CA SiteMinder®

Web Agent Installation Guide

r6.x QMR6

Second Edition

CA Product References

This document references the following CA products:

- SiteMinder®
- TransactionMinder®
- Identity Manager

Contact CA

Contact CA Support

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

- 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

Provide Feedback

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

If you would like to provide feedback about CA product documentation, complete our short customer survey, which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Preparation 13

Chapter 1: Preparation

This section contains the following topics:

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. Ensure you have an account with one of the following for your web server:
      - Administrative privileges (for Windows systems).
      - Root privileges (for UNIX systems).
   b. Confirm that the operating system has the proper service packs or patches installed.
   c. 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 19).
2. Confirm the following items for all Web Agent installations:
   - Ensure the Policy Server is installed and configured (see page 22).
   - Gather the information needed to complete the Web Agent installation (see page 22).
   - Preserve the changes in your WebAgentTrace.conf file (see page 23).
   - Select the correct Agent for your web server (see page 23).
3. (Optional) Meet the prerequisites for password services (see page 23).
4. (Optional) Meet the prerequisites for registration services (see page 24).

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 r6.0 SP6 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, you may need to perform one or more of the following tasks, as required by your environment:

- If you are installing a Web Agent on a 64-bit Windows platform, you must install the Visual C++ 2005 Redistributable package (see page 14) first.
- Install an Apache web server as a service for all users (see page 16).

Microsoft Visual C++ 2005 Redistributable Package (x64) Prerequisite

Before installing an r6.0 SP6 Web Agent on a Windows 64-bit platform, you must download and install the Microsoft Visual C++ 2005 Redistributable Package (x64). Go to the Microsoft downloads page, and then search for "Microsoft Visual C++ 2005 Redistributable Package (x64)."

How to Use a Non-Default IIS Website

SiteMinder requires the default IIS web site for proper installation. By default, this site exists when you install an IIS web server. If any of the following conditions exist, edit the Metabase before configuring a SiteMinder IIS Web Agent :

- If the default IIS website no longer exists.
- If the default IIS website has been renamed.
- If you want to install the SiteMinder virtual directories on a different (non-default) IIS website.

The actual tools and steps involved in editing the Metabase depend on the version of IIS you are using. For example, if you are using an r6.0 SP6 SiteMinder Web Agent, on IIS 6.0, you would edit the Metabase using the following process:

Note: For more information, see your Microsoft documentation, or go to http://support.microsoft.com/

1. Download and install the Metabase Explorer from Microsoft by doing the following:
   a. Go to the Microsoft Downloads website.
   b. Search for "IIS 6.0 Resource Kit Tools," which includes the Metabase Explorer.
   c. Download and install the tools.
   d. Create a backup copy of your metabase.xml file.
2. On your IIS web server, open the IIS Manager. Find the website on which you want to install the SiteMinder Web Agent, and note its identifier (number) for future reference.
3. Close the IIS Manager, and open the Metabase Explorer.
4. Expand the following key:

   `LM\W3SVC\`
5. Expand the key that corresponds to the identifier from Step 2.

   A list of sub keys appears.
6. Right-click the key from Step 5, select Rename, and then change the value of the key to 1.
7. From the list of sub keys in the left pane, expand the following key:

   `root`

   A list of keys appears in the right pane of the Metabase Explorer.
8. Double-click the following key:

   `AppRoot`

   The AppRoot Properties dialog appears. The Value Data field shows the following string:

   `/LM/W3SVC/`*`identifier_number`*`/Root`
9. Change the value of the *identifier_number* to 1, and then click OK.
10. Close the Metabase Explorer.
11. Run the Configuration Wizard to reconfigure your IIS Web Agent.
12. Repeat Steps 3 through 10, but change the number 1 back to the original identifier from in Step 2.
13. Restart the IIS web server.

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

The Web Agent Configuration Wizard will not detect a valid Apache installation if the Apache web server is installed for an individual user.

When you install an Apache web server, select the option to "install as a service, available for all users " so during configuration, the SiteMinder Web Agent can detect the existing web server on a user's system.

Installing the Apache Web Server with the option "manual start, for current user only" allows the Web Agent to be installed; however, because the Configuration Wizard cannot detect the Apache web server, the Web Agent cannot be configured for the server.

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 17)
   - Required Solaris patches

Set the DISPLAY For Web Agent Installations on UNIX

If you are installing the Web 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 Web Agent using the console mode installation, which does not require the X window display mode.

More Information

Run a Console Mode Installation on UNIX (see page 52)

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

Required HP-UX Patches

Before installing a Web Agent on an HP-UX 11i machine, you must install the patches listed in the table that follows. You can check the patch list by logging in as root and executing the swlist command.

HP-UX Release	Patch
HP-UX 11i v1	■ PHCO_29029 is recommended for SiteMinder 6.0.4 and SiteMinder 6.0.5.
HP-UX 11i v1	■ PHSS_26560 ld and linker cumulative patch

Required Solaris Patches

Before installing a Web Agent on a Solaris machine, you must install the patches listed in the table that follows. You can check on patch versions by logging in as root and executing the following command:

'showrev -p | grep *patchid*'

To locate Solaris patches, go to Sun Microsystems Solution Center.

Solaris Release	Patch
Solaris 8	■ 108434-22 (need this patch to avoid a runtime issue with Web Agent installation binaries)

Solaris Release	Patch
Solaris 9	■ 111711-16 (need this patch to avoid a runtime issue with Web Agent installation binaries)
Solaris 10	■ 119963-08 (need this patch to avoid a runtime issue with Web Agent installation binaries)

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 Linux release 2.1

glibc-2.4.2-32.20 for Linux Application Server 2.1

Required Linux Libraries

When installing a Red Hat Enterprise Linux version of a Web Agent, the following are required libraries:

- On Red Hat Enterprise Linux 2.1, if using the "linux" kit (the kit built with GCC 2.96), there are no libraries required that are not part of a basic installation.
- On Red Hat Enterprise Linux 3.0, use the "rhel30" kit (the kit built with GCC 3.2), and there are no libraries required that are not part of a basic installation.
- On Red Hat Enterprise Linux 4.0, use the "rhel30" kit (the kit built with GCC 3.2). The following is required:
  - compat-libstdc++-33-3.2.3-*patch_version*.i386.rpm
  - compat-gcc-32-c++-3.2.3-47.3-*patch_version*.i386.rpm

Linux Tools Required

Before installing a SiteMinder Web 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 Web 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.

To compile Apache on Linux for the Web Agent

1. Enter the following:

   LIBS=-lpthread

   export LIBS

2. Configure Apache as usual by entering the folloiwng:

   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 20)

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 Apache Web Agents, 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 Web 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 Web 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.

Policy Server Requirements

Before you install the Web Agent, the Policy Server must be installed, configured and able to communicate with the system where you plan to install the Web Agent.

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

You must configure Policy Server with 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 Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the privilege to register trusted hosts.

- Agent identity

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

- Host Configuration Object

  This object resides on the Policy Server and defines the communication between the Web Agent and the Policy Server after the initial connection between the two is made.

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

  Do not confuse this object with the trusted host's configuration file, SmHost.conf, which is installed on the trusted host after a successful host registration. The settings in the SmHost.conf file enable the Web Agent to connect to a Policy Server for the first connection only. Subsequent connections are governed by the Host Configuration Object.

- Agent Configuration Object

  This object includes the parameters that define the Web Agent configuration. The required parameters vary according to the type of web server that is hosting your Web Agent.

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 r6.0 SP6 Platform Support Matrix.

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.

   a. 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.

Prepare for Registration Services (Optional)

The following sections discuss prerequisites and guidelines for registration services.

Use Registration Services

The SiteMinder Web Agent includes Registration Services. Registration Services is a subset of the DMS product, but you can use it without a DMS license.

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

To continue using your existing DMS application with r6.0 SP6 do not install Registration Services when you install the r6.0 SP6 Web Agent, as shown in the following table.

If...	Then...
■ You have DMS 2.01 ■ You install r6.0 SP6 with SiteMinder SM r6.0 SP6	you can continue running DMS 2.0
■ You have DMS 2.01 ■ You install r6.0 SP6 with SM 6.0 SP 4	apply DMS 2.01 Hot Fix CR5 before you continue running DMS 2.01

Install a Servlet Engine for Registration Services (Optional)

If you want the Agent to provide Registration Services, you must install a supported servlet engine. For a list of supported servlet engines, go to Technical Support, and then search for the SiteMinder r6.0 SP6 Platform Support Matrix.

Use Active Directory for Registration Services (Windows Only)

If you want to use Active Directory with Registration Services, check that:

- Windows 2000, including Active Directory, is operational
- Microsoft's Certificate Server is configured for Active Directory
- Active Directory's Root Certificate is accessible from a browser

Note: For information about configuring Active Directory, see the *DMS 2.01 Release Notes.* To find this document, go to Technical Support, and search for the *DMS 2.01 Release Notes*.

Modify the DMS Admin Password for Registration Services

The DMS Administrator is a SiteMinder administrator with Manage User privileges. The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as:

- Self-registration
- Calls against the SiteMinder policy store, such as searching for roles
- Establishing an Organization Administrator's scope

The DMS Administrator account includes a user name and an encrypted password, which are stored in the Web Agent's dms.properties file. This name and password must match the DMS Admin user name and password set at the Policy Server.

During the Web Agent installation, you are prompted for the DMS administrator's password. To change the password, you have to modify the dms.properties file, and also modify the DMS Admin properties in the Policy Server User Interface.

At the Web Agent:

1. Navigate to the bin directory where DMS is installed—for example:
   - Windows: C:\Program Files\netegrity\webagent\bin
   - UNIX: export/smuser/netegrity/webagent/bin
2. Execute the following command:
   - Windows:

     dmsencryptkey -path "*DMS_home*\properties\dms.properties" -password *new_password*
   - UNIX:

     dmsencryptkey -path "*DMS_home*/properties/dms.properties" -password *new_password*

     where *DMS_home* is the installed location of DMS and *new_password* is the password that you want to specify.

At the Policy Server:

1. Access the Policy Server User Interface.
2. Select the System tab, then click Administrators.
3. In the right pane, double-click DMSAdmin.
4. SiteMinder displays the Administrator Properties dialog box.
5. In the Password group box, enter the new password in the User Password and Confirm Password fields.
6. Click OK.

Modify the ServletExecAS Startup Script to Run Registration Services with ServletExecAS (UNIX only)

If you are using Registration Services with ServletExecAS you must modify the StartServletExec script.

To modify the StartServletExec script

1. Open the StartServletExec script with a text editor. See the ServletExecAS documentation for the exact location of this script.

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

2. Extend the CLASSPATH definition by adding the entries in boldface to the end of the CLASSPATH:

   Note: Your specific entries may vary from the ones shown in this procedure. Replace /export/smuser/netegrity/siteminder/webagent with the actual Web Agent installation path.

   ```
   CLASSPATH=${NA_ROOT}/lib/ServletExec41.jar:${NA_ROOT}/lib/servlet.jar:${NA_ROOT}/lib/tools.jar:${NA_ROOT}/lib/jaxp.jar:${NA_ROOT}/lib/crimson.jar:${NA_ROOT}/lib/jndi.jar:${NA_ROOT}/se-${SEINSTANCE}/classes:/export/smuser/netegrity/siteminder/webagent/java/dms.jar:/export/smuser/netegrity/siteminder/webagent/java/smjavasdk2.jar:/export/smuser/netegrity/siteminder/webagent/java/env.jar:/export/smuser/netegrity/siteminder/webagent/java/jsafe.jar:/export/smuser/netegrity/siteminder/webagent/java/smjavaagentapi.jar:/export/smuser/netegrity/siteminder/webagent/java:/export/smuser/netegrity/siteminder/webagent/samples:/export/smuser/netegrity/siteminder/webagent/samples/properties:/export/smuser/netegrity/siteminder/webagent:/usr/iplanet/servers/myserver.example.com/config
   ```

   In this CLASSPATH entry, replace:

   - /usr/iplanet/servers with the actual server installation directory
   - myserver.example.com with the actual server instance where ServletExec is installed
   - /export/smuser/netegrity/siteminder/webagent/ with the actual SiteMinder Web Agent installation directory

3. Extend the document directories definition by adding the entry in bold:

   ```
   $SENAME $HOMEDIR $MIMEFILE $DOCROOTDIR  -port $PORT $SEOPTS -addl "/siteminderagent/dmspages=/export/smuser/netegrity/siteminder/webagent/samples/dmspages""
   ```

   Note: There are two double-quotes at the end of the definition.

4. Set the library path variable to point to *web_agent_home*/bin—for example:

   ```
   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/export/smuser/netegrity/siteminder/webagent/bin; export LD_LIBRARY_PATH
   ```

   The library path variable depends on the operating system. The following table lists the variables.

Operating System	Path Variable
Solaris	LD_LIBRARY_PATH
HP-UX	SHLIB_PATH
LINUX	LD_LIBRARY_PATH
AIX	LIBPATH

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:

   nete-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\netegrity\webagent

  Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

- 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 58)
Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server (see page 91)
Configure an Oracle iPlanet Web Agent (see page 133)
Configure an Apache Web Agent (see page 145)
Configure a Domino Web Agent (see page 155)
How to Configure a SiteMinder Web Agent on IIS 6.0 (see page 115)

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 nete-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 nete-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 nete-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.

More Information

Set Up the nete-wa-installer.properties File (see page 229)

Run an Unattended Installation on Windows

You should have completed an initial Web Agent installation and, if necessary, modified the nete-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. nete-wa-*version*-win32.exe (Agent executable) from where it resides on your system.
   b. nete-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. For more information, see the release notes for your SiteMinder component.
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:

   nete-wa-<*version*>-win32.exe -f nete-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 a SiteMinder Web Agent on IIS 6.0 (see page 115)
How to Configure Any Web Agent in Unattended Mode (see page 183)

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:
   - nete-wa-*version*-win.exe
   - wa_install.exe

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\netegrity\install-info\nete-install-history.log

UNIX

user_home_directory/netegrity/install-info/nete-install-history.log

More information:

Installation and Configuration Log Files (see page 39)

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 30)

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. 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 created successfully, the client computer becomes a trusted host.

You can register a trusted host immediately after installing the Web Agent or at a later time; however, the host must be registered to communicate with the Policy Server.

Note: You only register a system as a trusted host *once*, not each time you install and configure a Web Agent. If the Web Agent Configuration Wizard detects that a trusted host has been registered on that system previously, a warning appears.

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.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into 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 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. Do *not* select the following check box (SiteMinder r6.0 SP6 does *not* support this feature):

      `Enable PKCS11 DLL Cryptographic Hardware`

   c. 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. 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.

   Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

   - For Windows installations, the default location is C:\Program Files\netegrity\webagent
   - For UNIX installations, the default location is user_home_directory/netegrity/webagent
   - For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

7. Click Continue.

8. Continue with the configuration by doing the following appropriate tasks:

   - Configure an IIS Web Agent
   - Configure a Sun Java System Web Agent
   - Configure an Apache Web Agent
   - Configure a Domino Web Agent

More Information

Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server (see page 91)
Configure an Oracle iPlanet Web Agent (see page 133)
Configure an Apache Web Agent (see page 145)
Configure a Domino Web Agent (see page 155)
Modify the SmHost.conf File (UNIX) (see page 62)

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:

nete-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 34)

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 Policy Server User Interface.

   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 Policy Server User Interface.
- 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.

Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

- For Windows installations, the default location is C:\Program Files\netegrity\webagent
- For UNIX installations, the default location is user_home_directory/netegrity/webagent
- For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

To re-register a trusted host using the registration tool

1. Open a command prompt window.

   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. For more information, see the release notes for your SiteMinder component.

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: Put a space between each command argument and its value, as shown in the following

example:

```
smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn hostA
-hc DefaultHostSettings
```

The following example contains the -o argument:

```
smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn hostA
-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 servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:

"*policy_server_ip_address*,5555,5555,5555"

Example: 127.0.0.1,44442

-u *administrator_username*

Indicates 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 Policy Server User Interface.

-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.

-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 backups up the original and adds a .bk extension to the backup file name.

-o

Overwrites an existing trusted host. If you do *not* use this argument, you will have to delete the existing trusted host with the Policy Server User Interface 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, even if you are logged into 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. For more information, see the release notes for your SiteMinder component.

More Information

Re-register a Trusted Host Using the Registration Tool (Windows) (see page 42)

Registration Services Installed Files (Windows)

The Web Agent installation installs a number of virtual and physical directories for Registration Services:

Virtual Directories

- siteminderagent\dmspages
- siteminderagent\dmsforms

You can view these directories using the Internet Services Manager and looking at the Default Web Site for your server.

Physical Directories

The Web Agent installation puts the Registration Services sub-directories in:

- *web_agent_home*\samples

  Contains files used by Registration Services that you can customize.

- *web_agent_home*\samples_default

  Contains backup files for Registration Services. Do not modify these files.

The following table describes each Registration Service Directory:

Directory	Description
dmspages	Contains JSPs and JavaScript used in Registration Services pages. This directory includes files that support Registration Services in hierarchical and flat user directory structures.
dmsforms	Contains .fcc files, which collect user credentials.
properties	Contains the directories: ■ Default—Contains properties files for configuring a hierarchical directory structure ■ Default_attr-based—Contains properties files for configuring a flat directory structures

Fix the ServletExec CLASSPATH for DMS

If you install DMS on a Windows system and get 'servlet DMS not found' errors when you access a DMS page, 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.

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

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*/netegrity_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:

   - nete-wa-*version-operating_system*.bin (for most versions)
   - nete-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 nete-wa-*version-operating_system*.bin
4. From a console window, run the documentation installation using one of the following commands:

   GUI mode:

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

   Console mode:

   ./nete-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 r6.0 SP6 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 20)
Environment Variables Added or Modified by the Web Agent Installation (see page 253)

Run a GUI Mode Installation on UNIX

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

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:
   - nete-wa-*version-operating_system*.bin (for most versions)
   - nete-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 nete-wa-*version-operating_system-processor-architecture*.bin
8. Open a console window and from the local installation directory enter:

   ./nete-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

Register Your System as a Trusted Host on UNIX (see page 58)
Configurations Available for All Web Agents (see page 183)

Run a Console Mode Installation on UNIX

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

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.

   Download the installation programs from Technical Support. Go to the folder for your operating system and download the installation file.
3. Copy the appropriate binary file to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:

   - nete-wa-*version-operating_system*.bin (for most versions)
   - nete-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
4. 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 nete-wa-*version-operating_system*.bin
5. At the command prompt, start the console mode installation by entering:

   ./nete-wa-*version-operating_system*.bin

   - -i console

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

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

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

   Press Enter to page through the notes and continue through the installation.
10. 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/netegrity/wa, the path becomes export/netegrity/wa/webagent. However, if you specify export/netegrity/sm_webagent as the path, the installation program will accept this.

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

More Information

Register Your System as a Trusted Host on Windows (see page 36)
Configurations Available for All Web Agents (see page 183)

Set the Web Agent Environment Variables After Installation

You can set the Web Agent environment variables after installing the Web Agent using the nete_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 nete_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:

```
. ./nete_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

If you run your Apache server using the apachectl script (such as when running an Apache web server on POSIX), add a line to the apachectl script to set the environment variables for the SiteMinder Web Agent.

To set the web agent variables when using apachectl script on Apache servers

1. Locate a line resembling the following example:

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

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

   ```
   sh /web_agent_home/nete_wa_env.sh
   ```

   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\netegrity\webagent

   Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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 nete-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 nete-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 nete-wa-installer.properties file

1. Run an initial installation of the Web Agent.
2. Open the nete-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.

More Information

Run a GUI Mode Installation on UNIX (see page 50)
Set Up the nete-wa-installer.properties File (see page 229)

Run an Unattended Installation on UNIX

You should have completed an initial Web Agent installation and, if necessary, modified the nete-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. nete-wa-*version-operating_system*.bin (Agent executable) from where it resides on your system.
   b. Copy the nete-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:

   ./nete-wa-*version-operating_system*.bin -f nete-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 183)

Stop an Unattended Installation in Progress on UNIX

To manually stop the installation, press Ctrl + C.

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\netegrity\install-info\nete-install-history.log

UNIX

user_home_directory/netegrity/install-info/nete-install-history.log

More information:

Installation and Configuration Log Files (see page 39)

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)

More Information

Run a GUI Mode Installation on UNIX (see page 50)
Run a Console Mode Installation on UNIX (see page 52)

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

Re-register a Trusted Host Using the Registration Tool (Windows) (see page 42)
How to Configure Any Web Agent in Unattended Mode (see page 183)

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: ./nete-wa-config.bin

      Console Mode: ./nete-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. Do *not* select the following check box (SiteMinder r6.0 SP6 does *not* support this feature):

      `Enable PKCS11 DLL Cryptographic Hardware`

   c. Click Next.
3. 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 Sun Java System 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.

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 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.

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 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.

6. 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.

7. Configure your Web Agent.

More Information

Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server (see page 91)
Configure an Oracle iPlanet Web Agent (see page 133)
Configure an Apache Web Agent (see page 145)
Modify the SmHost.conf File (UNIX) (see page 62)

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:

nete-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 34)

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 Policy Server User Interface.

   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 Policy Server User Interface.
- 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.

Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

- For Windows installations, the default location is C:\Program Files\netegrity\webagent
- For UNIX installations, the default location is user_home_directory/netegrity/webagent
- For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

To re-register a trusted host using the registration tool

Open a command prompt window.

1. Ensure that the library path environment variable contains the path to the Web Agent's bin directory.
2. 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/netegrity/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

3. 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: There should be a space between each command argument and its value.

   Example:

   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn hostA
   -hc DefaultHostSettings

   Example with the -o argument:

   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn hostA
   -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 servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:

   "*policy_server_ip_address*,5555,5555,5555"

   Example: 127.0.0.1,44442

   -u *administrator_username*

   Indicates 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 Policy Server User Interface.

-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.

-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 backups up the original and adds a .bk extension to the backup file name.

-o

Overwrites an existing trusted host. If you do *not* use this argument, you will have to delete the existing trusted host with the Policy Server User Interface 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.

More Information

Re-register a Trusted Host Using the Registration Tool (UNIX) (see page 64)

Files Installed for Registration Services (UNIX)

The Web Agent installation installs a number of virtual and physical directories for Registration Services:

Virtual Directories

- siteminderagent/dmspages
- siteminderagent/dmsforms

You can view these directories using the Internet Services Manager and looking at the Default website for your server.

Physical Directories

The Web Agent installation puts the Registration Services sub-directories in the following locations:

- *web_agent_home*/samples

  Contains files used by Registration Services that you can customize.

- *web_agent_home*/samples_default

  Contains backup files for Registration Services. Do not modify these files.

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

The following table describes each directory.

Directory	Description

Directory	Description
dmspages	Contains JSPs and JavaScript used in Registration Services pages. This directory includes files that support Registration Services in hierarchical and flat user directory structures.
dmsforms	Contains .fcc files, which collect user credentials.
properties	Contains the directories: ■ Default—Contains properties files for configuring a hierarchical directory structure ■ Default_attr-based—Contains properties files for configuring a flat directory structures

Chapter 4: Install a Web Agent on z/OS

This section contains the following topics:

Run a Console-mode Installation on z/OS

You can install the SiteMinder Web Agent on a z/OS system using the console-mode installation option.

To run a console-mode installation

1. Set the path of the JRE in the PATH environment variable.

   For example:

   export PATH=$PATH:*path_to_the_ Java/bin_directory*

2. Execute the installer JAR after setting the Java path as shown with the following command:

   ```
   java -jar  nete-wa-install.jar -i console
   ```

   The installation starts in Console mode.

3. Follow the instructions in the wizard.

4. After installing the Web Agent, run the Agent Configuration Wizard to do the following tasks:

   - Register a trusted host
   - Configure the web agent

More information:

How to Configure a Web Agent on z/OS (see page 169)

Run a GUI-mode Installation on z/OS

You can install the SiteMinder Web Agent on a z/OS system using a GUI.

Note: An X11-based system is required to use the GUI mode.

To run a GUI mode installation

1. Set the path of the JRE in the PATH environment variable.

   For example:

   export PATH=$PATH: *path_to_the_Java/bin_directory*

2. Set the DISPLAY variable.

   For example:

   export DISPLAY=*IP_address_of_the_computer_from_which_telnet_is_done*:0.0, for example:

   export DISPLAY=138.42.191.42:0.0.

3. Execute the installer JAR after setting the Java path as shown in the following command:

   ```
   java -jar  nete-wa-install.jar
   ```

   The installation wizard starts in GUI mode.

4. Follow the instructions in the wizard.

5. After installing the Web Agent, run the Agent Configuration Wizard to do the following tasks:

   - Register a trusted host
   - Configure the web agent

More information:

How to Configure a Web Agent on z/OS (see page 169)

Location of Web Agent Version Information

For the z/OS platform, the Web agent installer creates a webroots.conf file in the *web_agent_home* directory.

Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

- For Windows installations, the default location is C:\Program Files\netegrity\webagent
- For UNIX installations, the default location is user_home_directory/netegrity/webagent
- For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

The webroots.conf file holds the SiteMinder version information after the agent is successfully installed and configured. The information in the file is updated as users upgrade and configure the agent to work with web servers.

The following is an example of the webroots.conf file:

```
SiteMinder Version=6QMR6
Hotfix=3
LastRegLevel=6QMR6
HostConfigFile=/siteminder/v6/webagent/config/SmHost.conf
```

Chapter 5: Upgrade a Web Agent to r6.0 SP6

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 *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. If you are upgrading a Web Agent from r4.x to r6.x, review the differences in cookie provider redirections.
7. 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.

Cookie Provider Redirection Differences Between 4.x and 6.x Agents

6.x Web Agents redirect to the cookie provider on GET and POST actions, whereas 4.x Web Agents redirect to the cookie provider only on GET actions. This functional difference causes upgrade issues when applications that require cookie provider support for GET actions and Web services responding to POST actions are installed on IIS virtual servers.

All traditional 6.x Web Agents (*not* the framework agents) have been modified to redirect to the cookie provider only for GET actions. New and rearchitected framework agents continue to redirect to the cookie provider for GET and POST actions so Web Agents can support POST preservation when a cookie provider is enabled.

Note: For more information on Framework agents, see the *Web Agent Guide*.

Web service applications or any custom application that cannot interpret 302 redirects should be configured separately from applications requiring multi-cookie domain single sign-on. Clients using Web services should consider moving these applications to servers separate from their other applications that require multi-cookie domain single sign-on.

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.

Manual Upgrade from 4.x QMR x Japanese Web Agents Required

SiteMinder r6.0 SP6 does not include automated upgrades for 4.x QMR x Japanese Web Agents to r6.0 SP6. You are required to perform manual upgrades by uninstalling earlier versions of the product and then installing the r6.0 SP6 version.

Upgrade a 5.x Web Agent to 6.x on Windows Systems

The SiteMinder Web Agent r6.0 SP6 installation media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 5.x QMR 4
- 5.x QMR 5
- 5.x QMR 6
- 5.x QMR 7
- 5.x QMR 8

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.

You can upgrade if you have applied a hotfix to any of these releases.

Be aware of 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 the system with the 5.x Web Agent being upgraded has not previously been registered as a trusted host, you will be prompted to register at this time.
- If you are installing an Agent on an Sun Java System 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

Exit all applications that are running and stop the web server.

1. Insert the SiteMinder DVD or download the installation program from the Technical Support web site.
2. Navigate to the win32 folder and double-click nete-wa-6qmr6-win32.exe.

   The program prepares the files.
3. In the Introduction dialog box, read the information then click Next.
4. Read the License Agreement select the radio button to accept the agreement then click Next.
5. Read the notes in the Important Information dialog box, then click Next.
6. Select the placement of the Agent Configuration Wizard shortcut in the Choose Shortcut Folder dialog box then click Next.

Note: To allow all users access to the Configuration Wizard via the shortcut, ensure the Create Icons for All Users check box is checked. Otherwise, deselect this option.

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

7. In the Confirm Upgrade dialog box, select one of the following then click Next:
   - Continue with the upgrade—upgrades the Web Agent to 6.x.
   - Abort the upgrade—exits the upgrade procedure without upgrading the Web Agent.
8. In the Pre-installation Summary dialog box, confirm that the installation settings are correct, and 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. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.
9. In the Install Complete dialog box, choose whether to restart your system immediately or later, and then click Done.

More Information

Register Your System as a Trusted Host on UNIX (see page 58)

Upgrade a 6.x Web Agent to r6.0 SP6 on Windows Systems

The SiteMinder Web Agent r6.0 SP6 installation media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 6.06.x QMR 4
- 6.x QMR 1
- 6.x QMR 2
- 6.x QMR 3
- 6.x QMR 4
- 6.x QMR 5

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.

You can upgrade if you have applied a hotfix to any of these releases.

Be aware of 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 Sun Java System 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. Insert the SiteMinder media or download the installation program from the Technical Support web site.
3. Navigate to the win32 folder and double-click nete-wa-6qmr6-win32.exe.

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

   The program prepares the files.
4. In the Introduction dialog box, read the information then click Next.
5. Read the License Agreement select the radio button to accept the agreement 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, ensure the Create Icons for All Users check box is checked. Otherwise, deselect this option.

