the web server where to look for the HTML page that contains the message. A directory specified by this URI will be created in the web server Document Root.

   When all the information is entered correctly, click Next.

9. In the Identity Server Information window, provide information about the web server that runs Identity Server policy and management services. The URL Policy Agent will connect to this server.

   Identity Server Services Host: Enter the fully qualified domain name of the system where the primary web server that runs Identity Server services is installed. For example, `myserver.siroe.com`.

   Identity Server Services Port: Enter the port number for the web server that runs Identity Server services.

   Identity Server Services Protocol: If the web server that runs Identity Server is SSL-enabled, select HTTPS; otherwise select HTTP.

   Identity Server Services Deployment URI: Enter the location that was specified when Identity Server was installed. The default Universal Resource Identifier (URI) for Identity Server is `/amserver`.

   Failover Server Host: If you have configured a failover web server to run Identity Server services, enter the host name of the failover system. Examples: `backup.siroe.com`. If there is no failover server, then leave this field blank.

   Failover Server Port: If you have configured a failover web server to run Identity Server services, enter the web server port number. If there is no failover host server, then leave this field blank.

10. Review the Installation Summary to be sure that the information you've entered is correct. If you want to make changes, click Back. If all the information is correct, click Next.

11. In the Ready to Install page, click Install Now.

12. When the installation is complete, you can click Details to view details about the installation, or click Exit to end the Installation program.

13. You must restart your IBM HTTP server for the installation to be complete. At the command line enter the following:

    ```
    /opt/IBMHTTPD/bin/apachectl stop
    ```

    ```
    /opt/IBMHTTPD/bin/apachectl start
    ```

Uninstalling and Disabling the Policy Agent

When you no longer require the URL policy agent, you can uninstall it or disable it.

Uninstalling a URL Policy Agent

Use the following steps to uninstall the Policy Agent.

1. In the directory where the agent is installed, at the command line, enter the following command:

   ```
   # ./uninstall_IBMHttp
   ```

   The uninstallation requires that you setup your `JAVA_HOME` variable correctly. However, in case you have incorrectly set the `JAVA_HOME` variable, the `setup` script will prompt you for supplying the correct `JAVA_HOME` value:

   ```
   Please enter path to pick up java:
   ```

   Enter the full path where JDK is located to launch the installer.

2. Click Next on Welcome panel.
3. In the Select Type of Uninstall panel, select Full and click Next.
4. Click Uninstall Now.
5. Click Exit after uninstallation is complete.

Disabling a URL Policy Agent

Use the following steps to disable a URL Policy Agents.

1. In the file `httpd.conf` remove or comment out the following line:

   ```
   # include
   /etc/opt/SUNwam/conf/IBMHTTP/_opt_IBMHTTPD_conf/dsame.conf
   ```

2. Restart the server:

   ```
   /opt/IBMHTTPD/bin/apachectl stop
   ```

   ```
   /opt/IBMHTTPD/bin/apachectl start
   ```

Using the Command-Line Version of the Installation Program

The command-line version of the Installation program provides you an alternative to the graphical user interface (GUI) version.

Installing an Agent Using the Command Line

You must have root permissions when you run the agent installation program.

1. Unpack the product binaries file using the following command:

   ```
   # /bin/gzcat ibm_httpserver_1.3.19_agent_1.0_Solaris2.8.tar.gz |
   /bin/tar -xvf -
   ```

NOTE Use the tar that is shipped with Solaris. Don't use the GNU tar.

2. Run the `setup` program. You'll find the program in the directory where you untarred the binaries file. At the command line, enter the following:

   ```
   # ./setup -nodisplay
   ```

3. Set your `JAVA_HOME` environment variable to a JDK version 1.3.1_04 or higher. The installation requires that you setup your `JAVA_HOME` variable correctly. However, in case you have incorrectly set the `JAVA_HOME` variable, the `setup` script will prompt you for supplying the correct `JAVA_HOME` value:

   ```
   Please enter path to pick up java:
   ```

   Enter the full path where JDK is located to launch the installer.

4. When prompted, provide the following information:

   Have you read, and do you accept, all of the terms of the preceding Software License Agreement? Enter yes.

   Install Sun ONE Identity Server Policy Agent in this directory: Enter the full path to the directory in which you want to install the policy agent.

   The following text displays:

```
Sun ONE Identity Server Policy Agent for IBM HTTP Server
components showing a checked box will be installed. Only one
agent may be installed at a time.
[ ]  1 Sun(TM) ONE Identity Server Policy Agent 1.0 for IBM HTTP
Server 1.3.19
```

To check a particular component, enter its number, or 0 when you are finished: Enter the number that corresponds to the policy agent you want to install. The following message displays, with a cross mark beside the server you specified.

```
[X]  1 Sun(TM) ONE Identity Server Policy Agent 1.0 for IBM HTTP
Server 1.3.19
```

To check a particular component, enter its number, or 0 when you are finished: Enter `0` to continue.

5. Provide the following information about the IBM HTTP server this agent will protect.

   - `Host Name`
   - `IBM HTTP Server config file`
   - `Web Server Port`
   - `Web Server Protocol`
   - `Agent Deployment URI`

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 140.

