CA SiteMinder®

Web Agent Installation Guide

r12.0 SP3

6th Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA CA Identity Manager
- CA SOA Security Manager

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- How to Prepare a Windows System for a Web Agent Installation (see page 13)—Removed reference to Visual C++ library prerequisite. Installation program now checks for and installs this library if needed. Resolves CQ171379.

Contents

Chapter 1: Preparation

This section contains the following topics:

Agent for IIS Procedures in Separate Guide

For SiteMinder r12.0 SP3, the procedures for installing a Web Agent on an IIS web server were moved to a separate installation Guide. Select the guide that fits your requirements from the following list:

- To install or configure an Agent on an IIS web server, see the SiteMinder *Agent Installation Guide for IIS*.
- To install or configure an Agent on any other type of web server, see the SiteMinder *Web Agent Installation Guide*.

How to Prepare for a Web Agent Installation

To prepare for a Web Agent installation, use the following process:

1. Prepare your web server by doing the following tasks:
   a. Verify that your web server meets the agent hardware requirements (see page 13).
   b. Ensure you have an account with one of the following for your web server:
      - Administrative privileges (for Windows systems).
      - Root privileges (for UNIX systems).
   c. Confirm that the operating system has the proper service packs or patches installed.
   d. Configure any options or settings required to operate a SiteMinder Agent on your type of web server. For example, compiling an Apache web server for use on a Linux System (see page 17).
2. Confirm the following items for all Web Agent installations:
   - Ensure the Policy Server is installed and configured (see page 20).
   - Gather the information needed to complete the Web Agent installation (see page 19).
   - Preserve the changes in your WebAgentTrace.conf file (see page 19).
   - Select the correct Agent for your web server (see page 20).
3. (Optional) Meet the prerequisites for password services (see page 23).
4. (Optional) Meet the prerequisites for registration services.

Hardware Requirements for SiteMinder Agents

Computers hosting SiteMinder agents require the following hardware:

Windows operating environment requirements

SiteMinder agents operating on Windows operating environments require the following hardware:

- CPU: x86 or x64
- Memory: 2-GB system RAM.
- Available disk space:
  - 2-GB free disk space in the installation location.
  - .5-GB free disk space in the temporary location.

UNIX operating environment requirements

SiteMinder agents operating on UNIX operating environments require the following hardware:

- CPU:
  - Solaris operating environment: SPARC
  - Red Hat operating environment: x86 or x64
- Memory: 2-GB system RAM.
- Available disk space:
  - 2-GB free disk space in the installation location.
  - .5-GB free disk space in /temp.

  Note: Daily operation of the agent requires 10 MB of free disk space in /tmp. The agent creates files and named pipes under /tmp. The path to which these files and pipes are created cannot be changed.

Supported Operating Systems and Web Servers

Before you install a Web Agent, make sure you are using a supported operating system and web server configuration. For a list of SiteMinder Web Agents and supported web server platforms, go to Technical Support, and search for the SiteMinder r12.0 SP3 Platform Matrix.

Note: After you install the Web Agent, you can configure multiple Web Agent instances for each Oracle iPlanet and Apache web server installed on your system.

How to Prepare a Windows System for a Web Agent Installation

To prepare your Windows system for a Web Agent installation, perform one or more of the following tasks, as required by your environment:

- Install an Apache web server as a service for all users (see page 14).

Install an Apache Web Server on Windows as a Service for All Users

When an Apache-based web server is installed using a single user account, the Agent configuration cannot detect the Apache-based web server installation.

To correct this problem, select the following option when you install an Apache-based web server on a Windows operating environment:

```
"install as a service, available for all users".
```

How to Prepare a UNIX System for a Web Agent Installation

To prepare your UNIX system for a Web Agent Installation, use the following process:

1. Set the DISPLAY variable.
2. Confirm that you have the required patches installed for your operating system, as shown in the following:
   - Required AIX patches (see page 15)
   - Required Solaris patches (see page 15)

Set the DISPLAY For SiteMinder Agent Installations on UNIX

If you are installing the SiteMinder Agent on a UNIX system from a remote terminal, such as a Telnet or Exceed terminal, be sure the DISPLAY variable is set for the local system. For example, if your machine is 111.11.1.12, set the variable as follows:

```
DISPLAY=111.11.1.12:0.0

export DISPLAY
```

Note: You can also install the agent using the console mode installation, which does not require the X window display mode.

Required Solaris Patches

Before installing a SiteMinder Agent on a Solaris computer, install the following patches:

Solaris 9

Requires patch 111711-16.

Solaris 10

Requires patch 119963-08.

You can verify installed patch versions by logging in as the root user and executing the following command:

```
showrev -p | grep patch_id
```

To locate Solaris patches, go to the Oracle Solution Center.

AIX Requirements

SiteMinder Web Agents running on AIX systems require the following:

- To run a re-architected (framework) SiteMinder Oracle iPlanet web agent or Apache Web Agent on an AIX system, your C/C++ runtime environment must be version 8.0.0.0.

  Note: For more information, see the following web site:
  http://www-1.ibm.com/support/docview.wss?uid=swg1IY78159

How to Prepare a Linux System for a Web Agent Installation

To prepare your Linux system for a Web Agent Installation, use the following process:

1. Verify that the proper Linux patches are installed.
2. Verify that the proper Linux libraries are installed.
3. Verify that the proper Linux tools are installed.
4. If you are using an Apache web server, compile it.

Required Linux Patches

The following Linux patches are required:

For Web Agents running on 64-bit Linux systems

- Binutils 2.17
- GCC 4.1.0

Required Linux Libraries

Certain library files are required for components operating on Linux operating environments. Failure to install the correct libraries can cause the following error:

```
java.lang.UnsatisfiedLinkError
```

If you are installing, configuring, or upgrading a Linux version of this component, the following libraries are required on the host system:

Red Hat 5.x

compat–gcc-34-c++-3.4.6-*patch_version*.I386

Red Hat 6.x (32-bit)

libstdc++-4.4.6-3.el6.i686.rpm

To have the appropriate 32-bit C run–time library for your operating environment, install the previous rpm.

Red Hat 6.x (64-bit)

libXau-1.0.5-1.el6.i686.rpm

libxcb-1.5-1.el6.i686.rpm

libstdc++-4.4.6-4.el6.i686.rpm

compat-db42-4.2.52-15.el6.i686.rpm

compat-db43-4.3.29-15.el6.i686.rpm

libX11-1.3-2.el6.i686.rpm

libXrender-0.9.5-1.el6.i686.rpm

libexpat.so.1 (provided by expat-2.0.1-11.el6_2.i686.rpm)

libfreetype.so.6 (provided by freetype-2.3.11-6.el6_2.9.i686.rpm)

libfontconfig.so.1 (provided by fontconfig-2.8.0-3.el6.i686.rpm)

libICE-1.0.6-1.el6.i686.rpm

libuuid-2.17.2-12.7.el6.i686.rpm

libSM-1.1.0-7.1.el6.i686.rpm

libXext-1.1-3.el6.i686.rpm

compat-libstdc++-33-3.2.3-69.el6.i686.rpm

compat-db-4.6.21-15.el6.i686.rpm

libXi-1.3-3.el6.i686.rpm

libXtst-1.0.99.2-3.el6.i686.rpm

libXft-2.1.13-4.1.el6.i686.rpm

libXt-1.0.7-1.el6.i686.rpm

libXp-1.0.0-15.1.el6.i686.rpm

Linux Tools Required

Before installing a SiteMinder Agent on a Red Hat Apache 2.2 web server running on the Red Hat Enterprise Linux operating environment, install all the items included in the Red Hat Legacy Software Development tools package.

Compile an Apache Web Server on a Linux System

For the SiteMinder Agent to operate with an Apache web server running Linux, you have to compile the server. Compiling is required because the Agent code uses pthreads (a library of POSIX-compliant thread routines), but the Apache server on the Linux platform does not, by default.

If you do not compile with the lpthread option, the Apache server starts up, but then hangs and does not handle any requests. The Apache server on Linux cannot initialize a module which uses pthreads due to issues with Linux's dynamic loader.

Follow these steps:

1. Enter the following:

```
LIBS=-lpthread
export LIBS
```

2. Configure Apache as usual by entering the following:

```
configure --enable-module=so --prefix=your_install_target_directory
make
make install
```

How to Prepare a Domino System for a Web Agent Installation

To prepare your Domino system for a Web Agent installation, ensure you have installed whichever of the following items is appropriate for your system:

- IBM Hot fixes for Domino 6.5.2 (see page 18)

IBM Hot Fix Required for Domino 6.5.2

IBM hot fix SPR #NORK632KQA is required for a Web Agent to run on a Domino 6.5.2 server.

This hotfix applies to Windows and UNIX platforms.

Miscellaneous Web Server Preparations

The following sections discuss installation preparations for various web servers.

Verify Presence of a Logs Subdirectory with Permissions for Apache-based Web Agents

For SiteMinder Agents for Apache-based web servers (including IBM HTTP Server), a logs subdirectory must exist under the root directory of the Apache-based web server. This subdirectory needs Read and Write permissions for the user identity under which the Apache child process runs.

If the logs subdirectory does not exist, create it with the required permissions.

Note: This configuration requirement applies to any Apache-based web server that writes log files outside the Apache root directory.

Enable Write Permissions for IBM HTTP Server Logs

If you install the SiteMinder Agent on an IBM HTTP Server, this web server gets installed as root and its subdirectories do not give all users in all groups Write permissions.

For the Low Level Agent Worker Process (LLAWP) to write agent initialization messages to the web server logs, the user running the web server needs permission to write to the web server's log directory. Ensure that you allow write permissions for this user.

Set the LD_LIBRARY_PATH Variable for IBM HTTP Server 7.0

Before you run the Web Agent Configuration wizard to configure an IBM HTTP Server 7.0, set the LD_LIBRARY_PATH variable as shown in the following example:

```
LD_LIBRARY_PATH=home_directory_of_your_IHS_7.0_server/lib
```

General Preparations for All Web Agents

The following sections describe general preparations for all Web Agents.

Gather information Needed to Complete the Agent Installation

You must have the following information before installing the Web Agent:

- Name of the SiteMinder Administrator allowed to install Agents
- Name of the Host Configuration Object. This defines the trusted host configuration.
- Name of the Agent Configuration Object, which contains the Agent configuration settings. A single Agent Configuration Object can be referenced by many Agents.

Backup your Existing WebAgentTrace.conf Files

If you are upgrading your Web Agent, and you have customized any WebAgentTrace.conf files, we recommend backing up your current WebAgentTrace.conf files

Important! Once the installer starts, the existing file is overwritten without warning. Your old settings are lost without a back-up copy of the original file.

After the installation, you can integrate your changes into the new file.

Install the Correct Agent for a Web Server

Install the following Web Agents with the corresponding web servers:

Web Agent	Web Server
Domino	IBM Lotus Domino
Sun Java System	Oracle iPlanet
Apache	Apache, HP-based Apache, IBM HTTP, Oracle HTTP Server. Most of the information for the Apache web server applies to these web servers.

For details on supported web server and operating system versions, go to Technical Support, and then search for the SiteMinder r12.0 SP3 Platform Support Matrix.

Policy Server Requirements

Verify that your Policy Server meets the following criteria:

- Is installed and configured.
- Is able to communicate with the computer where you plan to install the agent.

Note: For more information, see the Policy Server documentation.

To install and configure a SiteMinder agent, a Policy Server requires at least the following items:

- A SiteMinder administrator that has the right to register trusted hosts.

  A trusted host is a client computer where one or more SiteMinder Agents are installed and registered with the Policy Server. The SiteMinder administrator must have permissions to register trusted hosts with the Policy Server. Registering a trusted host creates a unique trusted host name object on the Policy Server.

- Agent identity

  An Agent identity establishes a mapping between the Policy Server and the name or IP address of the web server instance hosting an Agent. You define an Agent identity from the Agents object in the Administrative UI. You assign it a name and specify the Agent type as a Web Agent.

- Host Configuration Object (HCO)

  The host configuration object on the Policy Server defines the communication between the agent and the Policy Server. After an initial connection. Initial connections use the parameters in the SmHost.conf file.

- Agent Configuration Object (ACO)

  This object includes the parameters that define the agent configuration. All SiteMinder agents require at least one of the following configuration parameters defined in the ACO:

  AgentName

  Defines the identity of the web agent. This identity links the name and the IP address or FQDN of each web server instance hosting an Agent.

  The value of the DefaultAgentName is used instead of the AgentName parameter if any of the following events occur:

  - The AgentName parameter is disabled.
  - The value of AgentName parameter is empty.
  - The values of the AgentName parameter do *not* match any existing agent object.

  Note: This parameter can have more than one value. Use the multivalue option when setting this parameter in an Agent Configuration Object. For local configuration files, add each value to a separate line in the file.

  Default: No default

  Limit: Multiple values are allowed.

  Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. The value is not case-sensitive. For example, the names MyAgent and myagent are treated the same.

  Example: myagent1,192.168.0.0 (IPV4)

  Example: myagent2, 2001:DB8::/32 (IPV6)

  Example: myagent,www.example.com

DefaultAgentName

Defines a name that the agent uses to process requests. The value for DefaultAgentName is used for requests on an IP address or interface when no agent name value exists in the AgentName parameter.

If you are using virtual servers, you can set up your SiteMinder environment quickly by using a DefaultAgentName. Using DefaultAgentName means that you do not need to define a separate agent for each virtual server.

Important! If you do not specify a value for the DefaultAgentName parameter, then the value of the AgentName parameter requires every agent identity in its list. Otherwise, the Policy Server cannot tie policies to the agent.

Default: No default.

Limit: Multiple values are allowed.

Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. The value is not case-sensitive. For example, the names MyAgent and myagent are treated the same.

Agent Configuration Parameters Required by All Agents

All Agents *must* have a value set for the following parameter:

DefaultAgentName

Defines a name that the agent uses to process requests. The value for DefaultAgentName is used for requests on an IP address or interface when no agent name value exists in the AgentName parameter.

If you are using virtual servers, you can set up your SiteMinder environment quickly by using a DefaultAgentName. Using DefaultAgentName means that you do not need to define a separate agent for each virtual server.

Important! If you do not specify a value for the DefaultAgentName parameter, then the value of the AgentName parameter requires every agent identity in its list. Otherwise, the Policy Server cannot tie policies to the agent.

Default: No default.

Limit: Multiple values are allowed.

Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. The value is not case-sensitive. For example, the names MyAgent and myagent are treated the same.

The value of the previous parameter entry must exactly match the name of an Agent object that you defined in the Administrative UI.

Agent Configuration Parameters Required for Domino Web Agents

In addition to the parameters required by all Agents, Domino Web Agents must also have values set for the following parameters:

DominoDefaultUser

Specifies the name by which the Domino Web Agent identifies the users that SiteMinder has previously authenticated against another directory to the Domino server.

Important! This parameter must be encrypted if it is stored in a local configuration file. Use the encryptkey tool to encrypt this parameter. Do not change it by editing the local configuration file directly.

Default: **No default**

DominoSuperUser

Identifies a user who has access to all resources on the Domino server. Helps ensure that all users successfully logged in to SiteMinder are also logged in to the Domino server as the Domino SuperUser.

This value can be encrypted.

This parameter affects the following parameters:

- SkipDominoAuth

Default: No default

More information:

Run the Configuration Wizard for a Domino Web Agent on Windows (see page 95)

How to Verify that your Windows Operating Environment Meets the Prerequisites for Password Services

If you want to use the password services feature of SiteMinder, use the following process to verify that your operating environment meets the prerequisites:

1. Review the password services forms and directories created during the Web Agent installation (see page 24).
2. Repair the CLASSPATH used by the ServletExec application for JSP password services (see page 24).

Repair ServletExec's CLASSPATH for JSP Password Services (Windows)

If you install JSP-based Password Services on a Windows system and get an error message that a servlet is not found when you access an existing servlet or Password Services .jsp, verify that the ServletExec classpath is correct.

If your classpath appears correct and the error still occurs, you may need to repair your classpath.pref file.

To repair the ServletExec classpath

1. Use the ServletExec Administrative Interface to define the Classpath for the Java Virtual Machine. For more information, see the ServletExec documentation.

   Note: You can access the ServletExec documentation on the New Atlanta Web site.

2. Restart the Sun Java System web server or IIS Admin services. This forces ServletExec to write the classpath.pref.

Password Services and Forms Directories

When you install a Web Agent for the first time, the installation program creates the following folders in the Web Agent home directory:

- jpw_default and jpw (for Password Services)
- pw_default and pw (for Password Services)
- samples_default and samples (for standard forms)

The jpw, pw, and samples directories are the working directories that include templates and forms that you customize. The "default" versions are backup directories for the original documents.

Chapter 2: Install a Web Agent on a Windows System

This section contains the following topics:

Run a GUI Mode Installation on Windows

To install an Agent, you need to be logged into the computer which runs the web server.

1. Exit all applications that are running and stop the web server.
2. Download the installation file from Technical Support.
3. Navigate to the win folder then run the executable file for your operating system:

   ca-wa-*version*-win*processor_type*.exe

   The installation program prepares the files.
4. Review the information in the Introduction dialog box, then click Next.
5. Read the License Agreement then select the radio button to accept the agreement. Click Next.

   If you do not accept the agreement, the installation terminates.
6. Read the notes in the Important Information dialog box, then click Next.
7. In the Choose Install Folder dialog box, accept the default location or use the Choose button to select a different location. Click Next.

   If you select a non-default location then want to revert to the default directory, click Restore Default Folder.
8. Select the placement of the Agent Configuration Wizard shortcut in the Choose Shortcut Folder dialog box then click Next.