   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 6.x.
   - 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 by running the Web Agent Configuration Wizard.

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

More information:

Reconfigure a Web Agent (see page 186)

Upgrade a 4.x Web Agent to 6.x on Windows Systems

The SiteMinder Web Agent r6.0 SP6 installation media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 4.x QMR 5
- 4.x QMR 6

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.

You can upgrade if you have applied a hotfix to any of these releases.

Note: When upgrade from a 4.x Web Agent to a r6.0 SP6 Web Agent you can implement central agent configuration. However, this requires that you migrate the configuration settings in the 4.x WebAgent.conf file to an Agent Configuration Object on the Policy Server. See the *Upgrade Guide* for further instructions.

To upgrade Web Agents on Windows

1. Exit all applications that are running and stop the web server.
2. Insert the SiteMinder DVD or download the installation program from Technical Support.
3. Navigate to the win32 folder and double-click nete-wa-6qmr6-win32.exe.
4. In the Introduction dialog box, read the information then click Next.
5. Read the License Agreement select the radio button to accept the agreement 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.
8. To allow all users access to the Configuration Wizard via the shortcut, ensure the Create Icons for All Users check box is checked. Otherwise, deselect this option.

   The upgrade program locates the existing 4.x Web Agent and displays the Confirm Upgrade dialog box.
9. In the Confirm Upgrade dialog box, select one of the following then click Next:
   - Continue with the upgrade—Upgrades the Web Agent to 6.x.
   - Abort the installation—Exits the upgrade procedure without upgrading the Web Agent.
10. In the Pre-installation Summary dialog box, confirm the installation settings, 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. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

Afterward, the Web Agent Configuration dialog box is displayed.

11. Choose one of the following options, then click Next:
    - Yes. I would like to configure the Agent now.
    - No. I will configure the Agent later.

    If you select Yes to configure the Agent, the Web Agent Configuration Wizard starts up and does one of the following:
    - If you have not registered your system as a trusted host, the Wizard prompts you to register.
    - If your system is already registered as a trusted host, the Wizard prompts you to configure the Web Agent.

    Note: If you are installing an Agent on an Sun Java System 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.
12. When the Configuration Complete dialog box is displayed, click Done.
13. In the Install Complete dialog box, choose whether to reboot your system immediately or later, then click Done.

More Information

Register Your System as a Trusted Host on UNIX (see page 58)
Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server (see page 91)
Configure an Oracle iPlanet Web Agent (see page 133)
Configure an Apache Web Agent (see page 145)
Configure a Domino Web Agent (see page 155)

Upgrade a 4.x Web Agent to 6.x on UNIX Systems

The SiteMinder Web Agent r6.0 SP6 installation media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 4.x QMR 5
- 4.x QMR 6

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.

You can upgrade if you have applied a hotfix to any of these releases.

Note: When upgrading from a 4.x Web Agent to an r6.0 SP6 Web Agent, you can implement central agent configuration. However, this requires that you migrate the configuration settings in the 4.x WebAgent.conf file to an Agent Configuration Object on the Policy Server. See the *Upgrade Guide* for further instructions.

The upgrade instructions that follow reflect the GUI mode procedures. For UNIX systems, you can upgrade using console mode by executing the Web Agent binary file (nete-wa-6qmr6-*operating_system*.bin) with the -i console command argument. The command-line upgrade prompts will be similar to GUI mode prompts.

To upgrade a Web Agent on UNIX systems

1. Exit all applications that are running and stop the web server.
2. Insert the SiteMinder DVD into the drive or download the .bin file from the Technical Support web site.
3. Navigate to the directory for your operating system (aix, hpux, linux, solaris) on the SiteMinder DVD.
4. Copy the appropriate binary file to a local directory then navigate to that directory.
   - Solaris: nete-wa-6qmr6-sol.bin
   - AIX: nete-wa-6qmr6-aix.bin
   - Linux 2.1: nete-wa-doc-6qmr6-linux.bin
   - HP-UX: nete-wa-6qmr6-hp.bin
   - HP-UX Itanium: nete-wa-6qmr6-hp-itan.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 nete-wa-6qmr6-sol.bin
6. Open a console window and from the location of the installation program enter:

   ./nete-wa-6qmr6-*operating_system*.bin.

where *operating_system* is sol, aix, linux, hp, or hp-itan

The installation program prepares the files.

7. In the Introduction dialog box, read the information. Then click Next.
8. Read the License Agreement. Then select the radio button to accept the agreement. Click Next.
9. Read the notes in the Important Information dialog box. Then click Next.
10. Specify the installation directory in the Choose Install Folder dialog box, and then click Next.

    The Confirm Upgrade dialog box displays.
11. In the Confirm Upgrade dialog box, select one of the following then click Next:
    - Continue with the upgrade—Upgrades the Web Agent to 6.x.
    - Abort the installation—Exits the upgrade procedure without upgrading the Web Agent.
12. 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.
13. In the Install Complete dialog box, click Done.
14. 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 183)
Register Your System as a Trusted Host on UNIX (see page 58)

Upgrade a 5.x Web Agent to 6.x on UNIX Systems

The SiteMinder Web Agent r6.0 SP6 installation media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 5.x QMR 4
- 5.x QMR 5
- 5.x QMR 6
- 5.x QMR 7
- 5.x QMR 8

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.

You can upgrade if you have applied a hotfix to any of these releases.

To upgrade a Web Agent on UNIX systems:

1. Exit all applications that are running and stop the web server.
2. Insert the SiteMinder DVD into the drive or download the installation program from the Technical Support web site.
3. Navigate to the directory for your operating system (aix, hpux, linux, solaris).
4. Copy the appropriate binary file to a local directory then navigate to that directory.
   - Solaris: nete-wa-6qmr6-sol.bin
   - AIX: nete-wa-6qmr6-aix.bin
   - Linux 2.1: nete-wa-doc-6qmr6-linux.bin
   - Linux 3.0: nete-wa-6qmr6-rhel30.bin
   - Suse-zLinux: nete-wa-6qmr6-SuSE-zLinux.bin
   - HP-UX: nete-wa-6qmr6-hp.bin
   - HP-UX Itanium: nete-wa-6qmr6-hp-itan.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 nete-wa-6qmr6-sol.bin
6. Open a console window and from the location of the installation program enter:

   ./nete-wa-6qmr6-*operating_system*.bin

   where *operating_system* is sol, aix, linux, rhel30, SuSE-zLinux, hp, or hp-itan
7. In the Introduction dialog box, read the information. Then click Next.

8. Read the License Agreement then select the radio button to accept the agreement. Click Next.
9. Read the notes in the Important Information dialog box. 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 6.x.
    - 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.

    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.

More Information

Register Your System as a Trusted Host on UNIX (see page 58)

Upgrade a 6.x Web Agent to r6.0 SP6 on UNIX Systems

The SiteMinder Web Agent v6.x media contains a single executable. It will upgrade the following Web Agents to r6.0 SP6, provided the web server version has not changed since the last installation of the Web Agent:

- 6.x QMR 1
- 6.x QMR 2
- 6.x QMR 3
- 6.x QMR 4
- 6.x QMR5

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.

You can upgrade if you have applied a hotfix to any of these releases.

To upgrade a Web Agent on UNIX systems

1. Exit all applications that are running and stop the web server.
2. Insert the SiteMinder media into the drive or download the installation program from the Technical Support web site.
3. Navigate to the directory for your operating system (aix, hpux, linux, solaris).
4. Copy the appropriate binary file to a local directory then navigate to that directory.
   - Solaris: nete-wa-6qmr6-sol.bin
   - AIX: nete-wa-6qmr6-aix.bin
   - Linux 2.1: nete-wa-doc-6qmr6-linux.bin
   - Linux 3.0: nete-wa-6qmr6-rhel30.bin
   - Suse-zLinux: nete-wa-6qmr6-SuSE-zLinux.bin
   - HP-UX: nete-wa-6qmr6-hp.bin
   - HP-UX Itanium: nete-wa-6qmr6-hp-itan.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 nete-wa-6qmr6-sol.bin
6. Open a console window and from the location of the installation program enter:

   ./nete-wa-6qmr6-*operating_system*.bin

   where *operating_system* is sol, aix, linux, rhel30, SuSE-zLinux, hp, or hp-itan
7. In the Introduction dialog box, read the information then click Next.

8. Read the License Agreement then select 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 6.x.
    - 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.

    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.

More Information

Register Your System as a Trusted Host on UNIX (see page 58)

Chapter 6: Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server

This section contains the following topics:

How to Configure a SiteMinder Web Agent on IIS 7.5

To configure an SiteMinder Web Agent for an IIS 7.5 web server, use the following process:

1. Verify the following prerequisites:
   - The SiteMinder Web Agent is installed.
   - The computer running the SiteMinder Web Agent was restarted after the installation (*without* running the SiteMinder Web Agent Configuration wizard).
   - The web server (IIS) role is added your web server.
2. Add role services to your IIS 7.5 web server (see page 93).
3. If you are using the SiteMinder Windows authentication scheme, add the Windows authentication role service to your IIS 7.x web server (see page 94).
4. Configure a classic-mode application pool for SiteMinder (see page 95).
5. Move the applications you want to protect with SiteMinder to the classic-mode application pool (see page 96).
6. Run the Web Agent Configuration wizard (see page 97).
7. Add the ISAPI filters to all the web sites on the IIS 7.5 web server that you want to protect with SiteMinder (see page 98).
8. Add the handler mappings to all the web sites on the IIS 7.5 web server that you want to protect with SiteMinder (see page 100).
9. Grant the classic-mode application pool identity permissions for the following directories (see page 102):
   - *web_agent_home*\config
   - *web_agent_home*\log
10. If you are using the SiteMinder Windows authentication scheme, create and configure the virtual directory (see page 104).

Add Role Services to your IIS 7.5 Web Server

Before operating a SiteMinder Web Agent on an IIS 7.5 web server, you must configure the web server to use the role services that are required by the SiteMinder Web Agent.

To add role services to your IIS 7.5 web server

1. On your Windows Server 2008 system, click Start, Administrative Tools, Server Manager.

   Note: If the User Account Control dialog appears, click Continue.

   The Server Manager opens.

2. Expand Roles.

   A list of installed roles appears.

3. Click Web Server (IIS)

   The IIS Summary information appears.

4. In the Roles Summary section, click Add Roles.

   The Add Roles Wizard starts.

5. Use the wizard to add the following role services to your IIS 7.5 web server:

   - ASP.NET
   - CGI
   - ISAPI Extensions
   - ISAPI Filters
   - IIS Management Console
   - Windows Authentication (for SiteMinder Windows Authentication Scheme)

   The role services are added to your IIS web server.

Add the Windows Authentication Role Service to your IIS 7.x Web Server

To use the SiteMinder Windows Authentication scheme, add the Windows Authentication role service to your IIS 7.x web server. If you are adding SiteMinder to your IIS 7.x web server, there are other role services to add too. If you are already using SiteMinder on your IIS 7.x web server, and you only want to add the SiteMinder Windows authentication scheme use the following procedure.

Add the Windows authentication role service to your IIS 7.x web server

1. On your Windows Server 2008 system, click Start, Administrative Tools, Server Manager.

   Note: If the User Account Control dialog appears, click Continue.

   The Server Manager opens.

2. In the Roles Summary section, locate the Roles: list, and then click the Web Server (IIS) link.

   The Web Server (IIS) screen appears.

3. Click Add Role Services.

   The Add Role Services Wizard starts.

4. Use the wizard to add the following role service to your IIS 7.x web server:

   - Windows Authentication

   The authentication role service is added to your IIS 7.x web server.

More information:

Add Role Services to your IIS 7.x Web Server (see page 106)

Configure a Classic Mode Application Pool for the SiteMinder Web Agent

Application pools on IIS 7.x web servers use one of the following modes:

- Integrated mode (default)
- Classic mode

On IIS 7.x web servers, the SiteMinder Web Agent only operates on application pools configured in classic mode. The default application pool for IIS 7.x web servers uses integrated mode. To use the SiteMinder web Agent on an IIS 7.x web server, do one of the following tasks:

- If you do *not* need to run any applications on the IIS 7.x server in Integrated mode, then switch the mode of the default application pool (DefaultAppPool) to classic mode.
- If you want to run the SiteMinder Web Agent on the same IIS server with other applications that use application pools in integrated mode, create a new application pool with classic mode for SiteMinder as shown in the following procedure.

To configure a classic mode application pool for the SiteMinder Web Agent

1. Open IIS Manager.

   The Start page of the IIS Manager appears.

2. Expand the web server.

   The Application Pools icon and the Web Sites folder appear.

3. Right click Application Pools icon, and then select Add Application Pool.

   The Add Application Pool dialog appears. The cursor is in the Name field.

4. Type a name for the new application pool. We recommend using a distinctive name that is easy to recognize, such as SiteMinder.

5. Click the Managed pipeline mode drop-down list, and then select Classic.

6. Click OK.

   A classic mode application pool is created for the web agent.

Move the Applications you want to Protect to the Classic Mode Application Pool for SiteMinder

After you create a classic mode application pool for the on your IIS 7.x web server, you need to move the applications from their current application pools to the classic mode application pool used by SiteMinder.

To move the applications you want to protect to the classic mode application pool for SiteMinder

1. Open IIS Manager.
2. In the connections pane, expand the web server.

   The Application Pools icon and Site folder appear.
3. Click Application Pools.

   A list of application pools appears.
4. Right-click the application pool that contains the applications you need to move, and then select View Applications. For example, if the application you want to protect with SiteMinder is currently in the Default Application pool, then right-click the Default Application pool.

   A list of applications appears.
5. Right-click the application you want to move, and then select Change Application Pool.

   The Select Application pool dialog appears.
6. Click the Application Pool drop-down list, and then select the classic mode application pool you created for SiteMinder.
7. Click OK.

   The Select Application Pool dialog closes. The application is moved to the new application pool.

Run the Configuration Wizard for a SiteMinder Web Agent

Before you configure the SiteMinder Web 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 a SiteMinder 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 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, even if you are logged into 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 registered the trusted host, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

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, enter IISDefaultSettings to use the default.

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

   The Web Agent files are installed.

6. Click Done when the installation is complete.

   Note: You need to reboot the machine once the Agent is configured to ensure proper logging of Agent and trace messages.