6. Provide the following information about the web server that runs Identity Server services. The following fields refer to the system where Identity Server is installed.

   - `Identity Server Services Host Name`
   - `Identity Server Services Port Number`
   - `Identity Server Services Protocol`
   - `Identity Server Services Deployment URI`
   - `Failover Server Host`
   - `Failover Server Port`

   For details on these items, refer to “Using the Graphical User Interface (GUI) Version of the Installation Program” on page 140.

7. The following text displays:

```
Ready to Install

1. Install Now
2. Start Over
3. Exit Installation
```

When prompted, **What would you like to do?**, enter `1` to start the installation.

8. The following text displays:

```
Product                                  Result     More Info
1.Sun ONE Identity Server Policy Agent   Installed  Available
2.Done
```

To see log information, enter `1`. To exit the Installation program, enter `2`.

Uninstalling an Agent Using the Command Line

1. In the directory where you unpacked the binaries, at the command line, enter the following command at the command line:

```
#./uninstall_IBMHttp -nodisplay
```

2. The following text displays:

```
Please select the type of uninstall to perform from the following
choices:
1. Full
2. Partial
```

To remove the product and all of the components from your system, enter `1` for Full. To remove some, but not all, product components, enter `2` for Partial.

3. The following text displays:

```
Ready to Uninstall

1. Uninstall Now
2. Start Over
3. Exit Uninstallation
```

When prompted, **What would you like to do**? enter `1` to begin uninstallation.

4. The following text displays:

```
Product                                  Result  More Info
1.Sun ONE Identity Server Policy Agent   Full    Available
2.Done
```

To see log information on the agent, enter `1`. To exit the Installation program, enter `2`.

Using Secure Sockets Layer (SSL) with an Agent

During installation, if you specify the HTTPS protocol for the web server that runs Identity Server services, the agent is automatically configured to communicate over SSL with Identity Server services.

Configuring the IBM HTTP Server

Use the following instructions to configure the IBM HTTP Server to run in SSL Mode.

1. Create a new Key Database using the Key Management Utility (IKEYMAN). For information on creating new key database, see the documentation at: `http://www-3.ibm.com/software/webservers/httpservers/doc/v1319/9atikeyu.htm#HDRKMU2G`

2. Create a Self-signed certificate using the Key Management Utility (IKEYMAN). For information on creating a self-signed certificate, see the documentation at: `http://www-3.ibm.com/software/webservers/httpservers/doc/v1319/9atikeyu.htm#HDRKMU4G`

3. Start the Administration Server

   ```
   # /opt/IBMHTTPD/bin/adminctl start
   ```

4. Setup SSL using the IBM Administration Server. For information on setting up SSL, see the documentation at: `http://www-3.ibm.com/software/webservers/httpservers/doc/v1319/9atstart.htm#ssl`

The Agent's Default Trust Behavior

By default, a URL policy agent is installed on a IBM HTTP server that will trust any server certificate presented over SSL by the web server that runs Identity Server services; the agent does not check the root Certificate Authority (CA) certificate. If the web server that runs Identity Server services is SSL-enabled, and you want the URL policy agent to perform certificate-checking, you must do the following:

1. Disable the agent's default trust behavior.

2. Install a root CA certificate on the IBM HTTP Server (where the agent is installed). The CA certificate must the be same one that is installed on the web server that runs Identity Server service.

Disabling the Agent's Default Trust Behavior

The following property exists in the `AMAgent.properites` file, and by default it is set to true:

```
com.iplanet.am.policy.agents.trust_server_certs=true
```

This means that the agent does not perform certificate-checking.

To Disable the Default Behavior

The following property must be set to `false`:

```
com.iplanet.am.policy.agents.trust_server_certs=false
```

Installing the CA Certificate

The CA certificate that you install on the IBM HTTP Server must be the same one that is installed on the web server that runs Identity Server services.

To Install the CA Certificate on IBM HTTP Server

You can use the `certutil` program to install the CA Certificate on IBM HTTP Server.

1. In C shell, at the command line, enter the following commands:

   ```
   # cd /Agent_Install_Dir/SUNWam/IBMHttp/cert
   # setenv LD_LIBRARY_PATH /Agent_Install_Dir/SUNWam/IBMHttp/lib
   # export LD_LIBRARY_PATH
   # ./certutil -A -n cert-name -t "C,C,C" -d . -i cert-file
   ```

   In the commands above, the variables represent the following:

   - *cert-name* can be any name for this certificate.
   - *cert-dir* is directory where the certificate-related files are located.
   - *cert-file* is the base-64 encoded certificate file.

   For more information on the `certutil` utility, enter `certutil -H` for on-line Help.