   To allow all users access to the Configuration Wizard, ensure the Create Icons for All Users check box is selected. Otherwise, clear this option.
9. Review the information in the Pre-Installation Summary dialog box, then click Install.

   Note: The installation program may detect that newer versions of certain system dlls are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The Web Agent files are copied to the specified location. Afterward, the Web Agent Configuration dialog box is displayed.
10. Choose one of the following options:
    - Yes. I would like to configure the Agent now.
    - No. I will configure the Agent later.

    If the installation program detects that there are locked Agent files, it will prompt you to restart your system instead of reconfiguring it. Select whether to restart the system automatically or later on your own.
11. If you choose not to configure the Agent, the Install Complete dialog box displays, and prompts you to reboot the system.
12. Click Done.

If you selected the option to configure the Agent automatically, the installation program prepares the Web Agent Configuration Wizard and begins the trusted host registration and configuration processes.

Do the following:

- Register the trusted host. You can do this before or after configuring an Agent, but the Agent will *not* be able to communicate properly with the Policy Server unless the trusted host is registered.
- Configure the Web Agent.

Installation Notes:

- After installation, you can review the installation log file in *web_agent_home*\install_config_info. The file name is: CA_SiteMinder_Web_Agent_*version*_InstallLog.log

  web_agent_home

  Indicates the directory where the SiteMinder Agent is installed.

  Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

  Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

  Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

  Default (UNIX/Linux installations): /opt/ca/webagent

- You may choose not to start the Web Agent Configuration Wizard immediately after installation—you may have to reboot your machine after installation. If so, you can start the Wizard manually when you are ready to configure an Agent.

More Information

Register Your System as a Trusted Host on UNIX (see page 54)
Configure an Oracle iPlanet Web Agent (see page 73)
Configure an Apache Web Agent (see page 83)
Configure a Domino Web Agent (see page 93)

Unattended Installations on Windows

After you have installed the Web Agent on one system, you can automate installations on other web servers using the Agent's unattended installation feature. An unattended installation lets you install or uninstall the Web Agent without any user interaction.

An unattended installation uses a properties file that is initially configured with values from the initial GUI or console mode Web Agent installation. Therefore, you can only run an unattended installation on a system with the same platform and web server image as the system where you first installed the Web Agent. For example, if you install an Agent on a Windows system with an Oracle iPlanet web server first, you *cannot* use the properties file to run an unattended installation on a UNIX system with an Apache web server.

Prepare an Unattended Installation on Windows

Unattended installation uses the ca-wa-installer.properties file to propagate the Web Agent installation set up to all Agents in your network. In this properties file, you define installation parameters, then copy the file and the Web Agent executable file to any web server in your network to run an unattended installation.

The ca-wa-installer.properties file is installed in the following location:
web_agent_home\install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation.

To prepare for an unattended installation

1. Run an initial installation of the Web Agent.
2. Open the ca-wa-installer.properties file and modify the parameters in the file. The parameters are as follows:
   - USER_INSTALL_DIR--Specifies the installed location of the Web Agent. Enter the full path to the installation directory.
   - USER_SHORTCUTS--Specifies where the Web Agent Configuration Wizard shortcut should be installed. Enter the path to the desired location. (Windows only)
   - USER_REQUESTED_RESTART--Indicates whether the installation program should reboot a Windows machine if required. Set to YES to allow the reboot. (Windows only)
3. Save the file.

Run an Unattended Installation on Windows

You should have completed an initial Web Agent installation and, if necessary, modified the ca-wa-installer.properties file. Now, you can use the file to run subsequent Web Agent installations.

To run an unattended Web Agent installation

1. From a system where the Web Agent is already installed, copy the following files to a local directory:
   a. ca-wa-*version*-win32.exe (Agent executable) from where it resides on your system.
   b. ca-wa-installer.properties file from *web_agent_home*\install_config_info
2. Open a command window and navigate to the directory where you copied the files.

   Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.
3. Run the installation executable with the -f and - i silent options, as shown in the following example:

   agent_executable -f *properties_file* -i silent

   Assuming that you run the installation from the directory where the executable and properties file are located, the command would be:

   ca-wa-<*version*>-win32.exe -f ca-wa-installer.properties -i silent

   Note: If you are not at the directory where these files reside, you must specify the full path to each file. If there are spaces in the directory paths, enclose the entire path between quotation marks.

   When the installation is complete, you return to the command prompt.
4. Check to see if the installation completed successfully by looking in the CA_SiteMinder_Web_Agent _*version*_InstallLog.log file, located in the *web_agent_home*\install_config_info directory. This log file contains the results of the installation.
5. Register the trusted host and configure the Web Agent.

More Information

How to Configure Any Web Agent in Unattended Mode (see page 103)

How to Stop an Unattended Installation in Progress on Windows

To manually stop an unattended installation on Windows systems, use the following process:

1. Open the Windows Task Manager.
2. Stop the following processes:
   - ca-wa-*version*-win.exe
   - wa_install.exe

Reinstall the Web Agent on Windows

You can reinstall a Web Agent to restore missing application files. For this procedure, you do not need to uninstall the existing Web Agent; simply perform a reinstall over the existing Web Agent files by repeating the installation procedure.

To reinstall the Web Agent on Windows, use the following process:

1. Make back up copies of the following:
   - Your Windows registry settings.
   - Your Web Agent configuration settings.
2. Install the Web Agent on your Windows system using the GUI installer.

More Information

Run a GUI Mode Installation on Windows (see page 26)

Installation History Log File

The installer creates a log file with following information:

- The product name
- The installed location
- The complete (full) version number

This file is created in the following location:

Windows

C:\Program Files\CA\install-info\ca-install-history.log

UNIX

/opt/ca/install-info/ca-install-history.log

More information:

Installation and Configuration Log Files (see page 35)

Register Your System as a Trusted Host on Windows

A *trusted host* is a client computer where one or more SiteMinder Web Agents can be installed.

To establish a connection between the Web Agent and the Policy Server, you need to register the web server by creating a trusted host object on the Policy Server. The web server requires a corresponding trusted host object on the Policy Server before the Web Agent can operate.

Note: You only register the host once, *not* each time you install and configure a Web Agent on your system.

To register a trusted host

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

   Note: If you chose to configure the Web Agent immediately after the installation, SiteMinder automatically starts the Configuration Wizard.

2. In the Host Registration dialog box:

   a. Select Yes to register a host now or No to register the host at a later time.

   b. Click Next.

3. In the Admin Registration dialog box, complete the following fields to identify an administrator with the rights to register a trusted host, then click Next:

   - Admin User Name—enter the name of the administrator allowed to register the host with the Policy Server.

     This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.

   - Admin Password—enter the administrator's password.

   - Confirm Admin Password—re-enter the password.

   - Enabled Shared Secret Rollover—check this box to periodically change the shared secret used to encrypt communication between the trusted host and the Policy Server. Key rollover must be enabled at the Policy Server for this feature to work.

     To disable shared secret rollover or enable it at a later time, you have to re-register the trusted host, or use the Policy Management API in the C and Perl Scripting Interface to enable or disable shared secret rollover.

4. In the Trusted Host Name and Configuration Object dialog box, enter values for the two fields then click Next.

a. In the Trusted Host Name field, enter a unique name that represents the trusted host to the Policy Server. This name *does not* have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

Note: This name must be unique among trusted hosts and not match the name of any other Web Agent.

b. In the Host Configuration Object field, enter the name of the Host Configuration Object specified in the Policy Server, then click Next.

This object defines the connection between the trusted host and the Policy Server. For example, to use the default, enter DefaultHostSettings. In most cases, you will have created your own Host Configuration Object.

Note: The entry you specify must match the Host Configuration Object entry set at the Policy Server.

5. In the Policy Server IP Address dialog box:

a. Enter the IP address, or host name, and the authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

You can specify a non-default port number, but if your Policy Server is configured to use a non-default port and you omit it when you register a trusted host, SiteMinder displays the following error:

Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1)

Note also that if you specify a non-default port, that port is used for the Policy Server's authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port. The entry in the SmHost.conf file will look like:

policyserver="*ip_address*,5555,5555,5555"

b. Click Add.

You can add more than one Policy Sever; however, for host registration, only the first server in the list will be used.

If multiple Policy Servers are specified, the Agent uses them as bootstrap servers. When the Agent starts up, the Web Agent has several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap Policy Server is no longer used by that server process. The Host Configuration Object can contain another set of servers, which may or may not include any of the bootstrap servers.

c. Click Next.

6. If you want to use FIPS encryption, choose one of the following options:

FIPS Compatibility Mode (Default)

Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.

FIPS Migration Mode

Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.

FIPS Only Mode

Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using only FIPS 140-2 algorithms.

Important! A SiteMinder installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the corresponding versions of the respective SDKs to achieve the required support for Full FIPS mode.

If you do *not* want to use FIPS encryption, accept the default.

7. Click Next.
8. Accept the default location of the host configuration file, SmHost.conf or click Choose to select a different location. Click Next.

   If you select a non-default location then want to revert to the default directory, click Restore Default Folder.

   The host is registered and a host configuration file, SmHost.conf, is created in *web_agent_home*/config. You can modify this file.

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed.

   Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

   Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

   Default (UNIX/Linux installations): /opt/ca/webagent

9. Click Continue.

The Trusted Host is registered.:

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the Web Agent, check the following log files, located in *web_agent_home*\install_config_info:

ca-wa-details.log

Provides specific details on any failures or problems that may have occurred.

CA_SiteMinder_Web_Agent_*version*_InstallLog.log

Provides complete results of the installation, including the components that installed successfully and those that failed.

More information:

Installation History Log File (see page 30)

Modify the SmHost.conf File (Windows)

Web Agents and custom Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

To modify the SmHost.conf file

1. Navigate to the *web_agent_home*\config directory.
2. Open the SmHost.conf file in a text editor.
3. Enter new values for the any of the following settings that you want to change:

   Important! Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

   hostconfigobject

   Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

   If you want to change the host configuration object an object so the Web Agent u, you need to modify this setting.

   Example: hostconfigobject="*host_configuration_object*"

   policyserver

   Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

   "*IP_address*, *port*,*port*,*port*"

   The default ports are 44441,44442,44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

   To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

   Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

Important: If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Web Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

Default: *IP_address*, 44441,44442,44443

Example (Syntax for a single entry)**:** "*IP_address*, *port*,*port*,*port*"

Example (Syntax for multiple entries, place each Policy Server on a separate line)**:**
policyserver="123.122.1.1, 44441,44442,44443"
policyserver="111.222.2.2, 44441,44442,44443"
policyserver="321.123.1.1, 44441,44442,44443"

requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.

   The changes to the SmHost.conf file are applied.

Re-register a Trusted Host Using the Registration Tool (Windows)

When you install a Web Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the *web_agent_home*\bin directory when you install a Web Agent.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

Follow these steps:

1. Open a command prompt window.
2. Enter the smreghost command using the following required arguments:

```
smreghost -i policy_server_IP_address:[port]
-u administrator_username -p Administrator_password
-hn hostname_for_registration -hc host_configuration_ object
```

Note: Separate each command argument from its value with a space. Surround any values that contain spaces with double quotes ("). See the following

examples:

```
smreghost -i 192.168.2.1:44441,44442,44443 -u SiteMinder -p mypw -hn "host
computer A"
-hc DefaultHostSettings
```

The following example contains the -o argument:

```
smreghost -i 192.168.2.1:44441,44442,44443 -u SiteMinder -p mypw -hn "host
computer A"
-hc DefaultHostSettings -o
```

The following arguments are used with the smreghost command:

-i *policy_server_IP_ address:port*

Indicates the IP address of the Policy Server where you are registering this host. Specify the port of the authentication server only if you are *not* using the default port.

If you specify a port number, which can be a non-default port, that port is used for all three Policy Server processes (authentication, authorization, accounting). The Policy Server responds to any Agent request on any port.

Use a colon between the IP address and non-default port number, as shown in the following examples.

Default: (ports) 44441,44442,44443

Example: (IPv4 non-default port of 55555) -i 127.0.0.1:55555

Example: (IPv4 default ports) -i 127.0.0.1

Example: (IPv6 non-default port of 55555) -i [2001:DB8::/32][:55555]

-u *administrator_username*

Indicates the name of the SiteMinder administrator with the rights to register a trusted host.

-p *Administrator_password*

Indicates the password of the Administrator who is allowed to register a trusted host.

-hn *hostname_for_registration*

Indicates the name of the host to be registered. This can be any name that identifies the host, but it must be unique. After registration, this name is placed in the Trusted Host list in the Administrative UI.

-hc *host_config_object*

Indicates the name of the Host Configuration Object configured at the Policy Server. This object must exist on the Policy Server before you can register a trusted host.

-sh *shared_secret*

Specifies the shared secret for the agent, which is stored in the SmHost.conf file on the local web server. This argument changes the shared secret on only the local web server. The Policy Server is not contacted.

-rs

Specifies whether the shared secret will be updated (rolled over) automatically by the Policy server. This argument instructs the Policy Server to update the shared secret.

-f *path_to_host_config_file*

(Optional) Indicates the full path to the file that contains the registration data. The default file is SmHost.conf. If you do not specify a path, the file is installed in the location where you are running the smreghost tool.

If you use the same name as an existing host configuration file, the tool backs up the original and adds a .bk extension to the backup file name.

-cf *FIPS mode*

Specifies one of the following FIPS modes:

- COMPAT--Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.

- MIGRATE--Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.
- ONLY--Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using *only* FIPS 140-2 algorithms.

Important! A SiteMinder installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the corresponding versions of the respective SDKs to achieve the required support for Full FIPS mode.

If this switch is not used, or you use the switch without specifying a mode, the default setting is used.

Default: COMPAT

Note: More information on the FIPS Certified Module and the algorithms being used; the data that is being protected; and the SiteMinder Cryptographic Boundary exists in the *Policy Server Administration Guide*.

-o

Overwrites an existing trusted host. If you do *not* use this argument, you will have to delete the existing trusted host with the Administrative UI before using the smreghost command. We recommend using the smreghost command with this argument.

The trusted host is re-registered.

Register Multiple Trusted Hosts on One System (Windows)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SiteMinder client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.

To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server's SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

  Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

  Note: If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the smreghost command-line tool: Run the smreghost tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.

  Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

Chapter 3: Install a Web Agent on a UNIX System

This section contains the following topics:

Install the Web Agent Documentation on UNIX Systems

You install the Web Agent documentation independently from the Web Agent—it is not installed by default. We recommend that you install the documentation *before* installing the Web Agent so you can specify the install location.

Note: If you plan to install the Web Agent documentation on the same system as existing Policy Server documentation, the installation puts the Agent manuals in the same location as the Policy Server documents, for example, *policy_server_home*/ca_documents. You will not be prompted to specify a location.

To install the documentation

1. Download the documentation installation programs from Technical Support, and then navigate to the directory for your operating system.
2. Copy the appropriate installation file for your operating system to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:

   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
   - nete-wa-doc-*version*-linux.bin (linux 2.1)
3. Open a console window, and check the permissions on the binary file. You may need to add execute to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system*.bin
4. From a console window, run the documentation installation using one of the following commands:

   GUI mode:

   ./ca-wa-doc-*version-operating_system*.bin

   Console mode:

   ./ca-wa-doc-*version-operating_system*.bin -i console

   The documentation installation starts.
5. Read the License Agreement, pressing Enter to page through the entire document. If you agree with the terms, enter Y to continue the installation.
6. Review the Important Instructions, then click Next.
7. Specify the installation directory.

   The installation program installs the r12.0 SP3 Web Agent documentation in the directory you specified.

Install the Web Agent on a UNIX System

There are several types of Web Agent installations on a UNIX system:

Note: Installing a Web Agent on a 64-bit Suse Linux 10 system requires additional preparations.

- Installing from a graphical user interface
- Installing from a console window responding to command-line prompts
- Installing installation file, unattended by an administrator and requiring no user interaction.

Select the installation method that best suits your environment.

Note the following:

- The Web Agent installation adds and modifies a few system environment variables.
- In console mode, when the installation program prompts with a question, the default entry is displayed in brackets **[]**. Press ENTER to accept the default.
- In these procedures, *web_agent_home* refers to the installed location of the SiteMinder Web Agent.
- After installation, you can find the installation log file in *web_agent_home*. The file name is:

  CA_SiteMinder_Web_Agent_*version*_InstallLog.log

More Information

Miscellaneous Web Server Preparations (see page 18)
Environment Variables Added or Modified by the Web Agent Installation (see page 161)

Run a GUI Mode Installation on UNIX

To install an Agent, you must be logged into the account where the web server is installed.

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

To run a GUI mode installation on UNIX:

1. Consider the following before you begin:
   - Running a Web Agent GUI-mode installation or running the Configuration Wizard using the Exceed application may cause text in the dialog boxes to be truncated because of unavailable fonts. This limitation has no affect on Web Agent installation and configuration.
   - If you are installing the Web Agent via telnet or other terminal emulation software, you must have an X-Windows session running in the background to run the GUI mode installation. Additionally, you need to set the DISPLAY variable to your terminal, as follows:

     DISPLAY=111.11.1.12:0.0

     export DISPLAY

     If you try to run in GUI mode through a telnet window without an X-Windows session, the installer throws an Java exception and exits.
   - You can also run a command-line installation from a console window.
2. Exit all applications that are running.
3. Ensure that the /tmp directory has at least 300MB of disk space available.
4. Download the installation file from Technical Support.
5. Navigate to the directory for your operating system.
6. Copy the appropriate binary file to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:
   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
7. Depending on your permissions, you may need to add executable permissions to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system-processor-architecture*.bin
8. Open a console window and from the local installation directory enter:

   ./ca-wa-*version-operating_system-processor-architecture*.bin

   The installation program prepares the files.