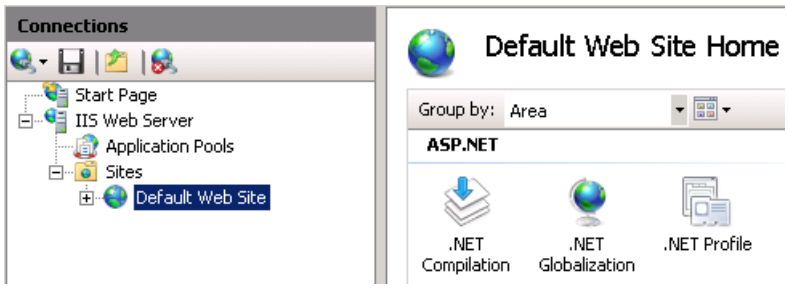
More Information

Register Your System as a Trusted Host on Windows (see page 36)
Install a Web Agent on a Windows System (see page 29)

Add the Agent ISAPI Filter to the IIS 7.5 Web Sites that you want to Protect with SiteMinder

To run a SiteMinder Web Agent on IIS 7.5, add a SiteMinder ISAPI filter to the top-level folder of each website you want to protect. This filter executes the Web Agent ISAPI scripts and other files.

The following illustration shows a top-level folder named "Default Web Site," which needs the ISAPI Filter added manually:



To add the agent ISAPI filter to the IIS 7.5 web sites that you want to protect with SiteMinder

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   The Sites folder appears.

3. Expand the Sites folder, and then click the icon of the additional website that you want to protect with SiteMinder.

4. Under the IIS section, double-click ISAPI Filters.

   The ISAPI Filters screen appears.

5. Under the actions pane, click Add.

   The Add ISAPI Filter dialog appears.

6. Type a name for the filter. We recommend using a name that is easy to recognize, such as "SiteMinder ISAPI Filter."

7. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgent.DLL

9. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add ISAPI Filter dialog.

10. Click OK.

    The Add ISAPI Filter dialog closes and the SiteMinder ISAPI Filter appears in the list.

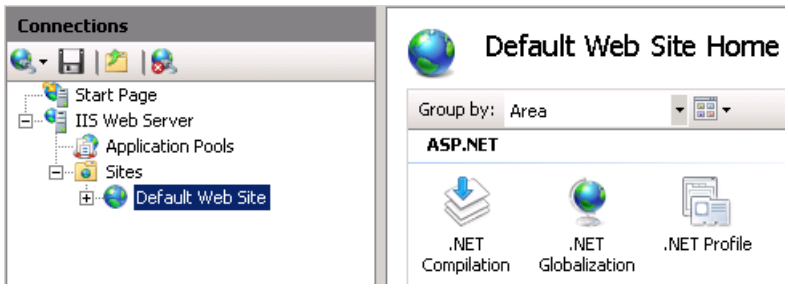
11. Repeat Steps 3 through 10 to protect any other web sites with SiteMinder.

    The Agent ISAPI filter is added.

Add Handler Mappings to the IIS 7.5 Web Sites you want to Protect with SiteMinder

To run a SiteMinder Web Agent on IIS 7.5, add the SiteMinder handler mappings to the top-level folder of each IIS 7.5 website you want to protect.

The following illustration shows a top-level folder named "Default Web Site," which needs the handler mappings added manually:



To add the handler mappings to the IIS 7.5 web sites that you want to protect with SiteMinder

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   The Sites folder appears.

3. Expand the Sites folder, and then click the icon of a website that you want to protect with SiteMinder.

4. Under the IIS section, double-click the Handler Mappings icon.

   A list of the installed handler mappings appears.

5. In the Disabled list, click the following handler mapping:

   `ISAPI-dll`

6. In the Actions pane, click Edit Feature Permissions...

   The Edit Feature Permissions dialog appears.

7. Select the following check boxes:

   - Read
   - Script
   - Execute

8. Click OK.

   The Edit Feature Permissions dialog closes.

9. In the Actions pane, click Add Wildcard Script map.

   The Add Wildcard Script Map dialog appears.

10. Click the ellipsis button (to the right of the Executable field).

    The Open dialog appears.

11. Navigate to the following file:

    web_agent_home`\bin\ISAPI6WebAgent.DLL`

    Note: The default value of the *web_agent_home* variable is C:\Program Files\netegrity\webagent.

12. Click Open.

    The ISAPI6WebAgentDLL.dll file appears in the Add Wildcard Script Map dialog.

13. In the Name field, type a name for the mapping. We recommend using a name that is easy to recognize, such as "handler-wa."

14. Click OK.

    A confirmation dialog appears.

15. Click Yes.

    The Add Wildcard Script Map dialog closes and the mapping appears in the list. The handler mapping is added to the protected website.

16. Repeat Steps 3 through 15 for all of the other web sites on the IIS 7.5 web server that you want to protect with SiteMinder.

    The handler mappings are added.

Grant the Application Pool Identities Permissions for the SiteMinder SmHost.conf File and Log Directory

All the application pool identities on IIS 7.5 web servers need permissions for the following SiteMinder items on the computer hosting the IIS web server:

- The SmHost.conf file
- The /log directory

To grant the application pools permissions for the SmHost.conf file and Log directory from Windows Explorer

1. Navigate to (but do *not* open) the following file:

   web_agent_home\config\SmHost.conf

2. Right-click the previous file, and then select Properties.

   The SmHost.conf Properties dialog appears.

3. Click the Security tab.

4. In the Group or User Names pane, verify that SYSTEM is selected, and then click Edit.

   Note: If the User Account Control dialog appears, click Continue.

   The Permissions for SmHost.conf dialog appears.

5. Click Add.

   The Select Users, Computers, or Groups dialog appears.

6. Do the following steps:

   a. Click Locations.

      The Locations dialog appears.

   b. Click the name of your computer (in the top of the list), and then click OK.

      The Locations dialog closes and the name of your computer appears in the From this location: field.

c. In the Enter the Object names to select field, enter the name of your application pool using the following format:

```
IIS AppPool\Application_Pool_Name
```

For example, to add the default application pool, enter the following:

```
IIS AppPool\DefaultAppPool
```

d. Click Check Names, and then click OK.

The Select Users, Computers, or Groups dialog closes. The Permissions for SmHost.conf appears with the Application Pool selected.

7. Under the Allow list, select the following check boxes:
   - Read
   - Read and Execute
   - Write
8. Click OK.

   The Permissions for SmHost.conf dialog closes.
9. Click OK.

   The SmHost.conf Properties dialog closes.
10. Navigate to (but do *not* open) the following directory:

    web_agent_home\log
11. Right-click the previous directory, and then select Properties.

    Note: If the User Account Control dialog appears, click Continue.
12. Repeat Steps 3 through 9.

    The application pool identities are granted permissions for the SiteMinder SmHost.conf file and Log directory.

To grant the application pools permissions for the SmHost.conf file and Log directory from the command line

1. Open the Windows Command Prompt.
2. Enter the following commands for each configured application pool identity:

   a. To grant permissions for the SmHost.conf file, type the following command and hit Enter:

   ```
   cacls "web_agent_home\config\SmHost.conf" /T /E /G
   "Application_Pool_Name":C
   ```

   b. To grant permissions for the Log directory, type the following and hit Enter:

   ```
   cacls "web_agent_home\log" /T /E /G "Application_Pool_Name":C
   ```

Create and Configure the Virtual Directory for Windows Authentication Schemes (IIS 7.5)

To use the SiteMinder Windows authentication scheme, configure a virtual directory on the IIS 7.5 web server. The virtual directory requires NT challenge and response for credentials.

To create and configure the virtual directory for Windows authentication schemes

1. Open the Internet Information Services (IIS) Manager.
2. In the left pane, expand the following items:
   - The web server icon
   - The Sites folder
   - The Default Web Site icon
3. Right-click the siteminderagent virtual directory, and then select Add Virtual Directory.

   The Add Virtual Directory dialog appears.
4. In the Alias field, type the following:

   `ntlm`
5. Click the Browse button (next to the Physical Path field), and then locate the following directory,

   web_agent_home`\samples`

   The virtual directory is created.
6. Configure the virtual directory with *one* of the following steps:
   - To protect all the resources on the entire website with SiteMinder Windows authentication scheme, click the Default Web Site icon.
   - If you do *not* want to protect the entire website, with the SiteMinder Windows authentication scheme, click the ntlm virtual directory (you created in Step 4)
7. Double-click the Authentication icon.

   The Authentication dialog appears.
8. Do the following steps:
   a. Right-click Anonymous Authentication, and then select Disable.
   b. Right-click Windows Authentication, and then select Enable..

   The virtual directory for Windows authentication schemes is configured.

   Note: Reboot the web server for these changes to take effect.

How to Configure a SiteMinder Web Agent on IIS 7.0

To configure a SiteMinder Web Agent for an IIS 7.0 web server, use the following process:

1. Verify the following prerequisites:
   - The SiteMinder Web Agent is installed.
   - The computer running the SiteMinder Web Agent was restarted after the installation (*without* running the SiteMinder Web Agent Configuration wizard).
   - The web server (IIS) role is added your web server.
2. Add role services to your IIS 7.0 web server.
3. If you are using the SiteMinder Windows authentication scheme, add the Windows authentication role service to your IIS 7.x web server.
4. Configure a classic-mode application pool for SiteMinder.
5. Move the applications you want to protect with SiteMinder to the classic-mode application pool.
6. Run the Web Agent Configuration wizard.
7. If you want to use the SiteMinder Windows Authentication scheme, configure the virtual directory on the IIS web server.
8. Add the handler mappings to any additional web sites that you want to protect with SiteMinder.

   Note: These settings are added to the Default Web Site of the IIS web server automatically by the Web Agent Configuration wizard.
9. Add the SiteMinder ISAPI filter any additional web sites that you want to protect with SiteMinder.

   Note: These settings are added to the Default Web Site of the IIS web server automatically by the Web Agent Configuration wizard.

Add Role Services to your IIS 7.x Web Server

Before operating a SiteMinder Web Agent on an IIS 7.x web server, you must configure the web server to use the role services that are required by the SiteMinder Web Agent.

To add role services to your IIS 7.x web server

1. On your Windows Server 2008 system, click Start, Administrative Tools, Server Manager.

   Note: If the User Account Control dialog appears, click Continue.

   The Server Manager opens.

2. Expand Roles, and then click Web Server (IIS)

   The Web Server (IIS) Summary appears.

3. In the Roles Summary section, click Add Roles.

   The Add Roles Wizard starts.

4. Use the wizard to add the following role services to your IIS 7.0 web server:

   - ASP.NET
   - CGI
   - ISAPI Extensions
   - ISAPI Filters
   - IIS Management Console
   - Windows Authentication (for the SiteMinder Windows Authentication Scheme)

   The role services are added to your IIS web server.

More information:

Add the Windows Authentication Role Service to your IIS 7.x Web Server (see page 94)

Add the Windows Authentication Role Service to your IIS 7.x Web Server

To use the SiteMinder Windows Authentication scheme, add the Windows Authentication role service to your IIS 7.x web server. If you are adding SiteMinder to your IIS 7.x web server, there are other role services to add too. If you are already using SiteMinder on your IIS 7.x web server, and you only want to add the SiteMinder Windows authentication scheme use the following procedure.

Add the Windows authentication role service to your IIS 7.x web server

1. On your Windows Server 2008 system, click Start, Administrative Tools, Server Manager.

   Note: If the User Account Control dialog appears, click Continue.

   The Server Manager opens.

2. In the Roles Summary section, locate the Roles: list, and then click the Web Server (IIS) link.

   The Web Server (IIS) screen appears.

3. Click Add Role Services.

   The Add Role Services Wizard starts.

4. Use the wizard to add the following role service to your IIS 7.x web server:

   - Windows Authentication

   The authentication role service is added to your IIS 7.x web server.

More information:

Add Role Services to your IIS 7.x Web Server (see page 106)

Configure a Classic Mode Application Pool for the SiteMinder Web Agent

Application pools on IIS 7.x web servers use one of the following modes:

- Integrated mode (default)
- Classic mode

On IIS 7.x web servers, the SiteMinder Web Agent only operates on application pools configured in classic mode. The default application pool for IIS 7.x web servers uses integrated mode. To use the SiteMinder web Agent on an IIS 7.x web server, do one of the following tasks:

- If you do *not* need to run any applications on the IIS 7.x server in Integrated mode, then switch the mode of the default application pool (DefaultAppPool) to classic mode.
- If you want to run the SiteMinder Web Agent on the same IIS server with other applications that use application pools in integrated mode, create a new application pool with classic mode for SiteMinder as shown in the following procedure.

To configure a classic mode application pool for the SiteMinder Web Agent

1. Open IIS Manager.

   The Start page of the IIS Manager appears.

2. Expand the web server.

   The Application Pools icon and the Web Sites folder appear.

3. Right click Application Pools icon, and then select Add Application Pool.

   The Add Application Pool dialog appears. The cursor is in the Name field.

4. Type a name for the new application pool. We recommend using a distinctive name that is easy to recognize, such as SiteMinder.

5. Click the Managed pipeline mode drop-down list, and then select Classic.

6. Click OK.

   A classic mode application pool is created for the web agent.

Move the Applications you want to Protect to the Classic Mode Application Pool for SiteMinder

After you create a classic mode application pool for the on your IIS 7.x web server, you need to move the applications from their current application pools to the classic mode application pool used by SiteMinder.

To move the applications you want to protect to the classic mode application pool for SiteMinder

1. Open IIS Manager.
2. In the connections pane, expand the web server.

   The Application Pools icon and Site folder appear.
3. Click Application Pools.

   A list of application pools appears.
4. Right-click the application pool that contains the applications you need to move, and then select View Applications. For example, if the application you want to protect with SiteMinder is currently in the Default Application pool, then right-click the Default Application pool.

   A list of applications appears.
5. Right-click the application you want to move, and then select Change Application Pool.

   The Select Application pool dialog appears.
6. Click the Application Pool drop-down list, and then select the classic mode application pool you created for SiteMinder.
7. Click OK.

   The Select Application Pool dialog closes. The application is moved to the new application pool.

Run the Configuration Wizard for a SiteMinder Web Agent

Before you configure the SiteMinder Web 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 a SiteMinder 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 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, even if you are logged into 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 registered the trusted host, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

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, enter IISDefaultSettings to use the default.

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

   The Web Agent files are installed.

6. Click Done when the installation is complete.

   Note: You need to reboot the machine once the Agent is configured to ensure proper logging of Agent and trace messages.

More Information

Register Your System as a Trusted Host on Windows (see page 36)
Install a Web Agent on a Windows System (see page 29)

Configure the Virtual Directory for Windows Authentication Schemes (IIS 6.0)

To use the SiteMinder Windows authentication scheme, configure a virtual directory on the IIS 6.0 web server. The virtual directory requires NT challenge and response for credentials.