2. To verify that the certificate is properly installed, at the command line, enter the following:

   ```
   # ./certutil -L -d .
   ```

   Trust database information will display including the name of the CA certificate you installed. Example:

```
Certificate Name Trust Attrubutes

rootCAcert

p    Valid peer
P    Trusted peer (implies p)
c    Valid CA
T    Trusted CA to issue client certs (implies c)
C    Trusted CA to certs(only server certs for ssl) (implies c)
u    User cert
w    Send warning
```

Setting the REMOTE_USER Server Variable

The REMOTE_USER server environment variable can be set to Identity Server authenticated user or anonymous user. By setting this variable to a specific user, the user becomes available to web applications (such as a CGI, servlet, or ASP program). This feature makes it possible to personalize the content of displayed HTML pages to specific users.

REMOTE_USER will be set while accessing allowed URLs.

To enable the REMOTE_USER setting for globally not-enforced URLs as specified in the AMAgent.properties file (these are URLs that can be accessed by unauthenticated users), you must set the following property in the AMAgent.properties file to TRUE (by default, this value is set to FALSE):

```
com.iplanet.am.policy.agents.anonRemoteUser.enable=TRUE
```

When you set this property value to TRUE, the value of REMOTE_USER will be set to the value contained in the following property in the AMAgent.properties file (by default, this value is set to anonymous):

```
com.iplanet.am.policy.agents.unauthenticatedUser=anonymous
```

Forwarding LDAP User Attributes via HTTP Headers

Identity Server agent has the ability to forward LDAP user attribute values via HTTP headers to end web applications. The LDAP user attribute values come from the server side of Identity Server. An Identity Server agent behaves like a broker to obtain and relay user attribute values to the destination servlets, CGI scripts, or ASP pages. These applications can in turn use the attribute values to personalize page content.

This feature is configurable through two properties in `AMAgent.properties` file. To turn this feature on and off, use the following `AMAgent.properties` file property:

`com.iplanet.am.policy.agents.foward_ldapattr_in_http_headers.enable`

By default, this property is set to `false`, and the feature off. To turn on attribute forwarding, set this property to `true`. To configure the attributes that are to be forwarded in the HTTP headers, use the `AMAgent.properties` file property `com.iplanet.am.policy.agents.ldapattr`.

Below is an example section in the `AMAgent.properties` file which shows how this feature is used:

```
# Ldap User Attributes
# format: ldap_attribute_name|http_header_name
#
# below are a few notes based on different behaviours of web servers
#
# NOTE: for iWS agents, "http_header_name" must be in lower-case letters,
#       and any _ will become _
# NOTE: for IIS, Apache and IBM HTTP Server agents"http_header_name" will
be prefixed
#       by HTTP_, and all lower case letters will become upper case,
#       and any - will become _
#
com.iplanet.am.policy.agents.ldapattr=cn|common-name,ou|organization-unit
,o|organization,c|country,mail|email,employeenumber|employee-number
```

By default, some LDAP user attribute names and HTTP header names are set to sample values.

To find the appropriate LDAP user attribute names, check the following XML file on the machine where the Identity Server is installed:

DSAME_Install_Dir/SUNWam/config/xml/amUser.xml

The attributes in this file could be either Identity Server User attributes or Identity Server Dynamic attributes (for explanation of these two types of user attributes, refer to the *Sun ONE Identity Server Administration Guide*).

The attribute and HTTP header names that need to be forwarded must be determined by the end-user applications on the IBM HTTP server that the agent is protecting—after all, these applications are the consumers of the forwarded header values (the forwarded information is used for the customization and personalization of web pages).

Each IBM HTTP server has its own peculiarities about HTTP header name conventions. For more information on this feature, refer to the comments listed before each respective property in the AMAgents.properties file.

Validating Client IP Addresses

This feature can be used to enhance security by preventing the stealing or *hijacking* of SSO tokens.

The AMAgent.properties file contains a property titled com.iplanet.am.policy.agents.client_ip_validation.enable, which by default is set to false.

If you set this property value to true, client IP address validation will be enabled for each in-coming request that contains an SSO token. If the IP address from which request was generated does not match the IP address issued for the SSO token, the request will be denied. This is essentially the same as enforcing a deny policy.

```
com.iplanet.am.policy.agents.client_ip_validation.enable=true
```

Cookie Reset Feature

This feature enables the Identity Server Policy Agent to reset some cookies in the browser session while redirecting to Identity Server for authentication. Currently, this feature is available only for IBM HTTP Server Agent.

This feature is configurable through two properties in AMAgent.properties file.

- Enable Cookie Reset

  ```
  com.iplanet.am.policy.agents.cookie.reset.enable=true
  ```

This property must be set to `true`, if this agent needs to reset cookies in the response while redirecting to Identity Server for Authentication. By default, this is set to `false`.

- Cookie List

  This property gives the comma separated list of cookies, that needs to be reset in the response while redirecting to Identity Server for authentication.

  This property is used only if the Cookie Reset feature is enabled.

  ```
  com.iplanet.am.policy.agents.cookie.reset.list=LtpaToken,
  otherToken
  ```

Known Issues

- First value not displayed for `objectclass` attribute

  Occasionally, the first value is not displayed for `objectclass` attribute that is added to HTTP LDAP header.

- Error message not dispalyed when null or space value is entered for installation directory.

  During agent installation, if space or null value is entered for installation directory, the installation program proceeds without displaying any error message and the agent is installed in the default directory (`/opt`).