9. In the Introduction dialog box, read the information then click Next.
10. Read the License Agreement then select the radio button to accept the agreement. Click Next.

    If you do not accept the agreement, the installation terminates.
11. Read the notes in the Important Information dialog box, then click Next.
12. In the Choose Install Location dialog box, accept the default location or use the Choose button to select a different location. Click Next.

    If you select a non-default location then want to revert to the default directory, click Restore Default Folder.
13. Review the information in the Pre-Installation Summary dialog box, then click Install.

    The Web Agent files are installed in the specified location.
14. In the Install Complete dialog box, click Done.
15. After installing the Agent, run the Agent Configuration Wizard to register a trusted host and configure the Web Agent.

More information:

Configurations Available for All Web Agents (see page 103)
Register Your System as a Trusted Host on UNIX (see page 54)

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the Web Agent, check the following log files, located in *web_agent_home*\install_config_info:

ca-wa-details.log

Provides specific details on any failures or problems that may have occurred.

CA_SiteMinder_Web_Agent_*version*_InstallLog.log

Provides complete results of the installation, including the components that installed successfully and those that failed.

More information:

Installation History Log File (see page 30)

Run a Console Mode Installation on UNIX

You can install the SiteMinder Web Agent on a UNIX system using the console mode.

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

To run a console mode installation on UNIX

1. Exit all applications that are running and stop the web server.
2. Ensure that the /tmp directory has at least 300MB of disk space available.
3. Download the installation programs from Technical Support.
4. Navigate to the directory for your operating system.
5. Copy the appropriate binary file to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:

   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
6. Open a console window, and check the permissions on the binary file. You may need to add execute permissions to the install file. For example:

   chmod +x ca-wa-*version-operating_system-processor-architecture*.bin
7. At the command prompt, start the console mode installation by entering:

   ./ca-wa-*version-operating_system-processor-architecture*.bin

   -i console

   The -i console command argument enables the installation to be run from the command line.

   The installation prepares the files.
8. Review the Introduction and press Enter to continue.

   The installation prepares the License Agreement.
9. Read the License Agreement, pressing Enter to read through the entire agreement.
10. Enter Y to accept the agreement and continue with the installation.
11. Review the Important Information section for information about the installation and documentation.

    Press Enter to page through the notes and continue through the installation.
12. In the Choose Install Location section, specify the location where the installation should place the Agent files. To accept the default location, press Enter.

If you specify a path, it must contain the word "webagent." If it does not, the installation program will create this folder and append it to the path. For example, if you specify export/ca/wa, the path becomes export/ca/wa/webagent. However, if you specify export/ca/sm_webagent as the path, the installation program will accept this.

13. Review the information in the Pre-Installation Summary, then press Enter to continue. The program begins installing files.
14. When the installation is complete, you will receive a message along with instructions on locating the Configuration Wizard.
15. Press Enter to exit the installer.
16. After installing the Agent, run the Agent Configuration Wizard to register a trusted host and configure the Web Agent.

More information:

Configurations Available for All Web Agents (see page 103)

Unattended Installations on UNIX

After you have installed the Web Agent on one system, you can automate installations on other web servers using the Agent's unattended installation feature. An unattended installation lets you install or uninstall the Web Agent without any user interaction.

An unattended installation uses a properties file that is initially configured with values from the initial GUI or console mode Web Agent installation. Therefore, you can only run an unattended installation on a system with the same platform and web server image as the system where you first installed the Web Agent. For example, you *cannot* install an Agent on a Solaris system with an Oracle iPlanet and then use the properties file to run an unattended installation on a Linux system with an Apache web server.

Prepare an Unattended Installation on UNIX

Unattended installation uses the ca-wa-installer.properties file to propagate the Web Agent installation set up to all Agents in your network. In this properties file, you define installation parameters, then copy the file and the Web Agent executable file to any web server in your network to run an unattended installation.

The ca-wa-installer.properties file is installed in the following location:

web_agent_home/install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation.

To install the ca-wa-installer.properties file

1. Run an initial installation of the Web Agent.
2. Open the ca-wa-installer.properties file and modify the parameters.

   The parameters are as follows:

Parameter	Meaning
USER_SHORTCUTS	Specifies where the Web Agent configuration shortcut should be installed. Enter the path to the desired location. (Windows only)
USER_INSTALL_DIR	Specifies the installed location of the Web Agent. Enter the full path to the installation directory.
USER_REQUESTED_RESTART	Indicates whether the installation program should reboot a Windows machine if required. Set to YES to allow the reboot. (Windows only)

3. Save the file.

Run an Unattended Installation on UNIX

You should have completed an initial Web Agent installation and, if necessary, modified the ca-wa-installer.properties file. Now, you can use the file to run subsequent Web Agent installations.

To run an unattended Web Agent installation

1. From a system where the Web Agent is already installed, copy the following files to a local directory:
   a. ca-wa-*version-operating_system*.bin (Agent executable) from where it resides on your system.
   b. Copy the ca-wa-installer.properties file from *web_agent_home*/install_config_info.
2. Open a console window and navigate to the directory where you copied the two files.
3. Run the installation executable with the -f and - i silent options, as follows:

   agent_binary -f *properties_file* -i silent

   Note: If you are not at the directory where these files reside, you must specify the full path to each file.

   Assuming that you run the installation from the directory where the executable and properties file are located, the command would be:

   ./ca-wa-*version-operating_system*.bin -f ca-wa-installer.properties -i silent

   When the installation is complete, you return to the command prompt.
4. CA_SiteMinder_Web_Agent _*version*_InstallLog.log file, located in the *web_agent_home*/install_config_info directory. This log file contains the results of the installation.
5. Register the trusted host and configure the Web Agent.

More Information

How to Configure Any Web Agent in Unattended Mode (see page 103)

Stop an Unattended Installation in Progress on UNIX

To manually stop the installation, press Ctrl + C.

Set the Web Agent Environment Variables After Installation

You can set the Web Agent environment variables after installing the Web Agent using the ca_wa_env.sh script Running the script for Web Agents installed on most UNIX platforms ensures that the Web Agent and web server can work together. The script sets environment variables required by the Web Agent.

The ca_wa_env.sh script has been enhanced to set the following environment variables:

- NETE_WA_ROOT
- PATH
- NETE_WA_PATH
- LD_LIBRARY_PATH

  Note: The Web Agent requires that LD_LIBRARY_PATH include /usr/lib before any other directory containing older versions of libm.so.
- SHLIB_PATH
- LIBPATH

To set the Web Agent environment variables after installation, source the following script after you install and configure the Web Agent:

```
. ./ca_wa_env.sh
```

You can list the script in either the user .profile file or envvars file. You must source this script if you are upgrading a Web Agent from v6.x QMR 1.

Note: You do not have to run this script for Oracle iPlanet web servers because this file as been added to the start script.

Set Web Agent Variables when using apachectl Script

You run your Apache server using the apachectl script (such as when running an Apache web server on POSIX). Adding a line to the apachectl script sets the environment variables for the agent.

Follow these steps:

1. Locate a line resembling the following example:

   ```
   # Source /etc/sysconfig/httpd for $HTTPD setting, etc
   ```

2. Add the following line *after* the line in the previous example:

   ```
   sh /web_agent_home/ca_wa_env.sh
   ```

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed.

   Default (UNIX/Linux installations): /opt/ca/webagent

Installation History Log File

The installer creates a log file with following information:

- The product name
- The installed location
- The complete (full) version number

This file is created in the following location:

Windows

C:\Program Files\CA\install-info\ca-install-history.log

UNIX

/opt/ca/install-info/ca-install-history.log

More information:

Installation and Configuration Log Files (see page 35)

Reinstall a Web Agent on UNIX

You can reinstall a Web Agent to restore missing application files. For this procedure, you do not need to uninstall the existing Web Agent; simply perform a reinstall over the existing Web Agent files by repeating the installation procedure.

To reinstall the Web Agent on UNIX, use the following process:

1. Make copies of your Web Agent configuration settings to have as a back up.
2. Install the Web Agent on your UNIX system using the GUI installer.

   During the reinstallation, you must confirm the reinstall by one of the following:

   - A Reinstall dialog box (GUI mode)
   - A Confirm Upgrade/Reinstall prompt (Console mode)

Register Your System as a Trusted Host on UNIX

A *trusted host* is a client computer where one or more SiteMinder Web Agents can be installed. The term trusted host refers to the physical system.

To establish a connection between the trusted host and the Policy Server, you need to register the host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. After this file is successfully created, the client computer becomes a trusted host.

Note: You only register the host once, *not* each time you install and configure a Web Agent on your system.

You can register the trusted host immediately after installing the Web Agent or at a later time; however, you must perform the registration at some point.

You can run the Registration Tool independently from GUI or Console mode.

More Information

How to Configure Any Web Agent in Unattended Mode (see page 103)

Register a Trusted Host in GUI or Console Mode

These instructions are for GUI and Console Mode registration. The steps for the two modes are the same, with the following exceptions for Console mode:

- You may be instructed to select an option by entering a corresponding number for that option.
- You press Enter after each step to proceed through the process. The prompts should guide you through the process.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

To register a host

1. If necessary, start the Configuration Wizard as follows:
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI Mode: ./ca-wa-config.bin

      Console Mode: ./ca-wa-config.bin -i console

   The Configuration Wizard starts.
2. In the Host Registration dialog box:
   a. Select Yes to register a host now or No to register the host at a later time.
   b. If you are using PKCS11 cryptographic hardware in your SiteMinder environment, select the check box.
   c. Click Next.
3. If you enabled cryptographic hardware, complete the fields. If not, skip to the next step.
   a. In the PKCS11 DLL field, enter the full path to the PKCS11 DLL. Click on Choose to search for the DLL.
   b. Optionally, specify the token label in the Token Label and Token Passphrase, if applicable. Re-confirm the passphrase in the Confirm token passphrase field then click Next.
4. Complete the following fields in the Admin Registration dialog box, then click Next:
   - Admin User Name—enter the name of the administrator allowed to register the host with the Policy Server.

     This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.
   - Admin Password—enter the administrator's password.

- Confirm Admin Password—re-enter the password.
- Enabled Shared Secret Rollover—check this box to periodically change the shared secret used to encrypt communication between the trusted host and the Policy Server. Key rollover must be enabled at the Policy Server for this feature to work.

  Important: If you enable shared secret rollover, the user who owns the web server process must have permissions to write to the SmHost.conf file. If this file cannot be modified by this user, then the shared secret rollover cannot be updated.

  For example, for Oracle iPlanet and Apache web servers, the person specified by the User directive needs write permission to the SmHost.conf file. If the SmHost.conf file is owned by User1 and no other user has write permissions, the shared secret rollover is not written to the SmHost.conf file if User2 owns the server process.

5. In the Trusted Host Name and Configuration Object dialog box, enter values for the two fields then click Next.

   a. In the Trusted Host Name field, enter a unique name that represents the trusted host to the Policy Server. This name *does not* have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

      Note: This name must be unique among trusted hosts and not match the name of any 4.x Web Agent. It can be the same name as a 5.0 Web Agent, but this is not recommended.

   b. In the Host Configuration Object field, enter the name of the Host Configuration Object specified in the Policy Server, then click Next.

      This object defines the connection between the trusted host and the Policy Server. To use the default, enter DefaultHostSettings. In most cases, you will use your own Host Configuration Object.

      Note: The entry you specify must match the Host Configuration Object entry set at the Policy Server.

6. In the Policy Server IP Address dialog box:

   a. Enter the IP address, or host name, and the authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

      You can specify a non-default port number, but if you are using a nondefault port and you omit it, SiteMinder displays the following error:

      Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1))

      Note also that if you specify a non-default port, that port is used for the Policy Server's authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port. The entry in the SmHost.conf file will resemble:

policyserver="*ip_address*,5555,5555,5555"

b. Click Add.

You can add more than one Policy Sever; however, for host registration, only the first server in the list will be used. If you add multiple entries, separate them by a comma.

If multiple Policy Servers are specified, the Agent uses them as bootstrap servers. When the Agent starts up, the Web Agent has several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap Policy Server is no longer used by that server process. The Host Configuration Object can contain another set of servers, which may or may not include any of the bootstrap servers.

c. Click Next.

7. If you want to use FIPS encryption, choose one of the following options:

FIPS Compatibility Mode (Default)

Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.

FIPS Migration Mode

Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.

FIPS Only Mode

Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using only FIPS 140-2 algorithms.

Important! A SiteMinder installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the corresponding versions of the respective SDKs to achieve the required support for Full FIPS mode.

If you are not using FIPS encryption, use the default value.

8. Click Next.

9. Accept the default location of the host configuration file, SmHost.conf or click Choose to select a different location. Click Next.

If you select a non-default location then want to revert to the default directory, click Restore Default Folder.

The host is registered and a host configuration file, SmHost.conf, is created in *web_agent_home*/config. You can modify this file.

10. Configure your Web Agent.

Modify the SmHost.conf File (UNIX)

Web Agents and custom Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

To modify the SmHost.conf file

1. Navigate to the *web_agent_home*/config directory.
2. Open the SmHost.conf file in a text editor.
3. Enter new values for the any of the following settings that you want to change:

   Important! Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

   hostconfigobject

   Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

   If you want to change the host configuration object an object so the Web Agent u, you need to modify this setting.

   Example: hostconfigobject="*host_configuration_object*"

   policyserver

   Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

   "*IP_address*, *port*,*port*,*port*"

   The default ports are 44441,44442,44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

   To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

   Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

Important: If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Web Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

Default: *IP_address*, 44441,44442,44443

Example (Syntax for a single entry)**:** "*IP_address*, *port*,*port*,*port*"

Example (Syntax for multiple entries, place each Policy Server on a separate line)**:**
policyserver="123.122.1.1, 44441,44442,44443"
policyserver="111.222.2.2, 44441,44442,44443"
policyserver="321.123.1.1, 44441,44442,44443"

requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.

   The changes to the SmHost.conf file are applied.

Re-register a Trusted Host Using the Registration Tool (UNIX)

When you install a Web Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the *web_agent_home*/bin directory when you install a Web Agent.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

Follow these steps:

1. Open a command prompt window.
2. Ensure that the library path environment variable contains the path to the Web Agent's bin directory.
3. Enter the following two commands:

   library_path_variable=${*library_path_variable*}:*web_agent_home*/bin

   export *library_path_variable*

   For example, for Solaris systems enter the following two commands:

LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/ca/webagent/bin

export LD_LIBRARY_PATH

The following list shows the different variables for each operating system:

Solaris

LD_LIBRARY_PATH

HP-UX

SHLIB_PATH

LINUX

LD_LIBRARY_PATH

AIX

LIBPATH

4. Enter the smreghost command using the following required arguments, as shown in the following example:

   smreghost -i *policy_server_IP_address:[port]*

   -u *administrator_username* -p *Administrator_password*

   -hn *hostname_for_registration* -hc *host_configuration_ object*

   Note: Separate each command argument from its value with a space. Surround any values that contain spaces with double quotes ("). See the following example:

   ```
   smreghost -i 192.168.2.1:55555 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings
   ```

   Example with the -o argument:

   ```
   smreghost -i 192.168.2.1:55555 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings -o
   ```

   The following arguments are used with the smreghost command:

   -i *policy_server_IP_ address:port*

   Indicates the IP address of the Policy Server where you are registering this host. Specify the port of the authentication server only if you are *not* using the default port.

   If you specify a port number, which can be a non-default port, that port is used for all three Policy Server processes (authentication, authorization, accounting). The Policy Server responds to any Agent request on any port.

   Use a colon between the IP address and non-default port number, as shown in the following examples.

   Default: (ports) 44441,44442,44443

   Example: (IPv4 non-default port of 55555) -i 127.0.0.1:55555

   Example: (IPv4 default ports) -i 127.0.0.1

Example: (IPv6 non-default port of 55555) -i [2001:DB8::/32][:55555]

-u *administrator_username*

Indicates the name of the SiteMinder administrator with the rights to register a trusted host.

-p *Administrator_password*

Indicates the password of the Administrator who is allowed to register a trusted host.

-hn *hostname_for_registration*

Indicates the name of the host to be registered. This can be any name that identifies the host, but it must be unique. After registration, this name is placed in the Trusted Host list in the Administrative UI.

-hc *host_config_object*

Indicates the name of the Host Configuration Object configured at the Policy Server. This object must exist on the Policy Server before you can register a trusted host.

-sh *shared_secret*

Specifies the shared secret for the agent, which is stored in the SmHost.conf file on the local web server. This argument changes the shared secret on only the local web server. The Policy Server is not contacted.

-rs

Specifies whether the shared secret will be updated (rolled over) automatically by the Policy server. This argument instructs the Policy Server to update the shared secret.

-f *path_to_host_config_file*

(Optional) Indicates the full path to the file that contains the registration data. The default file is SmHost.conf. If you do not specify a path, the file is installed in the location where you are running the smreghost tool.

If you use the same name as an existing host configuration file, the tool backs up the original and adds a .bk extension to the backup file name.

-cf *FIPS mode*

Specifies one of the following FIPS modes:

- COMPAT--Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.

- MIGRATE--Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.
- ONLY--Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using *only* FIPS 140-2 algorithms.

Important! A SiteMinder installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the corresponding versions of the respective SDKs to achieve the required support for Full FIPS mode.

If this switch is not used, or you use the switch without specifying a mode, the default setting is used.

Default: COMPAT

Note: More information on the FIPS Certified Module and the algorithms being used; the data that is being protected; and the SiteMinder Cryptographic Boundary exists in the *Policy Server Administration Guide*.