Configure the virtual directory for Windows authentication schemes

1. Open the Internet Information Services (IIS) Manager.
2. In the left pane, expand the following items:
   - The web server icon
   - The Web Sites folder
3. Do *one* of the following steps:
   - To protect all the resources on the entire website with SiteMinder Windows authentication scheme, right-click the Default Web Site folder, select Properties, and then go to Step 4.
   - If you do *not* want to protect the entire website, with the SiteMinder Windows authentication scheme, do the following steps:
     a. Locate the following folder:

     ```
     \siteminderagent\ntlm
     ```

     b. Right-click the ntlm folder, select Properties and go to Step 4.

   The Properties dialog appears.
4. Click the Directory Security tab.
5. In the Anonymous Access and Authentication Control group box, click Edit.

   The Authentication Methods dialog appears.
6. Do the following steps:
   - Clear the Enable Anonymous Access check box.
   - Select the Integrated Windows Authentication check box.
7. Click OK twice.

   The Authentication Methods dialog and the Properties dialog close. The virtual directory is configured and requires NT challenge and response for credentials.

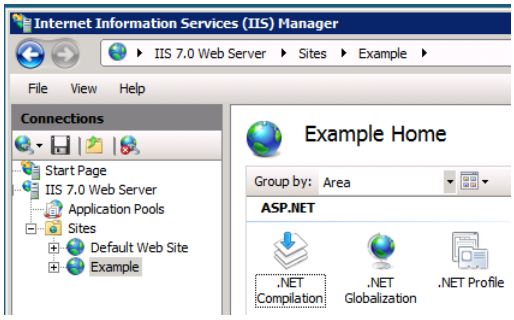
   Note: Reboot the web server for these changes to take effect.

Add Handler Mappings to Additional Web Sites you want to Protect with SiteMinder

Every additional web site (beyond the Default Web Site) in the IIS 7.0 web server that you want to protect with SiteMinder requires a handler mapping.

Note: These settings are added to the Default Web Site of the IIS web server automatically by the Web Agent Configuration wizard.

The following illustration shows a web site named "Example," which needs the handler mapping added manually:



To add a handler mapping to additional web sites

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   The Sites folder appears.

3. Expand the Sites folder, and then click the icon of the additional web site that you want to protect with SiteMinder.

4. Under the IIS section, double-click the Handler Mappings icon.

   A list of the installed handler mappings appears.

5. In the Actions pane, click Add Wildcard Script map.

   The Add Wildcard Script Map dialog appears.

6. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

7. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgent.DLL

   Note: The default value of the *web_agent_home* variable is C:\Program Files\netegrity\webagent.

8. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add Add Wildcard Script Map dialog.

9. In the Name field, type a name for the mapping. We recommend using a name that is easy to recognize, such as "handler-wa."

10. Click OK.

    A confirmation dialog appears.

11. Click Yes.

    The Add Wildcard Script Map dialog closes and the mapping appears in the list. The handler mapping is added to the protected web site.

12. Repeat Steps 3 through 11 for each additional web site you want to protect with SiteMinder.

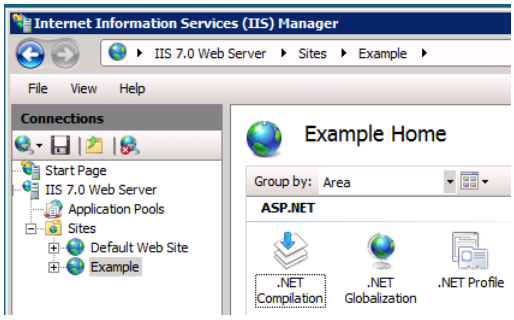
    The handler mappings are added.

Add the Agent ISAPI Filter to Additional Web Sites that you want to Protect with SiteMinder

To run a SiteMinder Web Agent on an additional (not the default) web site on IIS 7.0, add a SiteMinder ISAPI filter to each additional web site you want to protect. This filter executes the Web Agent ISAPI scripts and other files.

Note: These settings are added to the Default Web Site of the IIS web server automatically by the Web Agent Configuration wizard.

The following illustration shows a web site named "Example," which needs the ISAPI Filter added manually:



To add the agent ISAPI filter to additional web sites that you want to protect with SiteMinder

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   The Sites folder appears.

3. Expand the Sites folder, and then click the icon of the additional web site that you want to protect with SiteMinder.

4. Under the IIS section, double-click ISAPI Filters.

   The ISAPI Filters screen appears.

5. Under the actions pane, click Add.

   The Add ISAPI Filter dialog appears.

6. Type a name for the filter. We recommend using a name that is easy to recognize, such as "SiteMinder ISAPI Filter."

7. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgent.DLL

9. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add ISAPI Filter dialog.

10. Click OK.

    The Add ISAPI Filter dialog closes and the SiteMinder ISAPI Filter appears in the list.

11. Repeat Steps 3 through 10 to protect any other additional (non-default) web sites with SiteMinder.

How to Configure a SiteMinder Web Agent on IIS 6.0

Before you can use the Web Agent on an IIS 6.0 web server, you must complete the prerequisites using the following process:

1. Assign read permissions to samples and error files directories.
2. Allow IIS to execute Web Agent ISAPI and CGI extensions.
3. (Optional) Increase the Web Agent's size limit for uploaded files.
4. Gather the Web Agent information.
5. Run the Configuration Wizard for an IIS Web Agent.
6. Put the Agent filter and extension before other third-party filters.

Assign Read Permissions to Samples and Error Files Directories

The Network Service account must have Read permissions to any directory where the Web Agent reads forms credential collector (FCC) files and to any directory where the Web Agent reads Web Agent custom error files.

To Assign Read Permissions to the Samples and Error Files Directories

1. Open Windows Explorer and go to the appropriate directory:
   - samples: *web_agent_home*/samples
   - custom error file: the location or your custom error files. There is no default location.
2. Right-click the directory and select Sharing and Security.
3. Select the Security tab.
4. Click Add.

   The Select Users, Computers, or Groups dialog box opens.
5. Do one of the following:
   a. Accept the defaults for the Select this object type and From this Location fields.
   b. In the Enter the object names to select field, enter Network Service and click OK.

   You return to the Properties dialog box for the directory.
6. In the Permissions for Network Service scroll-box, allow Read permissions.
7. Click OK to finish.
8. Repeat this procedure for each directory.

Allow IIS to Execute the Agent ISAPI and CGI Extensions

You must add certain ISAPI and CGI extentions to the IIS 6.0 web server and grant the server permission to execute them before configuring the SiteMinder Web Agent. These extensions will execute the Web Agent ISAPI and CGI scripts and other files.

To add the extensions and permissions

1. Open the Internet Information Services (IIS) Manager, and then expand the web server you are configuring for the Agent.
2. Double-click Web Service Extensions

   The Web Service Extensions pane appears.
3. To add the ISAPI Web Agent extension, do the following:
   a. Click the Add a new Web service extension link.

      The New Web Service Extension dialog box opens.

   b. In the Extension name field, enter ISAPI6WebAgentDLL, and then click Add.

      The Add File dialog box opens.

   c. Click the Browse button, and then navigate to the ISAPI6WebAgent.dll file in the *web_agent_home*/bin directory. If the proper file does not appear, click the Files of type drop-down list and select either ISAPI dll files (for the .dll files) or CGI exe files (for .exe files).

      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\netegrity\webagent

      Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

   d. Click Open

      The path to the file appears in the Add File dialog box.

   e. Click OK.

      You return to the New Web Service Extension dialog box.

   f. Select the Set extension status to allowed check box.

   g. Click OK.

The New Web Service Extension dialog box closes.

4. Repeat Step 3 and add each of the following Web Agent files. Even though both files use the same name, you must add a separate extension for each because they are in different directories.
   - *web_agent_home*/pw/smpwservicescgi.exe (suggested extension name: Password Services CGI)
   - *web_agent_home*/pw_default/smpwservicescgi.exe (suggested extension name: PW Default CGI)

Increase the Agent's Size Limit for Uploaded Files

The Web Agent installed on an IIS 6.0 web server has a size limit of 2.5 MB for uploading files. If you want to increase this size limit, you can add a new key to the Windows registry on your web server.

To upload files that are larger than this limit

1. Open the registry editor.

   Note: For more information, see your Microsoft documentation, or go to http://support.microsoft.com/

2. Navigate to the following location:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\netegrity\SiteMinder Web Agent\Microsoft IIS
   ```

3. Create a new DWORD registry key in the previous location using the following name:

   ```
   MaxRequestAllowed
   ```

4. Set this value of the key to the number of bytes that corresponds to the size limit you want.

   The value of this key overrides the default limit. If the value of this key is less than or equal to 0, than the default of 2.5 MB (2,500,000 B) is used. This key accepts decimal values from 0 to 4294967295.

   Note: The IIS 6.0 web server has its own size limit. Changing the Web Agent's limit will not affect the IIS 6.0 limit. If you want to change the IIS 6.0 server's limit, see the Microsoft IIS 6.0 documentation or online help.

5. Close the registry editor.

   The size limit is changed.

Run the Configuration Wizard for a SiteMinder Web Agent

Before you configure the SiteMinder Web 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 a SiteMinder 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 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, even if you are logged into 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 registered the trusted host, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

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, enter IISDefaultSettings to use the default.

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

   The Web Agent files are installed.

6. Click Done when the installation is complete.

   Note: You need to reboot the machine once the Agent is configured to ensure proper logging of Agent and trace messages.

More Information

Register Your System as a Trusted Host on Windows (see page 36)
Install a Web Agent on a Windows System (see page 29)

Put the Agent Filter and Extension Before Other Third-Party Filters

The IIS 6.0 Web Agent consists of an ISAPI filter and an ISAPI extension. The majority of Web Agent processing occurs in the extension.

When the Web Agent is installed on an IIS 6.0 Web Server with other third-party software, such as WebSphere or ServletExec, the Agent has the following restrictions:

- The Web Agent filter and Web Agent extension must be configured to run before other third-party filters installed on the web server.
- The Web Agent must be configured as the first wildcard application map if it is going to protect applications running as or spawned by an ISAPI extension.
- The IIS 6.0 web server does not enforce how third-party filters and extensions behave. IIS 6.0 processes ISAPI filters before calling ISAPI extensions, including the Web Agent extension. Therefore, the SiteMinder Web Agent for IIS 6.0 is unable to authenticate or authorize access to applications implemented as pure ISAPI filters. This limitation impacts Web Agent integration with other third-party offerings for the IIS 6.0 web server, if those offerings are implemented as ISAPI filters that process and/or redirect the request before ISAPI extensions are called.

When you install the Web Agent on an IIS 6.0 web server, the Agent's filter is automatically placed at the top of the ISAPI filters list. However, if you install any other third-party plugins after installing the Web Agent, those filters may take precedence.

After you install and configure an IIS 6.0 Web Agent, you must ensure that the siteminderagent ISAPI filter and extension is listed before any third-party filter or extension. This enables the Web Agent to process requests before a third-party.

To put the agent filter and extension before other third-party filters

1. Check the ISAPI filter by doing the following steps:
   a. Open the IIS Manager.
   b. Select Web Sites then right-click and select Properties.
   c. Select the ISAPI Filters tab.
   d. Check the list of filters and ensure that siteminderagent is the first entry in the list. If it is not, use the Move Up button to place it at the top of the list.
   e. Click OK.
   f. Exit the IIS Manager.
2. Check the ISAPI extensions by doing the following steps:
   a. Open the IIS Manager, and then expand the web server.
   b. Right-click the Default Web Site folder, and select Properties.
   c. Click the Home Directory tab, and then click Configuration.

d. The following file should be at the top of the Wildcard application maps (order of implementation) field:

web_agent_home\bin\ISAPI6WebAgent.dll

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

How to Configure a SiteMinder Web Agent to Protect Microsoft Outlook Web Access

To have a SiteMinder Web Agent protect a Microsoft Outlook Web Access web site, use the following process:

Note: See the SiteMinder r6.0 SP6 Product Support Matrix at http://ca.com/support to determine which versions of this component are supported.

1. Install or configure the following prerequisites:
   a. Microsoft Exchange Server.
   b. Microsoft Web Access Client software configured for IIS 6.0

      Note: The Microsoft Exchage Server and Web Access Client components can be installed on the same system, or on separate systems. Only one Web Agent is required if both are installed on the same system. If the components are installed on different systems, then two Web Agents are used. When different systems are used, the Exchange Server acts as a back-end system, while the Web Access Client acts as a front-end system.
   c. A SiteMinder Policy Server with the following:
      - A Microsoft Active Directory used for a policy-store and user-directory.
      - A SQL Server database instance used for a session server.
      - Persistent sessions enabled for the realms (r6.x) or applications (r6.0 SP6) associated with the Microsoft Outlook Web Access resources you want to protect.
2. Perform the following steps on the IIS web server that hosts your Microsoft Exchange Server:
   a. Confirm the SiteMinder ISAPI filter appears first in the list.
   b. Allow IIS to Execute the Outlook Extensions.
   c. Set the Default Web Site Home directory location and Execute Permission settings.
   d. Add the ISAPI extension to Exchange Web Site.
   e. Set Directory Security for Exchange Web Site.
   f. Set the ISAPI Extension for Exchweb Virtual Site.
   g. Set the Directory Security for Exchweb Virtual Site.
   h. Set the Owa Web Site Home directory location and Execute Permission settings.
3. Repeat Steps 2a through 2g on the IIS web server that hosts your Microsoft Outlook Web Access Client.
4. Confirm that SiteMinder is protecting the Outlook Web Access web site.

Confirm the SiteMinder ISAPI filter appears first in the list

The IIS 6.0 Web Agent consists of an ISAPI filter and an ISAPI extension. The majority of Web Agent processing occurs in the extension.

When the Web Agent is installed on an IIS 6.0 Web Server with other third-party software, such as WebSphere or ServletExec, the Agent has the following restrictions:

- The Web Agent filter and Web Agent extension must be configured to run before other third-party filters installed on the web server.
- The Web Agent must be configured as the first wildcard application map if it is going to protect applications running as or spawned by an ISAPI extension.
- The IIS 6.0 web server does not enforce how third-party filters and extensions behave. IIS 6.0 processes ISAPI filters before calling ISAPI extensions, including the Web Agent extension. Therefore, the SiteMinder Web Agent for IIS 6.0 is unable to authenticate or authorize access to applications implemented as pure ISAPI filters. This limitation impacts Web Agent integration with other third-party offerings for the IIS 6.0 web server, if those offerings are implemented as ISAPI filters that process and/or redirect the request before ISAPI extensions are called.

When you install the Web Agent on an IIS 6.0 web server, the Agent's filter is automatically placed at the top of the ISAPI filters list. However, if you install any other third-party plugins after installing the Web Agent, those filters may take precedence.

After you install and configure an IIS 6.0 Web Agent, you must ensure that the siteminderagent ISAPI filter and extension is listed before any third-party filter or extension. This enables the Web Agent to process requests before a third-party.

To put the agent filter and extension before other third-party filters

1. Check the ISAPI filter by doing the following steps:
   a. Open the IIS Manager.
   b. Select Web Sites then right-click and select Properties.
   c. Select the ISAPI Filters tab.
   d. Check the list of filters and ensure that siteminderagent is the first entry in the list. If it is not, use the Move Up button to place it at the top of the list.
   e. Click OK.
   f. Exit the IIS Manager.
2. Check the ISAPI extensions by doing the following steps:
   a. Open the IIS Manager, and then expand the web server.
   b. Right-click the Default Web Site folder, and select Properties.
   c. Click the Home Directory tab, and then click Configuration.

d. The following file should be at the top of the Wildcard application maps (order of implementation) field:

web_agent_home\bin\ISAPI6WebAgent.dll

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

■

Allow IIS to Execute the Outlook Extensions

The IIS Web Server must have permissions to execute the Web Service Extensions for Microsoft Outlook.

To allow IIS to execute the Outlook extensions

1. Open the Internet Information Services (IIS) Manager, and then expand the web server you are configuring for the Agent.
2. Double-click Web Service Extensions.

   The Web Service Extensions pane appears.
3. Confirm that the following extensions show a status of Allowed:
   - Microsoft Exchange Client Access
   - Microsoft Exchange Server

Set the Default Web Site Directory Location and Execute Permissions

The Default Web Site of your IIS web server needs a specific directory location and execute permissions to integrate with Microsoft Outlook Web Access.

To set the default web site directory location and execute permissions

1. Open the Internet Information Services (IIS) Manager.
2. Right-click the Default Web Site folder, and then select Properties.

   The Default Web Site Properties dialog appears.
3. Click the Home Directory tab, and then confirm the following settings:
   - Local path: c:\inetpub\wwwroot
   - Execute Permissions: Scripts and Executables

   The Default Web Site Directory location and execute permissions are set.

Add the ISAPI Extension to the Exchange Web Site

The Microsoft Exchange web site on your IIS web server needs the SiteMinder ISAPI extension to operate with Microsoft Outlook Web Access.

To add the ISAPI extension to the Exchange web site

1. Open the Internet Information Services (IIS) Manager, and then expand the Web Sites folder.

   A list of web sites appears.

2. Right-click the Exchange folder, and then select Properties.

   The Exchange Properties dialog appears.

3. Click the Virtual Directory tab, and then verify the following settings:

   - Local path: *path_to_the exchange_folder* For example, C:\Program Files\Microsoft\Exchange Server\ClientAccess\owa
   - Application Name: Exchange
   - Execute Permissions: Scripts and Executables

4. Click Configuration.

   The Application Configuration dialog appears.

5. Click Insert.

   The Add/Edit Extension Mapping dialog appears.

6. Click Browse, and then navigate to the following file:

   `C:\Program Files\CA\webagent\bin\ISAPI6WebAgent.dll`

7. Click Open.

   The path appears in the Add/Edit Extension mapping dialog.

8. Clear the Verify that file exists check box.

9. Click OK.

   The Add/Edit Extension mapping dialog closes. The DLL file appears in the Wildcard Application Maps (order of implementation) list.

10. Click OK.

    The Application Configuration dialog closes.

11. Click OK.

    The Exchange Properties dialog closes. The ISAPI extension is added to the Exchange web site.

Set the Directory Security for the Exchange Web Site

The Microsoft Exchange web site on your IIS web server needs certain directory security settings to operate with Microsoft Outlook Web Access.

To set the directory security for the Exchange web site

1. Open the Internet Information Services (IIS) Manager, and then expand the Web Sites folder.

   A list of web sites appears.

2. Right-click the Exchange folder, and then select Properties.

   The Exchange Properties dialog appears.

3. Click the Directory Security tab.

4. In the Authentication and Access control settings section, click Edit.

5. The Authentication Methods dialog appears.

6. Verify the following settings:

   - The Enable Anonymous Access check box is selected.
   - All of the check boxes in the Authenticated Access section are cleared.

7. Click OK.

   The Authentication Methods dialog closes.

8. Click OK.

   The Exchange Properties dialog closes. The Directory Security for the Exchange web site is set.

Add the ISAPI Extension to the Exchweb Web Site

The Microsoft Exchweb web site on your IIS web server needs the SiteMinder ISAPI extension to operate with Microsoft Outlook Web Access.

To add the ISAPI extension to the Exchweb web site

1. Open the Internet Information Services (IIS) Manager, and then expand the Web Sites folder.

   A list of web sites appears.

2. Right-click the Exchweb folder, and then select Properties.

   The Exchweb Properties dialog appears.

3. Click the Virtual Directory tab, and then verify the following settings:

   - Local path: *path_to_the exchweb_folder*
   - Application Name: Exchweb
   - Execute Permissions: Scripts and Executables

4. Click Configuration.

   The Application Configuration dialog appears.

5. Click Insert.

   The Add/Edit Extension Mapping dialog appears.

6. Click Browse, and then navigate to the following file:

   `C:\Program Files\CA\webagent\bin\ISAPI6WebAgent.dll`

7. Click Open.

   The path appears in the Add/Edit Extension mapping dialog.

8. Clear the Verify that file exists check box.

9. Click OK.

   The Add/Edit Extension mapping dialog closes. The DLL file appears in the Wildcard Application Maps (order of implementation) list.

10. Click OK.

    The Application Configuration dialog closes.

11. Click OK.

    The Exchweb Properties dialog closes. The ISAPI extension is added to the Exchweb web site.

Set the Directory Security for the Exchweb Web Site

The Microsoft Exchweb web site on your IIS web server needs certain directory security settings to operate with Microsoft Outlook Web Access.

To set the directory security for the Exchweb web site

1. Open the Internet Information Services (IIS) Manager, and then expand the Web Sites folder.

   A list of web sites appears.

2. Right-click the Exchweb folder, and then select Properties.

   The Exchweb Properties dialog appears.

3. Click the Directory Security tab.
4. In the Authentication and Access control settings section, click Edit.
5. The Authentication Methods dialog appears.
6. Verify the following settings:
   - The Enable Anonymous Access check box is selected.
   - All of the check boxes in the Authenticated Access section are cleared.
7. Click OK.

   The Authentication Methods dialog closes.

8. Click OK.

   The Exchweb Properties dialog closes. The Directory Security for the Exchweb web site is set.

Set the Default Web Site Directory Location and Execute Permissions

The owa Web Site of your IIS web server needs a specific directory location and execute permissions to integrate with Microsoft Outlook Web Access.

To set the owa web site directory location and execute permissions

1. Open the Internet Information Services (IIS) Manager.
2. Right-click the owa Web Site folder, and then select Properties.

   The owa Web Site Properties dialog appears.

3. Click the Home Directory tab, and then confirm the following settings:
   - Local path: *full_path_to_the_owa_folder*
   - Execute Permissions: Scripts and Executables

   The owa Web Site Directory location and execute permissions are set.

Confirm that SiteMinder is protecting the Outlook Web Access web site

After configuring your Microsoft Exchange and Microsoft Outlook Web Access web sites, you can verify that the SiteMinder Web Agent is protecting them.

Confirm that SiteMinder is protecting the Outlook Web Access web site

1. Enable the Web Agent.
2. Open the Outlook Web Access Inbox page. The following URL is an example:

   `http://exchange_server_name.example.com/owa/`

   A SiteMinder login page appears.
3. Enter your credentials, and then click Login.

   The Inbox appears.

Chapter 7: 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 added by the wizard 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, even if you are logged into 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 Changes to Oracle iPlanet Web Server Files (see page 143)

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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 added by the wizard 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: **.**/nete-wa-config.bin

Console mode: ./nete-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 Changes to Oracle iPlanet Web Server Files (see page 143)

Modify Startup Script for Sun Java System (SunOne 6.1.11) Web Servers on UNIX

If you are running a SiteMinder Web Agent on a Sun Java System (SunOne 6.1.11) web server on any UNIX operating environment, modify the startup script for the web server.

To modify the startup script for the web server

1. Navigate to the root directory of the web server.
2. Open the start file with a text editor.
3. Add the following line to the start file:

   ```
   LD_LIBRARY_PATH_64=/usr/lib/lwp
   :${SERVER_LIBPATH}:${LD_LIBRARY_PATH}:${MPS_LIB_DIRS}; export
   LD_LIBRARY_PATH_64
   ```

4. Save the start file and close the text editor.

Manually Configure an Oracle iPlanet Web Server

The SiteMinder Web Agent Configuration wizard only configures the default instance of your Oracle iPlanet web server. If you want to configure a different instance of the Oracle iPlanet web server to use SiteMinder, you need to manually edit the obj.conf file that is used by that server instance. Examples of server instances that need manual configuration include:

- Servers installed in a non-default directory
- Servers 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 added by the wizard from the obj.conf file to the my_server.example.com-obj.conf file.
- Virtual servers on the same computer

To manually configure a Oracle iPlanet Web Server

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"
   ```

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files\netegrity\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 Changes to Oracle iPlanet Web Server Files

The Web Agent Configuration Wizard makes changes to the Oracle iPlanets.conf, obj.conf, and mime.types files. If you plan to use the Oracle iPlanet Administration console, you must apply the changes to these files *before* making any modifications with the console or the Web Agent configuration may be lost. If you lose your configuration, use the Configuration Wizard to reconfigure your Web Agent.

Note: The Web Agent adds settings to the Oracle iPlanet web server's obj.conf file when the Agent is configured to support an advanced authentication scheme. SiteMinder does not remove these settings later if the Agent is reconfigured to support a different advanced authentication scheme. Administrators must edit the obj.conf file manually to remove the settings that are no longer relevant.

To apply changes to the Oracle iPlanet configuration files

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

   You will see a warning message about loading the modified configuration files.
4. Click Load Configuration Files.
5. Exit the console.
6. Restart the web server.
7. Optimize the Oracle iPlanet Web Agent by tuning the shared memory segments.

You may be required reboot your machine once the Agent is configured.

More Information

Settings Added to the Sun Java System Server Configuration (see page 239)
Tune the Shared Memory Segments (see page 194)

Chapter 8: 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, even if you are logged into 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

Register Your System as a Trusted Host on Windows (see page 36)
Configuration Changes to Web Servers with Apache Web Agent (see page 247)
Configure an Apache Web Agent (see page 145)

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 149)
How to Configure Any Web Agent in Unattended Mode (see page 183)
Register Your System as a Trusted Host on Windows (see page 36)

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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: **./**nete-wa-config.bin

      Console mode: ./nete-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 247)
Configure an Apache Web Agent (see page 145)
Tune the Shared Memory Segments (see page 194)

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 for Apache Agent Operation

The LD_PRELOAD variable needs to be defined for the Apache Web Agent to operate on different platforms.

More Information

Set the LD_PRELOAD Variable for an Oracle 10G Web Server on Linux (see page 152)

Set the LD_PRELOAD Variable for an Oracle 10G Web Server on Linux

After you install the Web Agent r6.0 SP6 on an Oracle 10G web server running on a Linux platform, you must set the LD_PRELOAD environment variable in the apachectl script.

If the LD_PRELOAD variable is not included in the apachectl script, the Oracle 10G web server may dump core upon shutdown and fail to restart.

1. Open the apachectl file.
2. Add the LD_PRELOAD entry as follows:

   LD_PRELOAD=*web_agent_home*/bin/libbtunicode.so

   export LD_PRELOAD
3. Run the script to start the Apache server.

Note: Setting this environment variable causes any application executed from that environment to bind with libbtunicode.so. Therefore, set this variable only when starting or stopping a web server that loads the SiteMinder Web Agent.

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

Enabling SHLIB Path for an Agent on Apache 2.0/HP-UX 11

For the Web Agent to operate on an Apache 2.0 web server running HP-UX 11, be sure the SHLIB_PATH is enabled in the Apache executable.

1. Check if the SHLIB PATH is already enabled by executing the command chatr httpd. A partial sample of the output is shown below. Notice that SHLIB_PATH is disabled.

```
httpd:
shared executable
shared library dynamic path search:
SHLIB_PATH disabled second embedded path
enabled first /home/userx/apache2043hp/lib:
home/userx/apache2043hp//lib
```

2. If it is not enable, enter chatr +s enable httpd.

   A partial sample of the output is shown below. First the current values are shown followed by the new values.

```
httpd:
current values:
shared executable
shared library dynamic path search:
SHLIB_PATH disabled second
embedded path enabled first /home/userx/apache2043hp/lib:/
home/userx/apache2043hp//lib
.
.
.
shared library dynamic path search:
SHLIB_PATH enabled second
embedded path enabled first /home/userx/apache2043hp/lib:
home/userx/apache2043hp//lib
shared library list:
```

Modify the Apache Agent for an IBM HTTP Server 6.x on AIX

If you installed an Apache Web Agent on an IBM HTTP Server 6.x running on the AIX operating environment, make the following changes to the Apache Web Agent.

To modify the Apache Web Agent

1. Change the value of the EXTSHM environment variable to the following:

   ```
   ON
   ```

   Note: This value is case-sensitive.

2. Verify that the libapr-0.so library file is in the apr.exp file (the apr.exp file is located in *web_server_home*/lib).

3. If the library is *not* listed, create a link from the existing library to this library by entering the following command:

   ```
   ln -s libapr.so libapr-0.so
   ```

   The Apache Web Agent is modified.

How to Configure Red Hat Apache 64-bit Web Agents Running on Security Enhanced (SE) Linux

To run a Red Hat Apache 64-bit Web Agent with SELinux, use one of the following procedures:

- Change the security context of the Web Agent module to match the security context of the httpd file.
- Disable SELinux on the web server.

  Note: For more information, see your Linux documentation.

Change the Security Context of the Web Agent Module

You can change the security context of the Web Agent module to match the security context of the httpd binary file.

To change the security context of the web agent module, use the following command:

```
chcon --reference=Apache_service web_agent_home/bin/*
```

Example: chcon --reference=/usr/sbin/httpd /opt/netegrity/webagent/bin/*

Important! Changing this setting disables Web Agent logging.

Chapter 9: Configure a Domino Web Agent

This section contains the following topics:

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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, even if you are logged into 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

Register Your System as a Trusted Host on UNIX (see page 58)

Add the Domino Web Agent DLL (Windows)

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

To add the Domino Web Agent DLL

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 server's address book.

   In the Filename field you should see names.nsf displayed.
5. Click Open.

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

   The Domino server's administration console 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, for example:

   C:\Program Files\netegritywebagent\bin\
   DOMINOWebAgent.dll

   Note: This entry should be the first in the list of filters.
10. Click Save and Close.
11. Restart the web server.

    You may be required to reboot your machine after the Agent is configured.