-o

Overwrites an existing trusted host. If you do *not* use this argument, you will have to delete the existing trusted host with the Administrative UI before using the smreghost command. We recommend using the smreghost command with this argument.

The trusted host is re-registered.

Register Multiple Trusted Hosts on One System (UNIX)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SiteMinder client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.

To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server's SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

  Note: If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the smreghost command-line tool: Run the smreghost tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.

Chapter 4: Upgrade a Web Agent to r12.0 SP3

This section contains the following topics:

How to Prepare for a Web Agent Upgrade

You can prepare for upgrading a Web Agent using the following process:

1. Review the upgrade process in the *SiteMinder Upgrade Guide*.
2. Back up any customized files on your web server.
3. Review the Password Services and Form Template changes that occur during the upgrade.
4. Review the changes to the various Web Agent configuration files that occur when you run the Web Agent Configuration wizard *after* an upgrade.
5. Set the LD_PRELOAD variable to avoid conflicts with existing Web Agents.
6. Replace existing read-only files during the upgrade (if prompted).

Review the Upgrade Procedure

Before upgrading a Web Agent, you should review the upgrade process in the *SiteMinder Upgrade* Guide. This guide contains important overview information as well as critical tasks that you should complete *before* upgrading a Web Agent.

Note: If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation.

Back Up Customized Files

Customized files may be overwritten by the upgrade. Back up configured files, such as Agent and Host configuration files *before* upgrading.

Password Services and Forms Template Changes During Upgrades

For Password Services and forms templates, the jpw_default, pw_default, and samples_default directories are upgraded. However the non-default versions of these directories (jpw, pw, and samples), which may contain customized files, will not be modified in any way.

Results of Running the Configuration Wizard After an Upgrade

When you run the Web Agent Configuration Wizard after upgrading the Web Agent, the following occurs:

- SiteMinder saves a copy of the current Web Agent configuration file (WebAgent.conf).
- SiteMinder moves the IgnoreExt and BadURLCharacters lines into the new WebAgent.conf file as commented lines, so that you can easily add your custom elements.

Note: SiteMinder does not save a copy of the Trusted Host configuration file (SmHost.conf).

Ensure LD_PRELOAD Variable Does Not Conflict with Existing Agent

If you are upgrading or reinstalling a Web Agent on a Linux system, from the shell, set the LD_PRELOAD variable so that it points to a different location from any existing Web Agent installation directory. For example, if an existing LD_PRELOAD entry is set to:

LD_PRELOAD=*web_agent_home*/bin/libbtunicode.so

Before you reinstall or upgrade, set the variable to:

export LD_PRELOAD=

This entry sets the variable to a blank value.

Replace Existing Read-only Files

When you upgrade a Web Agent, you may see messages asking whether you want to replace read-only files. Select Yes to all.

Upgrade a Web Agent to r12.0 SP3 on Windows Systems

The executable on the SiteMinder media upgrades your existing SiteMinder Web Agents to r12.0 SP3, provided the web server version has not changed since the last installation of the Web Agent.

If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation. However, you can upgrade if you have applied a hotfix.

Important! Remove any 5.x Web Agent Option Packs before upgrading to r12.0 SP3. 6.x Web Agent Option Packs do not need to be removed before upgrading to r12.0 SP3. For more information about removing and reinstalling Web Agent Option Packs, see the SiteMinder Web Agent Option Pack Guide.

Consider the following:

- If the installation program detects any locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system immediately or later.
- If you are installing an Agent on an Oracle iPlanet web server, you may see an error message stating that the httpd.exe service is unable to locate the smconapi.dll. If this message appears, reboot your system before launching the Web Agent Configuration Wizard.

To upgrade Web Agents on Windows

1. Exit all applications that are running and stop the web server.
2. Download the installation program from Technical Support.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.
3. Navigate to the win32 folder and double-click the ca-wa-*version_number*-win32.exe file.

   The Installation Wizard starts.
4. In the Introduction dialog box, read the information then click Next.
5. Read the License Agreement. Click the radio button to accept the terms of the license agreement, and then click Next.
6. Read the notes in the Important Information dialog box, then click Next.
7. Select the placement of the Agent Configuration Wizard shortcut in the Choose Shortcut Folder dialog box then click Next.

To allow all users access to the Configuration Wizard via the shortcut, select the Create Icons for All Users check box. Otherwise, clear the check box.

The upgrade program locates the existing Web Agent and displays the Confirm Upgrade dialog box.

8. In the Confirm Upgrade dialog box, select one of the following options, and then click Next:
   - Continue with the upgrade—upgrades the Web Agent to r12.0 SP3.
   - Abort the upgrade—exits the upgrade procedure without upgrading the Web Agent.
9. In the Pre-installation Summary dialog box, confirm that the installation settings are correct, then click Install.

   The new Web Agent files are copied to the specified location.

   Note: The installation program may detect that newer versions of certain system .dlls are installed on your system. If you are prompted to overwrite these newer files with older files, click No To All.
10. In the Install Complete dialog box, choose whether to restart your system immediately or later. Then click Done.
11. Re-configure your upgraded web agent with the Web Agent Configuration Wizard.

    Note: You do not need to re-register your trusted host.

    Note: If you have upgraded IIS Web Agent r6, add write permission to the NETWORK SERVICE account for SmHost.conf.

Upgrade a Web Agent to r12.0 SP3 on UNIX Systems

The executable on the SiteMinder media upgrades your existing SiteMinder Web Agents to r12.0 SP3, provided the web server version has not changed since the last installation of the Web Agent.

If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation. However, you can upgrade if you have applied a hotfix.

Important! Remove any 5.x Web Agent Option Packs before upgrading to r12.0 SP3. 6.x Web Agent Option Packs do not need to be removed before upgrading to r12.0 SP3. For more information about removing and reinstalling Web Agent Option Packs, see the SiteMinder Web Agent Option Pack Guide.

To upgrade a Web Agent on UNIX systems

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

1. Exit all applications that are running and stop the web server.
2. Download the installation program from Technical Support.
3. Navigate to the appropriate directory for your operating system.
4. Copy the appropriate binary file to a local directory then navigate to that directory. The file names use the following convention:

   ca-wa-*version-operating_system*.bin
5. Depending on your permissions, you may need to add executable permissions to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system*.bin
6. Open a console window and from the location of the installation program enter:

   ./ca-wa-*version-operating_system*.bin
7. In the Introduction dialog box, read the information then click Next.
8. Read the License Agreement, and then click the radio button to accept the agreement. Click Next.
9. Read the notes in the Important Information dialog box, and then click Next.

   The Confirm Upgrade dialog box is displayed.
10. In the Confirm Upgrade dialog box, select one of the following, and then click Next:
    - Continue with the upgrade—upgrades the Web Agent to r12.0 SP3.

- Abort the installation—exits the upgrade procedure without upgrading the Web Agent.

11. In the Pre-installation Summary dialog box, confirm that the installation settings are correct, then click Install.

    The new Web Agent files are copied to the specified location.

12. In the Install Complete dialog box, click Done.

    The Web Agent upgrade is complete. If the system with the 5.x Web Agent being upgraded has *not* previously been registered as a trusted host, you need to register at the system at some point.

Chapter 5: Configure an Oracle iPlanet Web Agent

This section contains the following topics:

Run the Configuration Wizard on Windows

Note: The SiteMinder Agent Configuration wizard *only* modifies the *default* obj.conf file on the Oracle iPlanet (formerly Sun Java System) web server. To protect other instances or reverse proxy deployments with SiteMinder, copy the SiteMinder settings from the default obj.conf file to any respective *instance_name*-obj.conf files. For example, your web server created an obj.conf file when you installed it, but you later added a server instance named my_server.example.com. To protect resources on my_server.example.com with SiteMinder, copy the SiteMinder settings the wizard added from the obj.conf file to the my_server.example.com-obj.conf file.

To configure the Web Agent on an Oracle iPlanet web server

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

   Note: If you chose to configure the Web Agent immediately after the installation, SiteMinder automatically starts the wizard automatically.

2. If you have already done host registration, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

   To register a trusted host, go to the installation chapter for your platform.

3. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

4. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter iPlanetDefaultSettings.

5. If applicable, select one of the advanced SSL authentication schemes listed in the SSL Authentication dialog box. If the Agent is not providing advanced authentication, select No advanced authentication. Click Next.

   The selections are:

   - HTTP Basic over SSL—identifies a user based on a user name and password. The credential delivery is always done over an encrypted Secure Sockets Layer (SSL) connection.
   - X509 Client Certificate—identifies a user based on X.509 V3 client certificates. Digital certificates act as a signature for a user. Certificate authentication uses SSL communication.
   - X509 Client Cert and HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified **and** he or she must provide a valid user name and password.
   - X509 Client Cert or HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified, or he or she must provide a valid user name and password.
   - X509 Client Cert or Form—The X.509 Client Certificate or HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **or** the user must provide the credentials requested by an HTML form.
   - X509 Client Cert and Form—The X.509 Client Certificate and HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **and** the user must provide the credentials requested by an HTML form.

   Note: For additional information about advanced authentication schemes, see the *Policy Server Configuration* Guide.

6. In the Web Server Configuration Summary dialog box. Confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed and the Configuration Complete dialog box displays.

7. Click Done to exit the Configuration Wizard.

8. Enable the Web Agent:

   a. Open the WebAgent.conf file, located in:

      Sun_Java_System_server_home\servers\https-*hostname*\config

   b. Set the EnableWebAgent parameter to Yes.

   c. Save the file.

9. Apply changes to Oracle iPlanet Web Server files. This is required for the Agent's configuration to take effect.

More Information

Apply SiteMinder Changes to Oracle iPlanet Configuration Files with Oracle iPlanet Administration Server Console for SunOne 6.1 Servers (see page 81)

Configure Oracle iPlanet Web Agents Using GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Oracle iPlanet web server, enter a 3, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

To configure the Web Agent on a Oracle iPlanet Web Server

Note: The SiteMinder Agent Configuration wizard *only* modifies the *default* obj.conf file on the Oracle iPlanet (formerly Sun Java System) web server. To protect other instances or reverse proxy deployments with SiteMinder, copy the SiteMinder settings from the default obj.conf file to any respective *instance_name*-obj.conf files. For example, your web server created an obj.conf file when you installed it, but you later added a server instance named my_server.example.com. To protect resources on my_server.example.com with SiteMinder, copy the SiteMinder settings the wizard added from the obj.conf file to the my_server.example.com-obj.conf file.

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

GUI mode: **.**/ca-wa-config.bin

Console mode: ./ca-wa-config.bin -i console

2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.

3. In the Select Web Server(s) dialog box, select the option for the iPlanet or Sun ONE Web Server and click Next.

4. Specify the root path where the Sun Java System web server is installed and click Next. For example, /opt/iPlanet/servers.

   You can click Choose to locate the root directory.

5. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web server's configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter iPlanetDefaultSettings.

7. If applicable, select one of the advanced SSL authentication schemes listed in the SSL Authentication dialog box. If the Agent is not providing advanced authentication, select No advanced authentication. Click Next following your choice.

   The selections are:

   - HTTP Basic over SSL—identifies a user based on a user name and password. The credential delivery is always done over an encrypted Secure Sockets Layer (SSL) connection.
   - X509 Client Certificate—identifies a user based on X.509 V3 client certificates. Digital certificates act as a signature for a user. Certificate authentication uses SSL communication.
   - X509 Client Cert and HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified **and** he or she must provide a valid user name and password.

- X509 Client Cert or HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified, or he or she must provide a valid user name and password.
- X509 Client Cert or Form—The X.509 Client Certificate or HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **or** the user must provide the credentials requested by an HTML form.
- X509 Client Cert and Form—The X.509 Client Certificate and HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **and** the user must provide the credentials requested by an HTML form.

  Note: For more information, see the Policy Server documentation.

8. In the Web Server Configuration Summary dialog box. Confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed and the Configuration Complete message is displayed.

9. Click Done when the installation is complete.

10. Enable the Web Agent:

    a. Open the WebAgent.conf file, located in

       Sun_Java_System_server/servers/https-*hostname*/config

    b. Set the value of the EnableWebAgent parameter to Yes.

    c. Save the file.

    d. Restart the web server.

11. Apply changes to the Oracle iPlanet Web Server files. This is required for the Agent's configuration to take effect.

More Information

Apply SiteMinder Changes to Oracle iPlanet Configuration Files with Oracle iPlanet Administration Server Console for SunOne 6.1 Servers (see page 81)

Manually Configure Non-Default Server Instances, Virtual Servers, or Reverse Proxies for Oracle iPlanet Web Servers

The SiteMinder Web Agent Configuration wizard only configures the default instance of your Oracle iPlanet web server. To configure a different instance of the Oracle iPlanet web server for SiteMinder, manually edit the obj.conf file that is associated with that server instance. Examples of server instances that need manual configuration include:

- Servers installed in a nondefault directory
- Servers that you want to configure as a reverse proxy. We recommend configuring the reverse proxy using your Oracle iPlanet interface *before* adding the SiteMinder settings to the obj.conf file.

  Note: The SiteMinder Agent Configuration wizard *only* modifies the *default* obj.conf file on the Oracle iPlanet (formerly Sun Java System) web server. To protect other instances or reverse proxy deployments with SiteMinder, copy the SiteMinder settings from the default obj.conf file to any respective *instance_name*-obj.conf files. For example, your web server created an obj.conf file when you installed it, but you later added a server instance named my_server.example.com. To protect resources on my_server.example.com with SiteMinder, copy the SiteMinder settings the wizard added from the obj.conf file to the my_server.example.com-obj.conf file.
- Virtual servers on the same computer

Note: SunOne/Sun Java 7.0 web servers do *not* require these manual configuration steps.

Follow these steps:

1. Locate the directory of the server instance you want to configure.
2. Open the obj.conf file with a text editor.
3. Locate the following line:

   ```
   <Object name="default">
   ```

4. Insert a new line below the previous one, and then add the following text:

   ```
   AuthTrans fn="SiteMinderAgent"
   ```

5. Locate the following line:

   ```
   AuthTrans fn="match-browser" browser="*MSIE*" ssl-unclean-shutdown="true"
   ```

6. Insert a new line below the previous one, and then add the following text:

   ```
   NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi" dir="web_agent_home/pw"
   name="cgi"
   NameTrans fn="pfx2dir" from="/siteminderagent/pw" dir="web_agent_home/pw"
   NameTrans fn="pfx2dir" from="/siteminderagent/jpw" dir="web_agent_home/jpw"
   ```

```
NameTrans fn="pfx2dir" from="/siteminderagent/redirectjsp"
dir="web_agent_home/affwebservices/redirectjsp"
NameTrans fn="pfx2dir" from="/siteminderagent/certoptional"
dir="web_agent_home/samples"
NameTrans fn="pfx2dir" from="/siteminderagent" dir="web_agent_home/samples"
NameTrans fn="pfx2dir" from="/siteminderagent/pwservlet"
dir=web_agent_home/jpw"
```

web_agent_home

Indicates the directory where the SiteMinder agent is installed on your web server.

Default (Windows 32-bit installations only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations only): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64]): C:\Program Files (x86)\webagent\win32

7. Locate the following line:

   ```
   NameTrans fn="ntrans-j2ee" name="j2ee"
   ```

8. Insert a new line below the previous one, and then add the following text:

   ```
   PathCheck fn="SmRequireAuth"
   ```

9. Remove the following line:

   ```
   NameTrans fn="pfx2dir" from="/mc-icons" dir="C:/Program
   Files/Sun/WebServer7.0/lib/icons" name="es-internal"
   ```

10. Locate the following line:

    ```
    ObjectType fn="force-type" type="text/plain"
    ```

11. Insert a new line below the previous one, and then add the following text:

    ```
    Service method="(GET|POST)" fn="SmAdvancedAuth"
    ```

12. Save the obj.conf file.

    The Oracle iPlanet web server is manually configured.

Apply SiteMinder Changes to Oracle iPlanet Configuration Files with Oracle iPlanet Administration Server Console for SunOne 6.1 Servers

The Agent Configuration Wizard modifies the default obj.conf, and mime.types files that the Oracle iPlanet web server uses.

If you are using version 6.1 of a SunOne web server, and you plan to use the Oracle iPlanet Administration console, apply the changes to these files *before* using the console. If you do not apply the changes using the console first, the changes that are made for your SiteMinder configuration could be corrupted. If you lose your configuration, run the configuration program again.

Note: The agent adds settings to the obj.conf file of the Oracle iPlanet web server when the Agent is configured to support an advanced authentication scheme. SiteMinder does *not* remove these settings later. Edit the obj.conf file manually to remove any obsolete settings.

Follow these steps:

1. Log in to the Oracle iPlanet Administration Server console.
2. From the Servers tab, select the web server with the SiteMinder agent installed and click Manage.
3. In the right corner of the dialog, click Apply.

   A warning message about loading the modified configuration files appears.
4. Click Load Configuration Files.
5. Exit the console.
6. Restart the web server.
7. Optimize the Agent for Oracle iPlanet by tuning the shared memory segments.

   The SiteMinder changes are applied.

More Information

Reconfigured Web Agent Won't Operate (see page 134)

Chapter 6: Configure an Apache Web Agent

This section contains the following topics:

Configure an Apache Web Agent on Windows Systems

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

To configure the Apache Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you've placed the Wizard shortcut in a non-default location, the procedure will be different.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.

3. In the Select Web Server(s) dialog box, select the radio button for the Apache Web Server and click Next.

4. In the Apache Web Server Path dialog box, specify the Apache web server root.

   If you installed the Agent on an Apache-based server, such as an IBM HTTP Server, or Oracle server, the Web Agent may not recognize the path. In this case, the Configuration Wizard displays the Apache Web Server Failure dialog box with the following options:

   - I would like to re-enter the Apache Server Root.