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

Configure Domino Web Agents in GUI or Console Mode (see page 160)
How to Configure Any Web Agent in Unattended Mode (see page 183)
Register Your System as a Trusted Host on UNIX (see page 58)

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: **.**/nete-wa-config.bin

      Console mode: ./nete-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.

Add the Domino Web Agent DLL (UNIX)

For the Domino Web Agent to operate properly, you must add the dominowebagent.so library to the filter DLLs. This library must be first in the list.

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

To add the Domino Web Agent DLL

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 server's address book.

   In the Filename field you should see names.nsf displayed.
5. Click Open.

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

   The Domino server's administration console 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, for example:

   web_agent_home>/bin/dominowebagent.so

   Note: This entry should be the first in the list of filters.
10. Click Save and Close.
11. Restart the web server.

How to Install and Configure a SiteMinder Web Agent on a Domino 7 Web Server

To install and configure a SiteMinder Web Agent on a Domino 7 web server, use the following process:

1. Do the following tasks:
   a. Install the Domino web server.
   b. Configure the Domino web server.
   c. Start the Domino web server (on the Windows operating system, start it as an application).

   Note: For more information, see your Domino documentation or online help.
2. Create SiteMinder policies on your SiteMinder Policy Server.

   Note: For more information, see the *SiteMinder Policy Design Guide*.
3. Install the SiteMinder Web Agent.
4. Add the DSAPI settings to your Domino Web Server.
5. Run the SiteMinder Web Agent Configuration wizard.
6. (Optional) Add the CGI settings.
7. (Optional) Add the Alias settings.
8. Enable the Domino Web Agent.
9. For UNIX operating systems, set the environment variables.
10. Restart the Domino web server.

Add the DSAPI Settings to your Domino Web Server

After installing a SiteMinder Web Agent, you must add the DSAPI settings to your Domino web server before running the SiteMinder Web Agent Configuration wizard.

To add the DSAPI settings to your Domino Web Server

1. Open the following URL in a web browser:

   `http://host_name.domain_name:port_number/names.nsf`

   The browser challenges you for your credentials.

2. Enter your credentials.

   The browser displays the names.nsf file.

3. On the left pane, click Configuration, Servers, All Server Documentation.

4. In the center pane, click your web server, and then click the Internet Protocols tab.

5. In the DSAPI section, locate the following item:

   `DSAPI filter file names:`

6. Add one of the following filer files:

   - (Windows) *web_agent_home*\bin\DOMINOWebAgent.dll
   - (UNIX) *web_agent_home*/bin/libdominowebagent.so

   The DSAPI settings are added.

Add the CGI Settings

If you plan to use CGI password services, add the CGI settings to your Domino web server.

To add the CGI settings

1. Open the following URL in a web browser:

   `http://host_name.domain_name:port_number/names.nsf`

   The browser challenges you for your credentials.

2. Enter your credentials.

   The browser displays the names.nsf file.

3. On the left pane, click Configuration, Servers, All Server Documentation.

4. In the center pane, click your web server, and then click the Internet Protocols tab.

5. In the Mapping section, locate the CGI Directory: item, and then add the following value:

   `\domino\html\cgi-bin`

6. Locate the CGI URL Path: item, and then add the following value:

   `/cgi-bin`

   The CGI settings are added.

Add the Alias Settings

The following types of SiteMinder authentication schemes need additional directories containing SiteMinder specific-files on the Domino Web Server:

- HTML-based
- Forms based
- SSL-based

To add the alias settings

1. For any of the previous authentication schemes, do the following:
   a. Navigate to the following directory:

      `\domino\html\`

   b. Create a new subdirectory with the following name:

      `siteminderagent`

   c. Copy the contents of following directory (but not the directory itself) to the siteminderagent subdirectory:

      `web_agent_home``\samples`

   d. Copy the following directory (and all of its contents) to the siteminderagent subdirectory:

      `web_agent_home``\pw`

2. For SSL-based authentication schemes, do the following:
   a. Open the following directory:

      `\domino\html\siteminderagent`

   b. Create a new subdirectory with the following name:

      `certoptional`

   c. Copy the following directory (and all its contents) to the certoptional subdirectory:

      `web_agent_home``\samples`

   The alias settings are added.

Enable the Domino Web Agent

When a SiteMinder Web Agent is enabled, it starts automatically when the web server on which it is installed starts.

To enable the Domino web agent

1. Open the following file with a text editor.

   `WebAgent.Conf`

   Note: On Domino Web Servers, the WebAgent.conf file is in *one* of the following locations:

   - (Windows): C:\lotus\domino
   - (UNIX): $*HOME*/notesdata

2. Change the value of the EnableWebAgent parameter to yes.
3. Save and close the WebAgent.conf file.

   The Web Agent is enabled.

Set the Environment Variables for UNIX Systems

For UNIX operating systems, the SiteMinder environment variables are set by running the following script:

`/local/notesdata/nete_wa_env.sh`

To set the SiteMinder environment variables, run the nete_wa_env.sh script.

Restart the Domino Web Server

After the SiteMinder Web Agent is enabled, and the SiteMinder environment variables are set, restart the Domino Web Server. This starts the SiteMinder Web Agent and protects your resources.

For the Windows operating system, start it as an application.

Note: For more information, see your Domino documentation or online help.

Chapter 10: Configure a z/OS Web Agent

This section contains the following topics:

How to Configure a Web Agent on z/OS

To configure a Web Agent on z/OS, use the following process:

1. Gather the information required to complete the configuration wizard.
2. Run the Configuration wizard to do the following tasks:
   - Configure the Web Agent
   - Register a trusted host
3. Make the following changes manually:
   a. Add directives to the httpd.conf file. If you want to configure an agent manually, you must add the directives listed in all of the following sections:
      - Add Directives to the httpd.conf File After New Installations (see page 171)
      - Add or Verify the Directives After Upgrades (see page 172)
   b. Update the httpd.ewars file
   c. Change and export the _CEE_ENVFILE variable
4. Enable the Web Agent.
5. Restart the web server.

More information:

Enable a Web Agent (see page 192)

Configure the Web Agent and Register Your System As a Trusted Host

After you install the Web Agent, you need to configure it and register the system on which it runs as a trusted host.

Note: You may want to print out a copy of the related worksheet to record your settings before running the wizard.

To configure the Web Agent and register your system as a trusted host

1. Start the Configuration Wizard using *one* of the following commands from the root directory of the SiteMinder Web Agent:

   - sh nete-wa-config.sh (configures the Web Agent with a GUI)

     Note: An X11-based system is required to use the GUI mode.

   - sh nete-wa-config.sh -i console (configures the Web Agent using a console)

   The Configuration Wizard starts.

2. If this is the first time you are configuring this Web Agent, click Yes when you are prompted to register a trusted host. Follow the instructions in the wizard to register the trusted host.

   Note: A trusted host only needs to be registered *once*. If you have previously registered this agent as a trusted host, click No, and then go to the next step.

   The trusted host is registered and the SmHost.conf file is created on the web server.

3. Follow the instructions in wizard to configure the Web Agent.

   The WebAgent.conf file is created on the web server and the Web Agent is configured.

Add Directives to the httpd.conf File After New Installations

After running the configuration script (nete-wa-config.sh), you must add certain directives to the httpd.conf file of the IBM HTTP Server (Domino Go) Web Server in order for the server to run properly with the Web Agent.

To add directives to the httpd.conf file

1. Copy the *webagent_home*/samples folder to the *document_root* location of the web server.

   Example: /usr/lpp/internet/*my_instance*/pub is an example path of a *document_root* location.

   Note: For more information about the location of this directory, see the documentation for your web server.

2. Add the following directives to the httpd.conf file of the IBM HTTP Server (Domino Go) Web Server:

   - To execute PERL files in a given folder:

     Exec *folder_name*/* *path_to_the_folder*/*

     Example: Exec /cgi-bin/* /usr/lpp/internet/*my_instance*/pub/cgi-bin/*

     Note: /usr/lpp/internet/*my_instance*/ is an example of a path to the Web server instance.

   - To specify the document root of the Web server:

     Pass /* *Path_to_the_document_root*/*

     Example: Pass /* /usr/lpp/internet/*my_instance*/pub/*

     Note: /usr/lpp/internet/*my_instance*/ is an example of a path to the Web server instance.

   - To execute the .gif files on the browser:

     Pass *alias_name**.gif

     Pass *alias_name**.gif *path_to_the_folder_containing_the.gif_files*/*.gif

     Example: Pass /siteminderagent/pw/* .gif/usr/lpp/internet/*my_instance*/pub/samples/pw/*.gif

     Note: /usr/lpp/internet/*my_instance*/ is an example of a path to the Web server instance.

   The new directives are added.

Add or Verify the Directives After Upgrades

When upgrading a Web Agent to r6.0 SP6 on z/OS, or configuring a Web Agent manually (not using the wizard) you must make sure that the following directives exist in your httpd.conf file (along with those you added after the installation of the new version).

To add or verify directives after upgrades

Add the following directives to the httpd.conf file of the IBM HTTP Server (Domino Go) Web Server if they are not present:

Note: For SiteMinder 5.x for z/OS, these files were in the *web_agent_home*/lib directory. For SiteMinder 6.x on z/OS, these files are now in the *web_agent_home*/bin directory.

- **To initialize the SiteMinder Web Agent:**

  ServerInit *webagent_home*/bin/GWAPIWebAgent.so:SmInitAgent "path to WebAgent.conf"

  Example: ServerInit /siteminder/v6/webagent/bin/GWAPIWebAgent.so:SmInitAgent "/usr/lpp/internet/*my_instance*/WebAgent.conf"

  Note: /usr/lpp/internet/*my_instance*/ is an example of a path to the Web server instance.

- **For SiteMinder Web Agent authorization**:

  Authorization * *webagent_home*/bin/GWAPIWebAgent.so:SiteMinderAgent.

  Example: Authorization * /siteminder/v6/webagent/bin/GWAPIWebAgent.so:SiteMinderAgent

- **To use the CertOrForm and CertAndForm authentication schemes:**

  Service /siteminderagent/certoptional/forms/*.sfcc *webagent_home*/bin/GWAPIWebAgent.so:SmSSLLoginFcc/samples/forms/*.sfcc

  Service /siteminderagent/certoptional/forms/*.fcc *webagent_home*/bin/GWAPIWebAgent.so:SmLoginFcc/samples/forms/*.fcc

- **To use the forms authentication scheme:**

  Service /siteminderagent/forms/* *webagent_home*/bin/GWAPIWebAgent.so:SmLoginFcc/samples/forms/*

- **To use the French forms authentication scheme:**

  Service /siteminderagent/formsfr/*
  webagent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/formsfr/*

- **To use the Japanese forms authentication scheme:**

  Service /siteminderagent/formsja/*
  webagent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/formsja/*

- **To use the BasicOverSSL authentication scheme:**

  Service /siteminderagent/nocert/*/smgetcred.scc*
  webagent_home/bin/GWAPIWebAgent.so:smGetCred/*

- **To use the CertOrBasic authentication scheme:**

  Service /siteminderagent/certoptional/*/smgetcred.scc*
  webagent_home/bin/GWAPIWebAgent.so:smGetCred/*

- **To use the CertAndBasic and X509Cert authentication schemes:**

  Service /siteminderagent/cert/*/smgetcred.scc*
  webagent_home/bin/GWAPIWebAgent.so:smGetCred/* for CookieProvider:

- **To use the CookieProvider:**

  Service /siteminderagent/SmMakeCookie.ccc*
  webagent_home/bin/GWAPIWebAgent.so:smMakeCookie/*

Update the httpd.ewars File

You must update the httpd.ewars file in the installation root directory of your web server before starting the Web Agent.

To update the httpd.ewars file

1. Open the httpd.ewars file in the in the installation root directory of your web server with a text editor.
2. Locate the LIPATH variable in the file.
3. Add the following directory to the settings of the LIBPATH variable:

   web_agent_home/bin

   Example:
   LIBPATH=/usr/lpp/internet/bin:/usr/lpp/internet/sbin:/usr/lpp/ldap/bin:/usr/lpp/WebSphere/wc/bin:/siteminder/v6/webagent/bin

   Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

   - For Windows installations, the default location is C:\Program Files\netegrity\webagent
   - For UNIX installations, the default location is user_home_directory/netegrity/webagent
   - For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/
4. Save and close the httpd.ewars file.

   The httpd.ewars file is updated.

Sample httpd.envvars File

The following is an example of the httpd.envvars file:

```
PATH=/bin:.:/usr/sbin:/usr/lpp/internet/bin:/usr/lpp/internet/sbin:/usr/lpp/ldap/
bin:/usr/lpp/java/IBM/J1.3/bin
SHELL=/bin/sh
TZ=EST5EDT
LANG=C
LC_ALL=en_US.IBM-1047
NLSPATH=/usr/lib/nls/msg/%L/%N:/usr/lpp/internet/%L/%N:/usr/lpp/ldap/lib/nls/msg/
%L/%N:/usr/lpp/WebSphere/WebServerPlugIn/msg/%L/%N
LIBPATH=/usr/lpp/internet/bin:/usr/lpp/internet/sbin:/usr/lpp/ldap/lib:/usr/lpp/W
ebSphere/wc/lib:/siteminder/v6/webagent/lib
JAVA_HOME=/usr/lpp/java/IBM/J1.3
CLASSPATH=:/usr/lpp/WebSphere/wc/lib
STEPLIB=CURRENT
GSKV3CACHESIZE=1024
GSKV2CACHESIZE=512
```

Change and Export the _CEE_ENVFILE Variable

The _CEE_ENVFILE must be changed for the Web Agent to function.

To change and export the _CEE_ENVFILE variable

1. Set the value of the _CEE_ENVFILE environment variable to the location of the httpd.envvars file and
2. Export the _CEE_ENVFILE variable.

   The variable has been changed and exported.

Chapter 11: Configure Virtual Servers

This section contains the following topics:

How to Set Up Virtual Server Support

A virtual server is a logical entity that you configure on a physical server. This logical entity acts as an independent server. Virtual servers let you host multiple websites on one physical server. For example, using virtual servers, you could set up a server to host both www.mysite.com and www.yoursite.com.

You can assign any of the following to a virtual server:

- A unique IP address
- An IP address that is shared with the physical server
- An IP address that is shared with another virtual server

Although you configure only one Web Agent per web server, you can configure Agent identities to protect your virtual servers. If one user accesses the server through www.mysite.com and another user accesses the server through www.yoursite.com, each server is protected by an agent identity. The advantage of creating an agent identity for each virtual server is that you can define unique realms and rules for each site.

The settings that you define for the Web Agent apply to all virtual servers that you define for that web server instance; however, each virtual server processes requests independently and the Policy Server treats each virtual server request separately. For more information about virtual servers and how to configure them, see the documentation for your web server.