     Select this option for an Apache web server and re-enter the root path.

   - I would like to enter a specific configuration path.

     Select this option if you are using an Apache-based web server (such as, IBM HTTP, HP Apache-based, or Oracle). You are prompted to enter the full configuration path to the web server root.

   - I don't have an Apache web server.

     Choose this option to skip Apache configuration and continue with the Agent configuration.

   Click Next.

5. Following the server root path, specify the version of Apache you are using. Select from the following options:

   - Apache version 2.0

6. Select the web server instances that you want to configure with Web Agents.

If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

a. Select one of the following:

   Overwrite—to overwrite the server instance configuration.

   Preserve—to preserve the web servers configuration.

   Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

7. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter ApacheDefaultSettings.

8. In the Web Server Configuration Summary dialog box. Confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed.

9. Click Done when the installation is complete.

10. Enable the Web Agent:

    a. Open the WebAgent.conf file, located as follows:

       Apache_home\conf

       where *Apache_home* is the installed location of the Apache web server.

    b. Set the EnableWebAgent parameter to Yes.

    c. Save and close the file.

11. Restart the web server.

    When you run the Configuration Wizard for the Apache Web Agent, it makes changes to the Web Server's httpd.conf file and to the library path.

    For httpd.conf changes to take effect, you need to restart the web server.

More Information

Configuration Changes to Web Servers with Apache Web Agent (see page 155)
Configure an Apache Web Agent (see page 83)

Configuration Methods for Apache Web Agents on UNIX Systems

The following configuration methods are available for Web Agents on UNIX systems:

- GUI mode
- Console mode
- Unattended mode

Notes:

- For the IBM HTTP web server, HP Apache-based web server, and Oracle HTTP web server, the Apache Web Agent is the Agent you should have installed. All the information for the Apache web server applies to those web servers also.
- Before you configure the Agent, you may want to register the system as a trusted host; however, you can do this at a later time.

More Information

Configure an Apache Web Agent Using GUI or Console Mode (see page 87)
How to Configure Any Web Agent in Unattended Mode (see page 103)

Configure an Apache Web Agent Using GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Apache Web Server, you enter a 1, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

To configure the Apache Web Agent

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI mode: **.**/ca-wa-config.bin

      Console mode: ./ca-wa-config.bin -i console
2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.
3. In the Select Web server(s) dialog box, select the option for the Apache Web Sever and click Next.
4. In the Apache Web Server Path dialog box, specify the Apache Web Server root, for example, /opt/apache2. Click Next.

If you installed the Agent on an Apache-based server, such as an IBM HTTP Server, or Oracle server, the Web Agent may not recognize the path. In this case, the Configuration Wizard displays the Apache Web Server Failure dialog box with the following options:

- I would like to re-enter the Apache Server Root.

  Select this option for an Apache web server and re-enter the root path.

- I would like to enter a specific configuration path.

  Select this option if you are using an Apache-based web server (such as IBM HTTP, HP Apache-based, or Oracle). You are prompted to enter the full configuration path to the web server root.

- I don't have an Apache web server.

  Choose this option to skip Apache configuration and continue with the Agent configuration.

Click Next.

5. Following the server root path, specify the version of Apache you are using. Select from the following options:

   - Apache version 2.0

6. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

7. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter ApacheDefaultSettings.

8. In the Web Server Configuration Summary dialog box. Confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed.

9. Click Done when the installation is complete.

10. Enable the Web Agent:

a. Open the WebAgent.conf file, located as follows:

Apache_home/conf

b. Set the EnableWebAgent parameter to yes.

c. Save and close the file.

11. Restart the web server.

When you run the Configuration Wizard for the Apache Web Agent, it makes changes to the Web Server's httpd.conf file and to the library path.

For httpd.conf changes to take effect, you need to restart the web server.

12. For Apache on UNIX systems, optimize the Apache Web Agent by tuning the shared memory segments.

More Information

Configuration Changes to Web Servers with Apache Web Agent (see page 155)
Configure an Apache Web Agent (see page 83)
Tune the Shared Memory Segments (see page 114)

Improve Server Performance with Optional httpd.conf File Changes

You can improve server performance by modifying the default configuration settings in the httpd.conf file; however, these changes are *not* required:

To improve server performance with optional httpd.conf file changes

1. For Apache and Oracle iPlanet servers, assign a higher priority level to your Apache20WebAgent.dll file than any other auth or access modules installed in your server's configuration.
2. For low-traffic websites, define the following directives:
   - Set MaxRequestsPerChild>1000 *or* Set MaxRequestsPerChild=0
   - MinSpareServers >5
   - MaxSpareServers>10
   - StartServers=MinSpareServers>5

3. For high-traffic websites, define the following directives:
   - Set MaxRequestsPerChild>3000 *or* Set MaxRequestsPerChild=0
   - MinSpareServers >10
   - MaxSpareServers>15
   - StartServers=MinSpareServers>10

Note: CA Services can provide assistance with performance-tuning for your particular environment.

Set the LD_PRELOAD Variable

Apache-based SiteMinder agents require that the LD_PRELOAD variable is set to the following value:

`LD_PRELOAD=`*`web_agent_home`*`/bin/libbtunicode.so`

Set LD_PRELOAD for Using X.509-based Auth Schemes with Domino 6.5.3/SuSe8 Linux System

When accessing resource protected with any X.590-based Authentication Schemes on Domino 6.5.3/SuSe8 Linux, the Domino Server Crashes and generates an NSD.

To resolve this issue, set the following environment variable before starting the Domino Web Server:

export LD_PRELOAD=/usr/lib/libstdc++-libc6.2-2.so.3

Set the LD_ASSUME_KERNEL for Apache Agent on SuSE Linux 9 for zSeries

After you install the Web Agent on an Apache web server running on SuSE Linux 9 for zSeries, set the LD_ASSUME_KERNEL environment variable as follows:

```
LD_ASSUME_KERNEL=2.4.21

export LD_ASSUME_KERNEL
```

Important! You must set this variable to 2.4.21 because it represents the kernel release upon which the Web Agent libraries are built.

Without this setting, the following problems occur:

- The Apache web server will not start properly.
- Host registration dumps core.

Chapter 7: Configure a Domino Web Agent

This section contains the following topics:

Configure a Domino Web Agent on Windows Systems

To configure a Domino Web Agent on Windows systems, perform the following tasks:

- Add the Domino Web Agent DLL
- Run the Web Agent Configuration Wizard
- (Optional) Configure the CGI directory and CGI URL Path Settings
- (Optional) Configure alias settings to enable HTML Forms authentication schemes

Add the Domino Web Agent DLL (Windows)

To make the Domino Web Agent operate properly, add the DOMINOWebAgent.dll file to the filter DLLs. The Web Agent DLL must be the first DLL in the list.

Follow these steps:

1. Open Lotus Notes.
2. Select File, Database, Open.
3. In the Server field, select the Domino Server where you installed the Web Agent.
4. In the Database scroll box, select the address book of the server.

   Verify that names.nsf appears in the Filename field.
5. Click Open.

   The address book of the server opens.
6. In the left pane, expand the Server folder and double-click the All Server Documents icon.
7. Select your server and click Edit Server.

   The administration console of the Domino server opens.
8. Select the Internet Protocols tab.
9. In the DSAPI section of the window, find the DSAPI filter file names field and enter the full path to the Domino Web Agent DLL. Verify that the Domino Web Agent DLL appears first in the list. The default location of this DLL file is shown in the following example:

   web_agent_home\bin\
   DOMINOWebAgent.dll

   web_agent_home

   Indicates the directory where the SiteMinder agent is installed on your web server.

   Default (Windows 32-bit installations only): C:\Program Files\CA\webagent

   Default (Windows 64-bit installations only): C:\Program Files\CA\webagent\win64

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64]): C:\Program Files (x86)\webagent\win32
10. Click Save and Close.
11. Restart the web server. In some situations, a reboot could possibly be necessary.

Run the Configuration Wizard for a Domino Web Agent on Windows

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

To configure a Domino Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you've placed the Wizard shortcut in a non-default location, the procedure will be different.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with administrator permissions. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   For information on registering the trusted host, see the installation chapter for your platform.

3. In the Select the Web server(s) dialog box, select the radio button for the Domino Web Sever and click Next.

4. In the Domino Web Server Path dialog box, specify the location of the notes.ini file, such as C:\Lotus\Domino\notesdata, then click Next.

   Note: The installation automatically writes the path to the WebAgent.conf in the notes.ini file.

5. Select the Web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional Web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the Web servers that you have previously configured.

a. Select one of the following:

- Overwrite--replaces the existing configuration of server instance with the new one.
- Preserve--keeps the existing web server's configuration without changing it.

Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this Web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter DominoDefaultSettings.

7. In the Web Server Configuration Summary dialog box, confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed.

8. Click Done when the installation is complete.

9. Enable the Web Agent:

   a. Open the WebAgent.conf file, located in where you installed the Domino Web server root directory.

   b. Set the EnableWebAgent parameter to YES.

   c. Save the file.

More Information

Agent Configuration Parameters Required for Domino Web Agents (see page 23)
Register Your System as a Trusted Host on UNIX (see page 54)

Configure the CGI Directory and CGI URL Path Settings on Windows Operating Environments (Optional)

To configure appropriate cgi-bin (ScriptAlias) settings for the Domino Web Agent, navigate to Internet Protocols tab for your server configuration in the Domino Administrator and configure the following settings:

- CGI directory: domino\html\cgi-bin
- CGI URL path: /cgi-bin

Configure Alias Settings to Enable HTML Forms Authentication Schemes (Optional)

To configure the Domino Web Agent to support HTML Forms authentication schemes perform the following tasks:

1. Create a subdirectory named "siteminderagent" in the Domino document root (\domino\html\) directory.
2. Copy all the subdirectories of *agent_home*\samples to the siteminderagent directory you created in Step 1.

   agent_home

   Specifies the SiteMinder Web Agent installation path.
3. To support X.509 Client Certificate and HTML Forms authentication schemes, additionally create a directory named "certoptional" in the siteminderagent directory you created in Step 1 and also copy all the subdirectories of *agent_home*\samples into it.

How to Configure a Domino Web Agent on UNIX Systems

To configure a Domino Web Agent on Windows systems, perform the following tasks:

- Add the Domino Web Agent DLL
- Run the Web Agent Configuration Wizard
- (Optional) Configure the CGI directory and CGI URL Path Settings
- (Optional) Configure Alias settings to enable HTML Forms authentication schemes

Add the Domino Web Agent DLL (UNIX)

To make the Domino Web Agent operate properly, add the libdominowebagent.so library file to the filter files. The Web Agent library file must be the first file in the list.

Follow these steps:

1. Open Lotus Notes.
2. Select File, Database, Open.
3. In the Server field, select the Domino Server where you installed the Web Agent.
4. In the Database scroll box, select the address book of the server.

   Verify that names.nsf appears in the Filename field.
5. Click Open.

   The address book of the server opens.
6. In the left pane, expand the Server folder and double-click the All Server Documents icon.
7. Select your server and click Edit Server.

   The administration console of the Domino server opens.
8. Select the Internet Protocols tab.
9. In the DSAPI section of the window, find the DSAPI filter file names field and enter the full path to the Domino Web Agent file. Verify that the Domino Web Agent file appears first in the list. The default location of the file is shown in the following example:

   web_agent_home\bin\libdominowebagent.so

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed.

   Default (UNIX/Linux installations): /opt/ca/webagent

   Note: If the Domino Web Agent is installed on an AIX operating system, the file name of the Domino Web Agent for the DSAPI filter is libdominowebagent.a
10. Click Save and Close.
11. Restart the web server.

Configuration Methods for Domino Web Agents on UNIX Systems

The following configuration methods are available for Web Agents on UNIX systems:

- GUI mode
- Console mode
- Unattended mode

More Information

How to Configure Any Web Agent in Unattended Mode (see page 103)
Register Your System as a Trusted Host on UNIX (see page 54)

Configure Domino Web Agents in GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Apache Web Server, you enter a 1, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI mode: **.**/ca-wa-config.bin

      Console mode: ./ca-wa-config.bin -i console

   Note: If you chose to configure the Web Agent immediately after the installation, SiteMinder automatically starts the Configuration Wizard.
2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.
3. In the Select the Web server(s) dialog box, select the radio button for the Domino Web Sever and click Next.
4. In the Domino Web Server Path dialog box, specify the location of the notes.ini file, such as /local/notesdata, then click Next.

   Note: The installation automatically writes the path to the WebAgent.conf in the notes.ini file.
5. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.
   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter DominoDefaultSettings.

7. In the Web Server Configuration Summary dialog box. Confirm that the configuration settings are correct, then click Install.

   The Web Agent files are installed.

8. Click Done when the installation is complete.

9. Enable the Web Agent:

   a. Open the WebAgent.conf file, located in the Domino web server root directory.

   b. Set the EnableWebAgent parameter to Yes.

   c. Save the file.

10. If your Domino web server runs on AIX, you must enable run time linking after configuring your agent (you only need to do this once) with the following steps:

    a. Run the following commands:

    ```
    cd domino_server_path/lotus/notes/latest/ibmpow
    /usr/bin/rtl_enable ./http -brtl
    mv ./http ./http.orig
    mv ./http.new ./http
    ```

    b. Start the Domino web server.

Configure the CGI Directory and CGI URL Path Settings on UNIX Operating Environments (Optional)

To configure appropriate cgi-bin (ScriptAlias) settings for the Domino Web Agent, navigate to Internet Protocols tab for your server configuration in the Domino Administrator and configure the following settings:

- CGI directory: domino/html/cgi-bin
- CGI URL path: /cgi-bin

Configure Alias Settings to Enable HTML Forms Authentication Schemes on UNIX Operating Environments (Optional)

To configure the Domino Web Agent to support HTML Forms authentication schemes perform the following tasks:

1. Create a subdirectory named "siteminderagent" in the Domino document root (/domino/html) directory.
2. Copy all the subdirectories of *agent_home/*samples to the siteminderagent directory you created in Step 1.

   agent_home

   Specifies the SiteMinder Web Agent installation path.
3. To support X.509 Client Certificate and HTML Forms authentication schemes, additionally create a directory named "certoptional" in the siteminderagent directory you created in Step 1 and also copy all the subdirectories of *agent_home/*samples into it.

Chapter 8: Configurations Available for All Web Agents

This section contains the following topics:

How to Configure Any Web Agent in Unattended Mode

After you have installed the Web Agent on one system, you can automate the Web Agent configuration on other web servers using the Agent's unattended configuration feature. An unattended configuration lets you configure the Web Agent without any user interaction.

To configure any Web Agent in unattended mode, use the following process:

1. Prepare an unattended configuration.
2. Run an unattended configuration.

Prepare an Unattended Configuration

Unattended configuration uses the ca-wa-installer.properties file to propagate the Web Agent configuration set up across all Agents in your network. For configuration, you define configuration parameters in the properties file, then copy the file to any web server in your network to run an unattended configuration.

When you perform an initial Web Agent installation and configuration, the ca-wa-installer.properties file is installed in the following location:

web_agent_home/install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation and configuration.

To make the ca-wa-installer.properties file available on your system

1. Run an initial installation of the Web Agent.
2. Open the ca-wa-installer.properties file and, if necessary, modify the configuration parameters.
3. Save the file.

More Information

Install a Web Agent on a UNIX System (see page 43)
Install a Web Agent on a Windows System (see page 25)

Run an Unattended Configuration

Before you run an unattended configuration, you should have completed the following tasks:

- an initial (attended) Web Agent installation
- an initial (attended) Web Agent configuration
- modification of the ca-wa-installer.properties file

  You use this file to run subsequent unattended Web Agent configurations
- an installation (attended or unattended) on the system where you want to run the unattended configuration. This installation makes the configuration executable available.

To run an unattended Web Agent configuration

1. From a system where the Web Agent is already installed, copy the ca-wa-installer.properties file from *web_agent_home*/install_config_info to a local directory on the system where you want to run an unattended configuration.
2. Open a console window and navigate to *web_agent_home*/install_config_info.

   Important! Before running a SiteMinder utility or executable on Windows Server 2008, open the command line window with administrator permissions. Open the command line window this way, even if your account has administrator privileges.

   Note: You must run the unattended configuration from the install_config_info directory because the configuration executable file must remain in this directory.
3. Run the following command:

   agent_config_executable -f *properties_file* -i silent

   For example, if you copied the properties file to the install_config_info directory, the command would be:

   Windows:

   ca-wa-config.exe -f ca-wa-installer.properties -i silent

   UNIX:

   ca-wa-config.bin -f ca-wa-installer.properties -i silent

   If you do not copy the properties file to the install_config_info directory, specify the full path to this file in the command. If there are spaces in the directory path, enclose the entire path between quotation marks.

   When the configuration is complete, you return to the command prompt.
4. Check to see if the configuration completed successfully by looking in the CA_SiteMinder_Web_Agent_*version*_InstallLog.log file, located in the *web_agent_home*/install_config_info directory. This log file contains the results of the configuration.

Check SmHost.conf File Permissions for Shared Secret Rollover

If you enable shared secret rollover, the user who owns the web server process must have permissions to write to the SmHost.conf file. If this file cannot be modified by this user, then the shared secret rollover cannot be updated.

For example, for IIS web servers, the account associated with the IIS web server processes needs appropriate permissions for the SMHost.conf file. In many versions of IIS, this account is the Network Service account.

Reconfigure a Web Agent

Reconfigure a Web Agent for the following reasons:

- You have upgraded the Web Agent and now you need to update the configuration
- You need to change the configuration settings previously defined for a Web Agent
- You need to remove the configuration settings from the Web Agent without uninstalling the entire Web Agent (you would need to configure the Web Agent again at a later time)
- You want to configure the Web Agent for a different Web Server installed on the same system as the configured server.

To reconfigure a Web Agent in any mode, re-run the Configuration Wizard. There are no additional steps or prompts for reconfiguring an Agent.

More Information

Configure an Oracle iPlanet Web Agent (see page 73)
Configure an Apache Web Agent (see page 83)
Configure a Domino Web Agent (see page 93)

How to Set Up Additional Agent Components

The Web Agent Configuration Wizard guides you through basic Agent configuration. However, there are other Agent components that you can configure without the wizard.

All SiteMinder Web Agents can protect resources, act as forms credential collectors (FCC) and/or an SSL credential collectors (SCC), and serve as a cookie provider for single sign-on. The Web Agent can serve in one or more of these roles simultaneously.

At installation, some of these functions, such as acting as the forms credential collector, are set up automatically; however, other capabilities, such as the cookie provider require additional configuration.

You can set up any of the additional components as follows:

- Configuring an Agent as a forms credential collector

  The libraries and files for forms credential collection are set up automatically during installation.

- Configuring an Agent as an SSL credential collector

  You specify whether the Agent performs SSL credential collection during the initial Agent configuration with the Configuration Wizard.

- Configuring the Agent as a cookie provider for multiple cookie domain single sign-on

  A cookie provider lets the Agent implement single sign-on in a multiple cookie domain environment. All Web Agents can act as a cookie provider, but all cookie providers within a domain must use the same domain name. The cookie provider URL setting in the Agent's configuration dictates which Web Agent is the cookie provider. After you determine which Agent is the cookie provider, you configure all other Agents in the single sign-on environment to point to the cookie provider by entering that Agent's URL.

Chapter 9: Dynamic Policy Server Clusters

Earlier versions of SiteMinder agents did *not* automatically discover when Policy Servers were added or removed from a cluster. The agents recognized the changes only after their respective web servers were restarted.

SiteMinder r12.0 SP3 supports dynamic Policy Server clusters. Agents automatically discover Policy Servers that are added or removed from an existing cluster when dynamic Policy Server Clusters are enabled.

For example, suppose that your agent connects to a cluster of the following Policy Servers:

- 192.168.2.100
- 192.168.2.101
- 192.168.2.103
- 192.168.2.104

Suppose that you later decide to remove the server 192.168.2.103 to upgrade its operating system. In this situation, enabling dynamic Policy Server clusters lets your agents recognize the change in the membership of the cluster without restarting.

Restart your web server if you do any of the following tasks:

- Change the configuration of an existing Policy Server (using the configuration wizard).
- Create a Policy Server cluster.
- Delete a Policy Server cluster.
- Change the values for any of the following Policy Server settings:
  - EnableFailOver
  - MaxSocketsPerPort
  - MinSocketsPerPort
  - NewSocketStep
  - RequestTimeout

Connect a Web Agent to a Dynamic Policy Server Cluster

You can connect a Web Agent to one or more dynamic Policy Server clusters by modifying the SmHost.conf file on your web server.

Follow these steps:

1. Open the following file with a text editor:

   web_agent_home\config\SmHost.conf

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed.

   Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

   Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

   Default (UNIX/Linux installations): /opt/ca/webagent

2. Do *one* of the following tasks:

   - If this Web Agent has *never* been connected to dynamic cluster of Policy Servers before, create a line (anywhere in the file) with the following text:

     enableDynamicHCO="YES"

   - If this Web Agent has previously been connected to a dynamic cluster of Policy Servers, change the value of the existing enableDynamicHCO parameter from "NO" to "YES".

3. Save the SmHost.conf file, and then close the text editor.

4. Restart your web server.

   The Web Agent is connected to dynamic Policy Server clusters.

Chapter 10: Starting and Stopping Web Agents

This section contains the following topics:

Enable a Web Agent

Configure your agent parameters and then enable the agent to protect the resources on the web server.

Note: *No* resources are protected until you also define policies in the SiteMinder Policy Server.

Follow these steps:

1. Open the WebAgent.conf file with a text editor.

   Note: SiteMinder r12.0 SP3 Agents for IIS installed on 64-bit Windows operating environments have *two* WebAgent.conf files. One file is associated with 32-bit Windows applications. The other file is associated with 64-bit Windows applications. Modify *both* WebAgent.conf files to start or stop the SiteMinder Agent for IIS on all 32-bit *and* 64-bit applications on a particular IIS web server.

2. Change the value of the EnableWebAgent parameter to yes.
3. Save and close the WebAgent.conf file.
4. Restart the web server (the web server itself, not the computer on which it runs).

   The Web Agent is enabled.

Disable a Web Agent

To stop the Web Agent from protecting the resources on your web server and stop communicating with the Policy Server, disable the Web Agent.

Follow these steps:

1. Open the WebAgent.conf file with a text editor.

   Note: SiteMinder r12.0 SP3 Agents for IIS installed on 64-bit Windows operating environments have *two* WebAgent.conf files. One file is associated with 32-bit Windows applications. The other file is associated with 64-bit Windows applications. Modify *both* WebAgent.conf files to start or stop the SiteMinder Agent for IIS on all 32-bit *and* 64-bit applications on a particular IIS web server.

2. Change the value of the EnableWebAgent parameter to no.
3. Save and close the WebAgent.conf file.
4. Restart the web server (the web server itself, not the computer on which it runs).

   The Web Agent is disabled.

Starting or Stopping Most Apache-based Agents with the apachectl Command

Starting or stopping most Apache-based agents with the apachectl command on UNIX or Linux operating environments requires setting the environment variables for the product first.

Note: The Apache-based agents do *not* support the apachectl -restart option. This procedure does *not* apply to Apche-based IBM HTTP servers. Use this procedure instead.

Follow these steps:

1. For UNIX/Linux operating environments, set the environment variables by running the following script:

   ```
   ./ca_wa_env.sh
   ```

2. Use *one* of the following commands:

   ```
   apachectl -stop
   ```

   ```
   apachectl -start
   ```

Chapter 11: Operating System Tuning

This section contains the following topics:

Tune the Shared Memory Segments

If you install an Apache or Oracle iPlanet Web Agent on Solaris systems, you must tune the operating system's shared memory settings for the Web Agent to function correctly. By increasing the operating system's shared memory segments, you improve the performance of the Web Agent. The variables that control shared memory segments are defined in the operating system's specification file.

For AIX operating systems, you must run the following command before starting an Apache server:

```
export EXTSHM=ON
```

Note: You may need to tune the shared memory segments if you are using Linux. For more information about the shared memory segments and how to tune them, see the documentation for your particular operating system.

To increase shared memory segments

1. Follow the appropriate procedure for your operating system:
   - Solaris**:** Open the /etc/system file, using the editor of your choice.
2. Modify the shared memory variables using *one* of the following methods:
   - Solaris: Add the variables shown in the following list and configure them using the recommended settings shown in the examples. Use the following syntax:

     ```
     set shmsys:shminfo_shmmax=33554432
     ```

     shmsys:shminfo_shmmax

     Specifies the maximum shared memory segment size. Controls the maximum size of the Agent resource and session cache.

     Note: To estimate the amount of memory segments that are required, allocate 4 KBs per entry in each cache, or view cache usage statistics in the OneView Monitor. See the *Web Agent Configuration* Guide for more information about using the OneView Monitor.

     Example: 33554432 (32 MB) for busy sites that require large caches.

     shmsys:shminfo_shmmin

     (Not required for Solaris) Minimum shared memory segment size. Controls the minimum size of the Agent resource and session cache.

shmsys:shminfo_shmmni

Specifies the maximum number of shared memory segments that can exist simultaneously, systemwide.

Example: (except Solaris 9) N/A

Example: (Solaris 9) 200

shmsys:shminfo_shmseg

(Not required for Solaris 9) Specifies the maximum number of shared memory segments per process.

Example: 24

semsys:seminfo_semmni

Specifies the number of semaphore identifiers. Use 11 for every instance of the Agent that you run on the system.

Example: (except Solaris 9) 100

Example: (Solaris 9) 200

semsys:seminfo_semmns

Specifies the number of semaphores in the system. Use 10 for every instance of the Agent that you run on the system.

Example: (Solaris 9) 100

Example: (Solaris 9) 400

semsys:seminfo_semmnu

Specifies the number of processes using the undo facility. For optimal performance, set the semmnu value so it exceeds the number of Apache child processes running on the system at any one time. For Apache–based servers, use a value exceeding the maxclients setting by 200 or more.

Example: (Solaris 9) 200

3. Save your changes then exit the file or the utility.
4. Reboot the system.
5. Verify your changes by entering the command:

```
$ sysdef -i
```

How to Tune the Solaris 10 Resource Controls

Tune the resource controls at the project level to improve the performance of the agent.

Note: See your Solaris documentation for more information.

Tuning the resource controls on Solaris 10 uses the following process:

1. Determine the project that is associated with the user account under which the Web Agent runs.
2. Increase the settings for any of the following resource controls of that project:

   project.max-shm-ids

   Specifies the maximum shared memory IDs for a project.

   project.max-sem-ids

   Specifies the maximum number of semaphore IDs for a project.

   project.max-msg-ids

   Specifies the maximum number of message queue IDs for a project.

   project.max-shm-memory

   Specifies the total amount of shared memory allowed for a project.

   process.max-sem-nsems

   Specifies the maximum number of semaphores allowed per semaphore set.

   process.max-sem-ops

   Specifies the maximum number of semaphore operations allowed per semop.

   process.max-msg-messages

   Specifies the maximum number of messages on a message queue.

   process.max-msg-qbytes

   Specifies the maximum number of bytes of messages on a message queue.

Chapter 12: Password Services

This section contains the following topics:

Password Services Implementations

SiteMinder Password Services lets you manage user passwords using LDAP user directories or ODBC databases.

The following mechanisms are available for implementing password management:

Password Services CGI

(Default) Implements Password Services using customizable HTML forms. This implementation supports previously-customized password services such as .template forms.

FCC-based Password Services

Implements Password Services using SiteMinder forms.

Note: For more information, see the *Web Agent Configuration* Guide.

Password Services servlet

Implements Password Services using standard JSP forms that you can customize to meet the needs of your web site. To use Password Services with JSP forms, you must modify both your web server and your servlet engine.

Note: For a list of supported servlet engines, see the SiteMinder support matrix at http://ca.com/support.

How to Set Up Your Environment for JSP Password Services

To use Password Services with JSP forms, you must modify your web server and servlet engine using the following process:

1. Add the the following password-services JAR files to the servlet engine classpath:

   web_agent_home\jpw\jpw.jar
   web_agent_home\Java\servlet.jar
   web_agent_home\Java\ cryptoj.jar

2. Update the file that invokes your servlet engine to invoke the JSP Password Services servlet by adding the following line:

   ```
   /siteminderagent/pwservlet/PSWDChangeServlet=PSWDChangeServlet
   ```

3. Configure your servlet engine for JSP Password Services. See the documentation for your Servlet engine for more information.

   Note: For a list of supported servlet engines, see the SiteMinder support matrix at http://ca.com/support.

Chapter 13: Uninstall a Web Agent

This section contains the following topics:

Notes About Uninstalling Web Agents

Be aware of the following:

- All Web Agents for all installed web servers will be uninstalled.
- The Password Services and Forms directories, (pw_default, jpw_default, samples_default) will be removed. However, the non-default copies of these directories (pw, jpw, samples) are not removed because these directories may contain customized files.
- Make sure that the JRE is installed on the Web Agent system, as it is needed for uninstallation. For a supported version, see the SiteMinder r12.0 SP3 Platform Matrix at Technical Support.

Set JRE in PATH Variable Before Uninstalling the SiteMinder Agent

On Windows and UNIX systems, when you are uninstalling a SiteMinder Agent, make sure the JRE is in the PATH variable or the uninstallation program stops and issues one of the following error messages:

- “Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine.”
- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

Follow these steps:

On Windows

1. Go to the Control Panel.
2. Double-click System.
3. In the Environment Variables dialog, add the location of the JRE to the PATH system variable.

   For example, C:\j2sdk*version_number*\jre\bin

On UNIX

Run the following commands:

1. PATH=$PATH:*JRE*/bin

   JRE

   Specifies the location of your JRE.

   For example, /usr/bin/j2sdk*version_number*/jre
2. export PATH

Uninstall a Web Agent from a Windows Operating Environment

Before you un–install the SiteMinder Web Agent from a Windows operating environment, consider making backup copies of your registry settings and Web Agent configuration settings.

Follow these steps:

1. Stop the web server.
2. Choose *one* of the following procedures:
   - To remove the Web Agent using the wizard, go to Step 3.
   - To remove the Web Agent using the console-based program, go to Step 8.
3. Click Start, Control Panel, Programs and Features.

   A list of installed programs appears.
4. Click CA SiteMinder Web Agent *version_number*.
5. Click Uninstall/Change.

   The uninstallation wizard appears.
6. Review the information in the Uninstall SiteMinder Web Agent dialog, then click Uninstall.

   The wizard removes the web agent.
7. Wait for the wizard to finish, then go to Step 12.
8. Open a command-line window.
9. Navigate to the following directory.

   web_agent_home

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed on your web server.

   Default (Windows 32-bit installations of SiteMinder IIS Web Agents only): C:\Program Files\CA\webagent

   Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32
10. Run the following command:

    ```
    ca-wa-uninstall.cmd -i console
    ```
11. Wait for the un–installation program to finish, then go to Step 12.

12. Start the web server.

Important! Delete the ZeroG registry file from the following location after uninstalling the Web Agent: C:\Program Files\ZeroG Registry\com.zerog.registry.xml

Uninstall Documentation from a Windows System

Running the documentation uninstallation program removes the manuals for all products from the ca_documents directory.

To uninstall the documentation

1. Stop the web server.
2. Open the Control Panel.
3. Select Add/Remove Programs.
4. Scroll through the program list and select CA SiteMinder Documentation *version* for Web Agent.
5. Click Change/Remove.
6. Review the information in the dialog box to confirm the uninstallation.
7. Click Uninstall.

   The documents are removed.
8. Click Done to exit the installer.

Uninstall a Web Agent from a UNIX System

These instructions are for GUI and Console Mode removal.

Note: Removing a Web Agent from a 64-bit SuSE Linux 10 system requires additional preparations.

The steps for the two modes are the same, with these exceptions for Console Mode:

- Select the option that you want by entering a corresponding number.

Press Enter after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.

Note: Before you uninstall, we recommend copying your agent configuration settings to have as a backup.

1. Stop the web server.
2. Log in to the UNIX system.
3. Specify the JRE in the PATH environment variable to uninstall the Web Agent. If you receive an error message that the Java virtual machine could not be found, add the JRE to the PATH variable as follows:

   PATH=/*jre_home*/bin:${PATH}

   export PATH

   jre_home is the location of the JRE.
4. Navigate to the directory where the Web Agent is installed:

   web_agent_home/install_config_info/ca-wa-uninstall
5. If necessary, verify that you have execute permissions on the uninstallation program by entering chmod +x uninstall.
6. From a console window, enter one of the following commands:
   - GUI mode: ./uninstall
   - Console mode: ./uninstall -i console

   The uninstallation program starts.
7. Read the information in the dialog to confirm the removal of the Web Agent, then click Uninstall. The Web Agent is removed from the system.
8. Click Done to exit the uninstallation program.
9. (Optional) For Apache-based agents, remove the lines from the httpd.conf file that the Configuration Wizard added.
10. Change to your home directory (the current directory has been deleted).
11. Restart the web servers.

Uninstall Documentation from UNIX Systems

These instructions are for GUI and Console Mode uninstallation. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number.
- Press Enter after each step to proceed through the process instead of "clicking Next," as stated in the following procedure. The prompts for each mode help guide you through the process.

To uninstall documentation from UNIX systems

1. Navigate to the following directory:

   documentation_home/install_config_info/ca-wa-doc-uninstall

2. Enter one of the following commands:

   - GUI mode: ./uninstall
   - Console mode: ./uninstall -i console

   The uninstallation program begins and displays a dialog box to confirm the uinstallation.

3. Click Uninstall.

   The documentation is removed.

4. Click Done to exit the installer.

To reinstall the documentation, run the appropriate documentation program for the product.

Remove Leftover Items

The com.zerog.registry.xml file is left on the system after you uninstall the Web Agent. Remove this file.

You can locate this file at one of the following:

- $HOME/.com.zerog.registry.xml
- /var/.com.zerog.registry.xml

Chapter 14: Troubleshooting

This section contains the following topics:

Changing Document Root Folder after Agent Configuration Leaves Resources Unprotected

Symptom:

I changed the location of the document root folder on my web server after I configured my SiteMinder agent. Now the resources in the new document root folder are unprotected.

Solution:

If you change the location of the document root folder on your web server, run the agent configuration program again.

Agent Start-Up/Shutdown Issues (Framework Agents Only)

If the Web Agent does not start after installation or you cannot shut it down, check the following error logs:

- On Windows, check the Event Viewer's Application Log.
- On UNIX, messages are processed by the server's standard error handling. For the Apache 2.0, errors are written to the web server error log.
- On Windows or UNIX, run the Low Level Agent Worker Process (LLAWP) to isolate the problem.

Agent Won't Start Because LLAWP is Already Running or Log Messages not Written to the Correct Log Files

Valid on UNIX

Symptom:

I'm having one or more of the following problems:

- My Web Agent won't start because the LLAWP process is already running.
- My Web Agent starts, however the log messages are being written to the log files of a second agent instance.

Solution:

This problem may occur when multiple disks on the same computer use the same mount point. The Web Agent uses the inode of a directory to allocate system resources, and if the inodes are the same, resource collisions and errors result. To fix this problem, use the following process:

1. Create a new subdirectory on your web server (this creates a unique inode).
2. Change the path shown in the ServerPath parameter of the Web Agent so it points to the new subdirectory.

Note: For more information, see the *Web Agent Configuration Guide*.

Troubleshoot Agent Start-Up/ShutDown with LLAWP

If the Agent is not starting or shutting down properly, you can run the Low Level Agent Worker Process (LLAWP) from the command line.

The LLAWP handles inter-process Agent management. For Apache 2.0, the LLAWP process automatically starts when the Apache web server starts.

By running LLAWP from the command line, you eliminate the web server from the diagnostic process, which isolates Web Agent issues. Error messages are written to the Event log for Windows or to the console on UNIX systems.

Shut Down LLAWP

If the LLAWP process does not shut down properly when shutting down the web server, shut down the LLAWP from the command line. This shuts down the running worker process associated with a WebAgent.conf file.

To shut down the LLAWP, use the command with this syntax:

LLAWP *path_to_WebAgent.conf -web_server_type* -shutdown

For example:

LLAWP /usr/apache/conf/WebAgent.conf -APACHE20 -shutdown

Note: Configuration file names and version strings that contain spaces should be surrounded by quotes, such as "value with spaces."

The LLAWP process will take a few seconds to shut down.

Use the command line to shut the LLAWP down instead of the kill -9 command, so that the process cleans up shared system resources used by the Web Agent.

Web Agent Start Up and Shut Down Issues (IBM HTTP Server)

If the Web Agent does not start after installation or you cannot shut it down, check the following error logs:

- On Windows, check the Event Viewer's Application Log.
- On UNIX, messages are processed by the server's standard error handling.

Lack of Write Permissions on Host Configuration File

Symptom:

My web agent log shows the following error:

```
Siteminder Web Agent not having write permissions on host configuration file.
```

Solution:

Verify that the account under which the web server operates has write permissions for the SmHost.conf file.

Connectivity and Trusted Host Registration Issues

This section contains troubleshooting information related to trusted host registration.

Trusted Host Registration Fails

Symptom:

I cannot register a trusted host.

Solution:

Check the following:

- Make sure that the Policy Server is installed and configured on the target server, that the IP address for the server is correct, and that the Policy Server is running.
- Check the SiteMinder administrator name and password and make sure these are correct.
- Make sure that the Host Configuration Object and Agent Configuration Object specified during the Agent installation and configuration are defined at the Policy Server.
- You may be using a name for the trusted host that is already in use by an existing trusted host. Re-register using a unique name for the trusted host.

No Connection From Trusted Host to Policy Server

Symptom:

Trusted host cannot make a connection to the Policy Server.

Solution:

Do the following:

- Ensure that the EnableWebAgent parameter in the WebAgent.conf file is set to yes.
- Check for the SmHost.conf file in *web_agent_home*/config. The presence of this file indicates a successful registration of the trusted host.

  web_agent_home

  Indicates the directory where the SiteMinder Agent is installed.

  Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

  Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

  Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

  Default (UNIX/Linux installations): /opt/ca/webagent

- Ensure that the host where the Agent is installed and has been registered as a trusted host.
- Make sure the Agent Configuration Object has a DefaultAgentName specified. Also, ensure that the minimum required parameters are configured for your particular web server.
- Ensure that the Policy Server is running.

Host Registered, but the SMHost.conf file has been Deleted

Symptom:

A Trusted Host is registered but the SmHost.conf file has been deleted.

Solution:

In the Administrative UI, remove the Trusted Host Object corresponding to the host name for which the file was deleted. Re-register the host using the smreghost tool.

General Installation Issues

This section contains troubleshooting information related to installations.

One Installation Hangs During Multiple Installations on the Same System

Symptom:

You are running multiple installations on the same system at the same time and an installation hangs.

Solution:

Try the following tasks in the order listed:

1. Reboot the system and try the installation again.
2. Rename the ZeroG registry file, then retry the installation. The registry file is in the following locations:
   - Windows: C:\Program Files\ZeroG Registry\com.zerog.registry.xml
   - UNIX: $HOME/.com.zerog.registry.xml or /var/.com.zerog.registry.xml

   The registry file is locked while an installation is taking place, so if multiple installations are running at the same time, they cannot write to this file, causing the installation to hang.

Location of the Installation Failure Log

Symptom:

I want to see what failed during the installation.

Solution:

See the ca-wa-details.log file, located in *web_agent_home*/install_config_info.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

Web Agent Not Shown in Add/Remove Programs Control Panel

Symptom:

I cannot uninstall the Web Agent from the Add/Remove Programs list control panel because the SiteMinder Web Agent is not listed.

Solution:

Remove the Agent as follows:

1. Open the registry editor.
2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SiteMinder\WebAgent
3. Highlight the entire UninstallString entry and copy it.
4. Open a DOS window and paste the UninstallString into the window at a DOS prompt.
5. Press ENTER.

   The Agent is uninstalled.

Error Message During Upgrade

Valid on Windows, UNIX

Symptom:

You receive the following error during an upgrade:

ComponentMoveData Error -115

Solution:

Do the following:

1. Click OK to exit the error message.
2. Start the Policy Server Management Console.
3. From the console, stop the Policy Server.
4. Close the Management Console.
5. Run the upgrade or again and this error message should no longer appear.

Miscellaneous Issues

This section contains troubleshooting information related to miscellaneous issues.

Netscape Browser Won't Open PDFs

Valid on UNIX

Symptom:

I cannot open PDF Files from the Online Manuals Index HTML page on a UNIX system using a Netscape browser.

Solution:

If a .pdf file does not open after you click a link on the doc_index.htm page, set Acrobat Reader as a helper application in Netscape Navigator. When you set this option, Netscape automatically launches Acrobat Reader each time you request to view a .pdf file.

To set Acrobat Reader as a helper application

1. In Navigator, go to Edit, Preferences.
2. In the Netscape Preferences dialog, select Navigator, Applications.
3. Under Applications, Specify helper applications for different file types, select Portable Document Format and click Edit.
4. In the Netscape Applications dialog, select Applications and set it to the following:

   Acrobat_Reader_home/bin/acroread %s

   For example, if you installed Acrobat Reader in the default location, set this value to:

   /usr/local/Acrobat4/bin/acroread %s.
5. Click OK to close these dialogs.

   After you set this option, Navigator launches Acrobat Reader and opens the .pdf file in the /tmp directory.

Adobe Acrobat Reader Won't Install on a Windows System

Valid on Windows

Symptom:

I cannot install Adobe Acrobat Reader on a Windows system.

Solution:

If the Acrobat Reader installation program hangs while the Policy Server is running, stop the server using the Policy Server Management Console, then the installation program should start.

Oracle iPlanet Web Agent Issues

This section contains troubleshooting information related to Oracle iPlanet Web Agents.

Web Server Starts but Web Agent Not Enabled

Symptom:

The Web Agent is not enabled even though the web server has started.

Solution:

Open the WebAgent.conf file, and then set the EnableWebAgent parameter to yes.

smget Error Message When Web Server Starts

Valid on Oracle iPlanet web servers

Symptom:

When starting the Web Server, you see the message:

shmget failed. You may be trying to make a cache that is too large.

Solution:

Make the recommended adjustments to the shared memory segments.

More information:

Tune the Shared Memory Segments (see page 114)
How to Tune the Solaris 10 Resource Controls (see page 116)

Reconfigured Web Agent Won't Operate

Valid on Oracle iPlanet web servers

Symptom:

Web Agent configuration changes are not in the obj.conf file. The Web Agent cannot operate.

Solution:

The Oracle iPlanet Administration console was used to make server modifications before the changes the Agent configuration program made to the obj.conf were applied. Reconfigure the Web Agent.

More information:

Apply SiteMinder Changes to Oracle iPlanet Configuration Files with Oracle iPlanet Administration Server Console for SunOne 6.1 Servers (see page 81)

Oracle iPlanet Web Server Fails at Runtime

Symptom:

Oracle iPlanet web server is failing at run time.

Solution:

Set the value of the StackSize setting (in the magnus.conf file of the Oracle iPlanet server) to 256 KB. The magnus.conf file is located in:

Oracle_iPlanet_home/*web_server_instance*/config

More Information

Tune the Shared Memory Segments (see page 114)

Apache Web Agent Issues

This section lists troubleshooting information for the Apache Web Agent.

More Information

Tune the Shared Memory Segments (see page 114)

Apache Server Shows shmget Failure On Startup

Symptom:

When starting the web server, you see: shmget failed.

You may be trying to make a cache that is too large or be doing apachectl restart.

Solution:

Make the recommended adjustments to the shared memory segments.

Apache Agent is Enabled but Default Server Page or Protected Resource Not Accessible

Symptom:

The default web server page or the protected resource is not accessible after enabling Web Agent.

Solution:

Make the recommended adjustments to the shared memory segments.

Apache Web Agent Not Operating

Symptom:

The Apache Web Agent is not operating.

Solution:

Tune the Apache operating system shared memory.

Domino Web Agent Issues

This section contains troubleshooting information related to Domino Web Agents.

Domino Web Agent Not Enabled but the Web Server has Started

Valid on Domino

Symptom:

The Domino Web Agent is not enabled even though the web server has started.

Solution:

Do the following:

- In the WebAgent.conf file, set the EnableWebAgent parameter to yes.
- Ensure that the DOMINOWebAgent.dll file has been added to the filter DLLs. The Web Agent DLL must be the first DLL in the list.

More Information

Add the Domino Web Agent DLL (Windows) (see page 94)

Domino Agent Cannot Initialize When Local Configuration Mode is Used

Valid on Domino

Symptom:

Domino Agent cannot initialize in local configuration mode.

Solution:

Check that the full path to the WebAgent.conf file is added to the notes.ini file.

Chapter 15: Unattended Installation

ca-wa-installer.properties File

The web agent installation and configuration wizards generate the ca-wa-installer.properties file. This file contains all of the information you entered into the respective wizards.

After creating a ca-wa-installer.properties file using the wizards once, use this properties file to install and configure additional web agents in your environment. Each additional agent requires the same operating environment, web server version and configuration wizard values as the agent installed and configured with the wizard.

For example, you *cannot* install an agent on a Solaris system with an Oracle iPlanet web server, and then use the same file on a Linux system with an Apache web server.

Modify General Information

In the General Information section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
USER_INSTALL_DIR	The location where the unattended installation will place the Web Agent. For example: C:\\Program Files\\ca\\webagent
USER_SHORTCUTS	The location where the installation places a shortcut to the Configuration Wizard. For example: C:\\Documents and Settings\\jdoe\\Start Menu\\Programs

Register a Trusted Host

In the Trusted Host Registration section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
HOST_REGISTRATION_YES	Indicates whether the installation will go through the trusted host registration process. For example, HOST_REGISTRATION_YES=1
ADMIN_REG_NAME	Name of the administrator with the rights to register a trusted host. For example, ADMIN_REG_NAME=siteminder
ADMIN_REG_PASSWORD	Password for the administrator with the rights to register a trusted host. This value is encrypted by the installation program. For example, ADMIN_REG_PASSWORD=ENC:nGDaSDy1H7qZqcdbkJKPEQ To change the password, you can either re-configure the Agent or modify this parameter by entering a new password in clear text.
SHARED_SECRET_ROLLOVER_YES	Enables shared secret rollover, which periodically changes the secret that encrypts communication between the trusted host and the Policy Server. The default is 0. Set this parameter to 1 to enable shared secret rollover. For example, SHARED_SECRET_ROLLOVER_YES=1

Identify Policy Servers for Trusted Host Registration

In the section to list Policy Servers for trusted host registration, you can modify the setting in the following table:

Parameter	Description and Sample Value
IP_ADDRESS_STRING	Specifies the IP address of the Policy Server where you are registering the trusted host. To have multiple bootstrap servers for failover. you can specify multiple addresses, separated by a comma. For example, IP_ADDRESS_STRING=111.11.1.11, 122.123.2.34

Specify the Host Configuration File

In the Host Configuration File Location section you can modify the settings in the following table:

Parameter	Description and Sample Value
SM_HOST_FILENAME	Names the Host Configuration File, SmHost.conf. For example, SM_HOST_FILENAME=SmHost.conf
SM_HOST_DIR	Identifies the directory where the SmHost.conf file is installed. The default For example, SM_HOST_DIR=C:\\Program Files\\ca\\webagent\\config

Select a Web Server for Configuration

In the Trusted Host Registration section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
APACHE_SELECTED APACHE_WEBSERVER_ROOT	Indicates which Apache web server you are configuring and that server's root directory. For example, for UNIX Systems: APACHE_SELECTED=0 APACHE_WEBSERVER_ROOT=/export/agent5qa/apache
IPLANET_SELECTED IPLANET_WEBSERVER_ROOT	For UNIX Systems. Indicates which Oracle iPlanet web server you are configuring and that server's root directory. For example, for UNIX Systems: IPLANET_SELECTED=1 IPLANET_WEBSERVER_ROOT=/export/agent5qa/sunonewebserver
DOMINO_SELECTED DOMINO_WEBSERVER_ROOT	For UNIX Systems. Indicates which Apache web server you are configuring and that server's root directory. For example, for UNIX Systems: DOMINO_SELECTED=0 DOMINO_WEBSERVER_ROOT=

Parameter	Description and Sample Value
WEB_SERVER_INFO	The WEB_SERVER_INFO setting contains information about the web servers configured with a SiteMinder Web Agent. You can either edit this setting in the file or re-run the Web Agent configuration to regenerate this string with the appropriate values. The WEB_SERVER_INFO entry consists of a set of web servers, separated by a semicolon. Each web server consists of comma-separated values. **Important!** The WEB_SERVER_INFO setting can be modified from one web server to another, even for the same machine, but modify the setting at your own risk. Making a mistake when changing a value could cause the Agent installer to fail or the Agent to be configured with inappropriate data. The WEB_SERVER_INFO setting is as follows: WEB_SERVER_INFO=;*server_instance*,*web_server_config_dir*,*web_server_listing*,*service_name*,*web_server_type*,*web_server_version*,*web_server_path*,empty_string,*empty_string*,*selected_web_server*,*existing_server_config*,*preserve_web_server*,*document_selection*,*OneView_Monitor_config*,*confirm_web_server_config*,*advanced_auth_scheme*,*agent_config_obj*

More Information

WEB_SERVER_INFO Variables (see page 143)

WEB_SERVER_INFO Variables

The WEB_SERVER_INFO variables and their values are as follows:

server_instance

Indicates the web server instance.

Example: https-server1

web_server_config_dir

Indicates the path to the web server's config directory.

Example: /usr/iplanet/servers/https-server1/config

web_server_listing

Reflects how the web server is shown in the list of available web servers to configure during configuration.

Example: https-server1 (Oracle iPlanet 6.0)

service_name

Indicates the web server service name.

Example: https-server1

web_server_type

Indicates the type of web server. Choose from the following types:

- apache
- domino
- iplanet
- sunone

For the Oracle iPlanet web server, use iplanet or sunone.

Example: sunone

web_server_version

Indicates the web server version

Example: 6.0

web_server_path

Indicates the path to the web_server_instance root

Example: /usr/iplanet/servers/https-server1

web_agent_operating_system

Indicates the type of operating system used by the Web Agent.

Limits: Windows, Unix

Example: Windows

empty_string

Indicates an empty string saved for future use.

Example: +EMPTYSTR+

selected_web_server

Indicates whether the selected web server should be configured with an Agent.

Limits: 1 (yes) or 0 (no)

existing_server_config

Previous web server configuration states whether there is an existing Agent configuration

Limits: 1 (yes) or 0 (no)

preserve_web_server

Indicates whether the specified web server's configuration with a Web Agent should be overwritten with a new configuration or preserved.

Limits: 1 (preserve) or 0 (overwrite)

document_selection

Used only for the Policy Server only. The Web Agent ignores this entry. Accept the default.

Limits: 1 (yes) or 0 (no)

OneView_Monitor_config

Used only for the Policy Server only. The Web Agent ignores this entry. Accept the default.

Limits: 1 (yes) or 0 (no)

confirm_web_server_config

Confirms whether the selected web server should be configured with an Agent.

Limits: 1 (yes) or 0 (no)

advanced_auth_scheme

Specifies which advanced authentication scheme, if any, is being used. Choose one of the following options:

- HTTP Basic over SSL
- X509 Client Certificate
- X509 Client Certificate and HTTP Basic
- X509 Client Certificate or HTTP Basic
- X509 Client Certificate or Form
- X509 Client Certificate and Form
- No advanced authentication

agent_config_object

Indicates which Agent Configuration Object to use.

Example: iplanetdefaultsettings

The following is an example of the file:

```
WEB_SERVER_INFO=;https-server1,/usr/iplanet/servers/https-server1/config,https-se
rver1 (iPlanet
6.0),https-server1,iplanet,6.0,/usr/iplanet/servers/https-host,Unix,+EMPTYSTR+,1,
0,1,0,0,1,HTTP Basic over
SSL,agent1,0,undefined,ENC:6f1I5TLVEpuSBHpf4GrASg==,;https-host2,/usr/iplanet/ser
vers/https-host2/config,https-host2 (Netscape ES
6.0),https-host2,iplanet,6.0,/usr/iplanet/servers/https-iplanetdefaultsettings,+E
MPTYSTR+,+EMPTYSTR+,1,0,0,0,1,No advanced
authentication,host2,0,undefined,ENC:6f1I5TLVEpuSBHpf4GrASg==
```

Configure the Web Server to Restart (Windows Only)

In the section to list Policy Servers for trusted host registration, you can modify the setting in the following table:

Parameter	Description and Sample Value
USER_REQUESTED_RESTART	Allows the installation program to reboot the Windows machine, if required after the configuration process. Set to Yes to allow a reboot. Otherwise, set to No.

Name the Trusted Host Name and Host Configuration Object

In the section for naming the Trusted Host and Host Configuration Object, you can modify the settings in the following table:

Parameter	Description and Sample Value
TRUSTED_HOST_NAME	Names the trusted host. This name must be unique. For example: TRUSTED_HOST_NAME=mytrustedhost
CONFIG_OBJ	Identifies the Host Configuration Object, which defines communication between the trusted host and Policy Server. For example: CONFIG_OBJ=MyHostSettings

Appendix A: Settings Added to the Sun Java System Server Configuration

This section contains the following topics:

Additions for Sun Java System Server 6.0

When you install the Web Agent on an Oracle iPlanet web server 6.0, configuration settings are automatically added to the following files:

- magnus.conf
- obj.conf file
- mime.types

These files load automatically when the web server starts. The additional settings initialize the Web Agent. When the Web Agent installation program adds information to the web server's configuration, it divides this information differently for different versions of the Oracle iPlanet web server.

For Windows platforms, these files are in the *Sun_Java_System_install_location*\servers\https-*hostname*\config\ directory.

For UNIX platforms, these files are in the /usr/*Sun_Java_System_install_location*/servers/https-*hostname*/config/ directory.

Note: The *Sun_Java_System_install_location* is the directory where you installed the Sun Java System server on your computer, and *hostname* is the name of the server.

magnus.conf File Additions for Windows Platforms

The following lines are added to the magnus.conf file on Windows platforms:

```
Init fn="load-modules" shlib="C:/Program Files/ca/webagent/bin/SunOneWebAgent.dll"
funcs="SmInitAgent,SmInitChild,SiteMinderAgent,SmRequireAuth,SmAdvancedAuth"
Init fn=SmInitAgent config="C:/iPlanet/Servers/https-server1/config/WebAgent.conf"
errortext="Error initializing Web Agent..."
Init fn="SmInitChild" LateInit="yes"
```

Note: Some entries in your file may differ slightly from the example shown.

The additional lines instruct the web server to load the SiteMinder Web Agent with the following NSAPI functions:

- SmInitAgent
- SiteMinderAgent
- SmRequireAuth
- SmAdvancedAuth

Code Added to the magnus.conf File on UNIX Platforms

The following lines are added to the magnus.conf file for UNIX platforms:

```
Init fn="load-modules" shlib="/usr/ca/siteminder/agents/bin/libSunOneWebAgent.so"
funcs="SmInitAgent,SmInitChild,SiteMinderAgent,SmRequireAuth,SmAdvancedAuth"
Init fn=SmInitAgent config="/usr/iPlanet/servers/https-yourserver/config/WebAgent.conf"
errortext+"Error initializing Web Agent..."
Init fn="SmInitChild" LateInit=”yes”
```

These lines instruct the web server to load the SiteMinder Web Agent with the following NSAPI functions:

- SmInitAgent
- SmInitChild
- SiteMinderAgent
- SmRequireAuth
- SmAdvancedAuth

obj.conf File Additions for Windows Platforms

When a Web Agent is configured to support an advanced authentication scheme, the Web Agent adds settings to the Sun Java System's obj.conf file. SiteMinder does not remove these settings later if the Agent is reconfigured to support a different advanced authentication scheme. You must manually edit the obj.conf file to remove the settings that are no longer relevant.

Most of the additional lines in the file are added by the Web Agent installation program. Other lines (shown in bold) are added by the servlet engine that you configure for the JSP version of the SiteMinder Password Services.

The lines added by the servlet engine must come before the NameTrans fn functions added by the SiteMinder Web Agent.

In the following example of a modified obj.conf file, smhome represents the installed location of SiteMinder on your system:

Note: Some entries in your file may differ slightly from the example shown.

```
AuthTrans fn="SiteMinderAgent"
NameTrans fn="assign-name" from="*.jsp*" name="myservletengine"
NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"
NameTrans fn="assign-name" from="/siteminderagent/pwservlet/*"
name="servletengine"
NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi"
dir="/smhome/siteminder/webagent/pw" name="cgi"
NameTrans fn="pfx2dir" from="/siteminderagent/pw"
dir="/smhome/siteminder/webagent/pw"
NameTrans fn="pfx2dir" from="/siteminderagent/certoptional"
dir="/smhome/siteminder/webagent/samples"
NameTrans fn="pfx2dir" from="/siteminderagent/jpw"
dir="/smhome/siteminder/webagent/jpw"
NameTrans fn="pfx2dir" from="/siteminderagent"
dir="/smhome/siteminder/webagent/samples"

PathCheck fn="SmRequireAuth"
PathCheck fn="get-client-cert" dorequest="1"
PathCheck fn="get-client-cert" require="0" dorequest="1"

Service method="(GET|POST)" fn="SmAdvancedAuth"
```

The following items describe the content of the lines that are added to the obj.conf file:

- The line that reads AuthTrans fn="SiteMinderAgent" is added to the default object (<Object name="default">). It sets up the SiteMinder Web Agent as the Authorization method, or AuthTrans function, for the Web server.

- The line that reads NameTrans fn="assign-name" from= "/siteminderagent/pwservlet/*" name="myservletengine" is a filter added by the Web Agent that maps the JSP Password Services servlet to the instance of the servlet engine so that engine can process it.
- Most of the lines that begin NameTrans fn="pfx2dir" add virtual directories and mappings for the Agent to support SiteMinder's Password Services (CGI and JSP versions).
- The line that begins NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" is added if you chose to configure a certificate based authentication scheme.
- The line that reads PathCheck fn="SmRequireAuth" is added to any existing PathCheck lines in the default object. It verifies that the user is authorized to perform the requested action on the requested resource.
- The line that reads PathCheck fn="get-client-cert" dorequest="1" is added if, during configuration, you indicated that the Web Agent would support advanced authentication schemes. It supports the use of certificate, certificate plus basic, and certificate and forms authentication schemes.
- The line that reads PathCheck fn="get-client-cert" require="0" dorequest="1" is added if, during configuration you indicated during installation that the Web Agent would support advanced authentication schemes. It supports the use of certificate or basic or the certificate or forms authentication schemes.

  Note: Both PathCheck lines for advanced authentication should be commented out for "Basic Auth over SSL."
- The lines that begin Service method are added to instruct the Web server what to do with the MIME types.
- The lines that read NameTrans fn="assign-name" from="*.jsp*" name="myservletengine" and NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"create mappings for the Agent to support SiteMinder's Password Services.

obj.conf File Additions for UNIX Platforms

When a Web Agent is configured to support an advanced authentication scheme, the Web Agent adds settings to the Sun Java System's obj.conf file. SiteMinder does not remove these settings later if the Agent is reconfigured to support a different advanced authentication scheme. You must manually edit the obj.conf file to remove the settings that are no longer relevant.

Most of the additional lines in the file are added by the Web Agent installation program. Other lines (shown in bold) are added by the servlet engine that you configure for the JSP version of the SiteMinder Password Services.

The lines added by the servlet engine must come before the NameTrans fn functions added by the SiteMinder Web Agent.

In the following example of a modified obj.conf file, smhome represents the installed location of SiteMinder on your system:

Note: Some entries in your file may differ slightly from the example shown.

```
AuthTrans fn="SiteMinderAgent"

NameTrans fn="assign-name" from="*.jsp*" name="myservletengine"
NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"
NameTrans fn="assign-name" from="/siteminderagent/pwservlet/*"
name="servletengine"
NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi"
dir="/smhome/siteminder/webagent/pw" name="cgi"
NameTrans fn="pfx2dir" from="/siteminderagent/pw"
dir="/smhome/siteminder/webagent/pw"
NameTrans fn="pfx2dir" from="/siteminderagent/certoptional"
dir="/smhome/siteminder/webagent/samples"
NameTrans fn="pfx2dir" from="/siteminderagent/jpw"
dir="/smhome/siteminder/webagent/jpw"
NameTrans fn="pfx2dir" from="/siteminderagent"
dir="/smhome/siteminder/webagent/samples"

PathCheck fn="SmRequireAuth"
#SMSSL The line below should be uncommented for "cert" and "cert plus basic" schemes
PathCheck fn="get-client-cert" dorequest="1"
#SMSSL The line below should be uncommented for "cert or basic" or "cert or form"
schemes
PathCheck fn="get-client-cert" require="0" dorequest="1"
#SMSSL Both of the above PathCheck lines should be commented out for "Basic Auth over
SSL"

Service method="(GET|POST)" fn="SmAdvancedAuth"
```

The following items describe the content of the lines that are added to the obj.conf file:

- The line that reads AuthTrans fn="SiteMinderAgent" is added to the default object (<Object name="default">). It sets up the SiteMinder Web Agent as the Authorization method, or AuthTrans function, for the Web server.
- The line that reads NameTrans fn="assign-name" from= "/siteminderagent/pwservlet/*" name="myservletengine" is a filter added by the Web Agent that maps the JSP Password Services servlet to the instance of the servlet engine so that engine can process it.
- Most of the lines that begin NameTrans fn="pfx2dir" add virtual directories and mappings for the Agent to support SiteMinder's Password Services (CGI and JSP versions).
- The line that begins NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" is added if you chose to configure a certificate based authentication scheme.
- The line that reads PathCheck fn="SmRequireAuth" is added to any existing PathCheck lines in the default object. It verifies that the user is authorized to perform the requested action on the requested resource.
- The line that reads PathCheck fn="get-client-cert" dorequest="1" is added if, during configuration, you indicated that the Web Agent would support advanced authentication schemes. It supports the use of certificate, certificate plus basic, and certificate and forms authentication schemes.
- The line that reads PathCheck fn="get-client-cert" require="0" dorequest="1" is added if, during configuration you indicated during installation that the Web Agent would support advanced authentication schemes. It supports the use of certificate or basic or the certificate or forms authentication schemes.

  Note: Both PathCheck lines for advanced authentication should be commented out for "Basic Auth over SSL."
- The lines that begin Service method are added to instruct the Web server what to do with the MIME types.

mime.types File Additions for Windows and UNIX Platforms

The following lines are added to the mime.types file by the setup program:

```
type=magnus-internal/sfcc exts=sfcc
type=magnus-internal/fcc exts=fcc
type=magnus-internal/scc exts=scc
type=magnus-internal/ccc exts=ccc
```

These lines set up the mime types to support advanced SiteMinder features.

Check Agent Start-up with LLAWP

You can see if the Web Agent is starting up properly by starting the LLAWP process.

To start the LLAWP process

1. Ensure you have configured the Web Agent with the Configuration Wizard.
2. Open a console window and enter the following command:

   LLAWP *path_to_WebAgent.conf* **-***web_server_type*

   Note: Replace web_server_type with one of the following abbreviations:

   - APACHE20
   - APACHE22
   - ISAPI60
   - SPS60
   - SUNONE

   path_to_WebAgent.conf can be a full path or a relative path from the location where you are running LLAWP. For example:

   - Windows:

     LLAWP "C:\Program Files\ca\Siteminder Web Agent\Bin\IIS\WebAgent.conf" -ISAPI60

   - UNIX:

     LLAWP /usr/apache/conf/WebAgent.conf -APACHE20

   Note: If you start the LLAWP from the command line, you must also shut it down from the command line.

Appendix B: Configuration Changes to Web Servers with Apache Web Agent

This appendix lists changes made automatically by running the Web Agent Configuration Wizard to configure an Apache Web Agent. These changes apply to all web servers that support the Apache Web Agent, including Apache 2.0, IBM HTTP Server, and the HP Apache web server.

This section contains the following topics:

Set the Library Path Variable on UNIX or Linux Systems

Set the library path variable on UNIX or Linux systems before running the agent configuration program.

The following table lists the library path variables for the various UNIX and Linux operating environments:

Operating System	Name of Library Path Variable
AIX	LIBPATH
Linux	LD_LIBRARY_PATH
Solaris	LD_LIBRARY_PATH

Set the value of the library path variable to the *web_agent_home*/bin directory.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (UNIX/Linux installations): /opt/ca/webagent

Changes to the httpd.conf File

The Configuration Wizard modifies the httpd.conf configuration file to enable the web server to operate with the Apache Web Agent.

The examples in this procedure are for UNIX platforms; however the same changes are made to Windows platforms using the appropriate Windows syntax.

web_agent_home

Indicates the directory where the SiteMinder Agent is installed.

Default (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent

Default (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

Default (UNIX/Linux installations): /opt/ca/webagent

For most Apache-based web servers, this file is located in the conf directory:

Apache_home/conf

Note: For more information about the location of this file, see the documentation provided by the vendor of your web server.

Entries Added to DSO Support Section

The following line(s) are added to the Dynamic Shared Object (DSO) Support configuration section, which precedes the Main server configuration section of the file.

LoadModule Entries Added

The SiteMinder Agent requires one of the following modules in order to load:

Apache 2.0

LoadModule sm_module *web_agent_home*/bin/libmod_sm20.so

Apache 2.0 running on Windows

LoadModule sm_module *web_agent_home*/bin/mod_sm20.dll

Apache 2.2 running on Windows

LoadModule sm_module web_agent_home/bin/mod_sm22.dll

mod_sm.c Entry Added to ClearModuleList

If the directive ClearModuleList exists in the DSO configuration section, the mod_sm.c entry is placed at the end of the AddModule section of the file, as shown in bold:

ClearModuleList

AddModule mod_env.c

.

.

.

AddModule mod_servletexec.c

#Siteminder

AddModule mod_sm.c

SmInitFile Entry Added

In the Main server section of the file, the SmInitFile entry is added:

SmInitFile *Apache_home*/conf/WebAgent.conf

This entry is placed after the LoadModule entry. A full path is used, not a relative path. For example:

SmInitFile "/export/Apache2/conf/WebAgent.conf"

Alias Entries Added

In the Aliases section of the file, entries are added to enable SiteMinder features.

Note the following:

- The Alias /siteminderagent/ "*web_agent_home*/samples/" entry must come **after** all other aliases in the Aliases section.
- For SiteMinder to use Basic over SSL or X.509 certificate-based authentication schemes with an Apache Web Agent, SSL must be enabled by compiling the Apache server to include the mod_ssl module. To obtain this module, see www.modssl.org.
- Each alias entry appears on its own line.

Password Services

```
Alias /siteminderagent/pwcgi/ "<web_agent_home/pw/>"
 <Directory "/export/webagent/pw/">
   Options Indexes MultiViews ExecCGI
   AllowOverride None
   Order allow,deny
   Allow from all
 </Directory>

Alias /siteminderagent/pw/ "<web_agent_home>/pw/"
 <Directory "/export/webagent/pw/">
   Options Indexes MultiViews ExecCGI
   AllowOverride None
   Order allow,deny
   Allow from all
 </Directory>
```

Basic over SSL authentication

```
AliasMatch /siteminderagent/nocert/[0-9]+/(.*)
 "<web_agent_home>/$1"
 <Directory "<web_agent_home>/$1">
   Options Indexes MultiViews
   AllowOverride None
   Order allow,deny
   Allow from all
 </Directory>
```

X509 Client Cert or X509 Client Cert and Basic authentication

```
AliasMatch /siteminderagent/cert/[0-9]+/(.*)
"<web_agent_home>/$1"
 <Directory "<web_agent_home>/$1">
   Options Indexes
   AllowOverride None
   Order allow,deny
   Allow from all
```

```
</Directory>
```

X509 Client Cert or Basic authentication

```
AliasMatch /siteminderagent/certoptional/[0-9]+/(.*) "<web_agent_home>/$1"
  <Directory "<web_agent_home>/$1"
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
  </Directory>
```

X509 Certificate or Form or X509 Client Cert and Form authentication

```
Alias /siteminderagent/certoptional/"<web_agent_home>/
   samples/"
  <Directory "<web_agent_home>/samples/"
    Options Indexes
    AllowOverride None
    Order allow,deny
    Allow from all
  </Directory>
```

Forms authentication or Agent is cookie provider for single sign-on

```
 Alias /siteminderagent/ “<web_agent_home>/samples/”
  <Directory "/export/webagent/samples/">
    Options Indexes MultiViews
    AllowOverride None
    Order allow,deny
    Allow from all
  </Directory>
```

Note: This is the alias that should be placed at the end of the section.

Certificate Authentication Entries Added

- If you are using X509 Client Cert, X509 Client Cert and Basic, or X509 Client Cert or Basic authentication, the following SSL Engine Options entry in the Virtual Hosts section is uncommented for the appropriate virtual host (if multiple hosts are defined):

  SSLOptions +ExportCertData +StdEnvVars

  Note: If there is an existing SSL option in the Virtual Hosts section, then that existing entry is commented out and the new SSL entry is added.

- If you are using X509 Client Cert or Forms authentication, the following SSL Engine Options entry in the Virtual Hosts section is uncomment for the appropriate virtual host (if multiple hosts are defined):

  SSLOptions +StdEnvVars +CompatEnvVars

- In the Virtual Hosts section of the file, the SSL Client Authentication type is set it to optional:

  SSLVerifyClient optional

Appendix C: Environment Variables Added or Modified by the Web Agent Installation

This section contains the following topics:

Added or Modified Environment Variables

The following environment variables are added or modified by the Web Agent installation:

- NETE_WA_ROOT = $INSTALL_PATH$
- NETE_WA_PATH = $INSTALL_PATH$$/$bin

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X