To configure support for virtual servers, do *one* of the following tasks:

- Define and add an Agent identity for each virtual server, specify a value for the AgentName parameter, and assign it the IP address or host header name of a virtual server.
- Define an Agent identity only for virtual servers that need to be uniquely identified.
- Set a Default Agent Name.

Note: If you have more than one instance of the Oracle iPlanet web server, such as a server for HTTP communication and a server for HTTPS communication, two WebAgent.conf files exist. Each file can have multiple agent identities. (The name Oracle iPlanet refers to the web server that was formerly called Sun ONE and iPlanet.)

Add a SiteMinder Wildcard Mapping to Protect IIS 6.0 Virtual Web Sites

SiteMinder automatically protects only the Default Web Site folder of the IIS web server. If you are running virtual web sites on your IIS 6.0 web server, add wildcard mappings to *each* virtual web site that you want to protect. After adding the wildcard mapping to the virtual sites, enable the Web Agent.

To add a SiteMinder wildcard mapping to protect IIS 6.0 virtual web sites

1. Configure virtual servers for the IIS 6.0 web server.

   Note: For more information, see your IIS documentation.

2. Open the IIS Management Console.
3. Right-click on the Virtual Web Site, and then select Properties.

   The Properties dialog appears.

4. Click the Home Directory tab.
5. Click Configuration.

   The Application Configuration dialog appears.

6. In the Wildcard application maps section, click Insert.
7. Click Browse and navigate to the following file:

   web_agent_home\SiteMinder Web Agent\Bin\ISAPI6WebAgent.dll

   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\netegrity\webagent

   Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

8. Click OK twice.

   The Application Configuration and Properties dialogs close.

9. Restart the virtual website.
10. Repeat Steps 3 through 9 for each virtual web site you want to protect.

The IIS Web Agent is ready to be enabled.

Assign Web Agent Identities for Virtual Servers

Additional Web Agents for each virtual server are not actually *defined*, but are *assigned* a Web Agent identity. To protect virtual servers that have unique access requirements or to protect distinct realms, assign each server a unique Agent identity and use the default agent name for all other virtual servers. The advantage of this option is that you can configure your SiteMinder installation quickly, yet still guard virtual servers hosting realms that require separate protection.

The AgentName parameter and its associated IP address provide mapping for web server interfaces to agent names as defined in the policy store. Web Agents need to make Agent API calls in the proper agent name context in order for the correct set of rules and policies to apply. If no Agent name or IP address is assigned for mapping to the policy store, then the Web Agent uses the value of the DefaultAgentName parameter only for a virtual server.

To protect virtual servers using unique Agent identities, add a Web Agent for each virtual server in the AgentName parameter. Adding separate Web Agents for each virtual server lets you define unique realms and rules for each virtual server.

To assign a Web Agent identity

1. Enter the name of the agent and the IP address, separated by a comma.
2. Specify the port number associated with the IP address (for example: 112.12.12.1:8080) if your virtual servers share the same IP address, but use different ports. If you are using default ports, port numbers are not required.
3. To add more than one Agent, put each entry on a separate line, as in the following example:

   ```
   agentname="agent1,123.123.12.12:8080"
   agentname="agent2,123.123.12.12:8081"
   agentname="agent3,123.123.12.13"
   ```

4. If you add an Agent Identity, you must define it in the Policy Server User Interface with the same configuration. Make sure that the Agent Identity is defined in Policy Server User Interface exactly as it is defined for the Agent configuration.

If it finds no entries in the AgentName parameter, SiteMinder uses the value of the DefaultAgentName only for a virtual server.

Note: If you change the DefaultAgentName, make sure that it is defined in the Policy Server User Interface exactly as it is defined for the Agent.

Specify Virtual Servers for the Web Agent to Ignore

If a web server at your site supports several virtual servers, there may be resources on these virtual servers that you do not want to protect with the Web Agent. To simplify how the Web Agent distinguishes which portions of a web server's content it protects, use the following parameter:

IgnoreHost

Specifies the fully qualified domain names of any virtual servers that you want the web Agent to ignore. Resources on such virtual servers will be auto-authorized, and the Web Agent always grants access to them regardless of which client makes the request. The authorization decision is based on the configuration of the Web Agent instead of being based on a policy.

The list of ignored hosts is checked first before any other auto-authorization checks, such as the IgnoreExt and IgnoreURL settings. Therefore, the double-dot rule will not trigger an authorization call to the Policy Server for resources on an ignored host but would not be ignored by extension.

The host portion of the URL entries for the IgnoreHost parameter must exactly match what the Web Agent reads for the host header of the requested resource.

Note: This value is case-sensitive.

If the URL uses a specific port, then the port must specified.

For centrally-managed agents, use a multi-value parameter in the Agent Configuration Object to represent several servers. For agents configured with a local configuration file, list each host on a separate line in the file.

Example: (URL shown with port specified)

IgnoreHost="myserver.example.org:8080"

Example: (local configuration file)

IgnoreHost="my.host.com"

IgnoreHost="your.host.com"

Default: No default

To specify virtual servers for the Web Agent to Ignore, do either of the following tasks:

- For central configuration, add the servers you want to ignore to your agent configuration object. For more than one server, use the multi-value setting for the parameter.
- For local configuration, add a separate line for each server in the local configuration file.

Resources using the specified URLs are ignored by the Web Agent and access to those resources is granted automatically.

Resolve Agent Identity by IP Address

On virtual web servers, when IP addresses and host names are used to resolve the Agent name, the Web Agent can potentially use an incorrect value for AgentName to evaluate the request. This situation would allow unauthenticated users to access protected resources.

You can force the Web Agent to resolve the Agent name based on the physical IP address of the virtual server, with the following parameter:

UseServerRequestIp

Instructs the Web Agent to resolve the AgentName according to the physical IP address of a virtual web server. Use this parameter to increase security if a web server uses IP addresses for virtual server mappings. If this parameter is set to no, the Web Agent resolves the AgentName according to the host name in the HTTP Host header of the client's request.

For Domino servers, this parameter is supported only for Domino 6.x. If this parameter is enabled for an Agent on other Domino versions, the Web Agent uses the default Agent name.

For IIS Web Agents configured for SSL communication and virtual hosts, you must set this parameter to yes. IIS does not allow virtual host mappings using host names with SSL enabled.

Default: No

To resolve a Web Agent's identity using the IP Address, set the UseServerRequestIp parameter to yes.

Chapter 12: 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 nete-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 nete-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 nete-wa-installer.properties file available on your system

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

More Information

Set Up the nete-wa-installer.properties File (see page 229)
Install a Web Agent on a UNIX System (see page 47)
Install a Web Agent on a Windows System (see page 29)

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 nete-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 nete-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. For more information, see the release notes for your SiteMinder component.

   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:

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

   UNIX:

   nete-wa-config.bin -f nete-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 a SiteMinder Agent for IIS or Web Agent on an IIS Web Server (see page 91)
Configure an Oracle iPlanet Web Agent (see page 133)
Configure an Apache Web Agent (see page 145)
Configure a Domino Web Agent (see page 155)
Upgrade a 6.x Web Agent to r6.0 SP6 on Windows Systems (see page 80)

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.

Dynamic Policy Server Clusters

In previous versions of SiteMinder, Web Agents did *not* automatically discover if a particular Policy Server had been added to or removed from a cluster. The Web Agents recognized the changes only after their respective web servers were restarted.

SiteMinder r6.0 SP6 supports dynamic Policy Server clusters. When dynamic Policy Server Clusters are enabled, Web Agents automatically discover any additions or removals of individual Policy Servers from an existing cluster.

For example, if your Web 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

and you decide to remove the server 192.168.2.103 to upgrade its operating system, enabling dynamic Policy Server clusters lets your Web Agents recognize the change in the membership of the cluster without restarting.

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

- 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.

To connect a Web Agent to a dynamic Policy Server cluster

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\netegrity\webagent

   Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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 13: Starting and Stopping Web Agents

This section contains the following topics:

Disable a Web Agent

If you want to stop the Web Agent from protecting the resources on your web server and stop communicating with the Policy Server, you must disable the Web Agent.

To disable a Web Agent

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

   Note:SiteMinder r6.0 SP6 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.

Enable a Web Agent

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

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

To enable a Web Agent

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

   Note:SiteMinder r6.0 SP6 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.

Chapter 14: 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 required, allocate 4KB/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 need large cache capacity.

     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, system-wide.

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, semmnu should be greater than the number of Apache child processes or Oracle iPlanet web server processes running on the system at any one time. For Apache servers, this value should exceed the maxclients setting by 200 or more. For Oracle iPlanet web servers, this value should exceed the maxprocs setting by 200 or more.

Example: (Solaris 9) 200

Example: (Solaris 9) 400

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

You may want to tune the resource controls at the project level if you need to improve the performance of the Web Agent.

Note: See your Solaris documentation for more information.

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

1. Determine the project 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 15: 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\jsafe.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.

More Information

How to Configure the ServletExec Servlet Engine for JSP Password Services on an Oracle iPlanet Web Server in the UNIX Operating Environment (see page 200)
How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server (see page 199)

How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server

To configure the ServletExec Servlet Engine for SiteMinder JSP-based Password Services, use the following process:

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

1. Open the ServletExec Administration interface.
2. Add the following items to the classpath of the virtual machine:

   web_agent_home\jpw\jpw.jar

   web_agent_home\java\jsafe.jar

   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\netegrity\webagent

   Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

3. Make the following modifications to the top-level web.xml file of your web application.
   a. Add the following servlet:.
      - Servlet Name: PSWDChangeServlet
      - Servlet Class: PSWDChangeServlet
   b. Create the following servlet mapping:
      - URL pattern: /siteminderagent/pwservlet/PSWDChangeServlet
      - Servlet Name: PSWDChangeServlet
4. Repeat Step 3 for each web.xml file of your web application.

How to Configure the ServletExec Servlet Engine for JSP Password Services on an Oracle iPlanet Web Server in the UNIX Operating Environment

To configure the ServletExec Servlet Engine for JSP Password Services on a Oracle iPlanet Web server in the UNIX operating environment, use the following process:

1. Use the Oracle iPlanet Web server to make the following changes to the web server instance on which your SiteMinder Web Agent runs:
   a. Add the following legacy servlet attributes:
      - Servlet Name: PSWDChangeServlet
      - Servlet Code: PSWDChangeServletServlet
      - Classpath: *web_agent_home*/jpw/jpw.jar

      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\netegrity\webagent

      Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

   b. Add the following virtual path to the Servlet Virtual Path Translation of the Legacy Servlets:

      `/siteminderagent/pwservlet/PSWDChangeServlet and Servlet Name: PSWDChangeServlet`

   c. Disable the Oracle iPlanet servlet engine.
2. Install the ServletExec ASAPI software.
3. Use a text editor to update the *ServletExec_installation_directory*/se-*instance_name*/StartServletExec file with the following modifications:
   a. Find PORT="8888", and change the port of communication with web server to any free port (for example, PORT="7777").
   b. Extend the CLASSPATH definition by adding the following entries to the end of the CLASSPATH:

web_agent_home/jpw/jpw.jar

web_agent_home/java/jsafe.jar

c. Extend the document directories definition by adding the directory entries after the following line:

$SENAME $HOMEDIR $MIMEFILE $DOCROOTDIR -port $PORT $SEOPTS -addl "/siteminderagent/jpw=*web_agent_home*/jpw""

Note: There are two quotation marks at the end of the entry.

4. Start the ServletExec Servlet engine, and then use its Administrative interface to do the following:

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

a. Add the following servlets:

- Servlet Name: PSWDChangeServlet
- Servlet Class: PSWDChangeServlet

b. Add the following Servlet Alias:

- alias: /siteminderagent/pwservlet/PSWDChangeServlet
- Servlet Name: PSWDChangeServlet

5. Make the following changes to the magnus.conf file of the Oracle iPlanet web server on which your Web Agent runs:

a. For the following line, change the IP address and port number to match the address for the Agent system that you already defined:

```
Init fn="ServletExecInit" instance_name.instances="IP_address:7777"
```

6. Add the following entry to the obj.conf file the Oracle iPlanet server instance on which your Web Agent runs:

```
NameTrans fn="assign-name" from="/siteminderagent/pwservlet/PSWDChangeServlet"
name="instance_name"
```

Insert the entry into the following block:

```
<Object name="default">

AuthTrans fn="SiteMinderAgent"

NameTrans fn="assign-name" from="/servlet/*" name="instance_name"

NameTrans fn="assign-name" from="/siteminderagent/pwservlet/PSWDChangeServlet"

name="instance_name"

-----

-----

</Object>
```

7. Restart the Oracle iPlanet web server, and then start the ServletExec Servlet engine.

Chapter 16: 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 r6.0 SP6 Platform Matrix at Technical Support.

Set JRE in PATH Variable Before Uninstalling the Web Agent

On Windows and UNIX systems, when you are uninstalling the Web 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."

To set the JRE in the PATH variable:

On Windows

a. Go to the Control Panel.

b. Double-click System.

c. In the Environment Variables dialog, add the location of the JRE to the PATH system variable.

For example, C:\j2sdk1.5.0_01\jre\bin

On Solaris

Run these two commands:

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

where *JRE* is the location of your JRE.

For example, /usr/bin/j2sdk1.5.0_01/jre

b. export PATH

Uninstall a Web Agent from a Windows Operating Environment

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

Note: To remove the SiteMinder Web Agent for IIS from a server farm, run the uninstall program on *each* node in the farm. Start by removing the Web Agent from first web server in the farm, and then remove the Web Agent from all other nodes. The first server refers to the IIS web server where the shared configuration information is stored. A node refers to any IIS web servers which read the shared configuration from the first server.

To uninstall a Web Agent from a Windows operating environment

1. Stop the web server.
2. Click Start, Control Panel, Programs and Features.

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

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

   The wizard removes the Web Agent.

Uninstall Documentation from a Windows System

Running the documentation uninstallation program removes the manuals for all products from the netegrity_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 uninstallation.

Note: Removing a Web Agent from a 64-bit Suse Linux 10 system requires additional preparations (see page 209).

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 will help guide you through the process.

Note: Before you uninstall, you may want to make copies of your Web Agent configuration settings to have as a back up.

1. Stop the web server.
2. Log into 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/nete-wa-uninstall
5. If necessary, ensure 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 box 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. Optionally, if you are uninstalling an Apache Web Agent, 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 server(s).

Note: For Oracle iPlanet web servers, the obj.conf, magnus.conf, and mime.types files are restored to its original settings prior to the Web Agent installation.

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/netegrity-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.

Uninstall a Web Agent from a 64-bit Suse 10 Linux System

To use a SiteMinder Web Agent version *earlier than* r6. SP5 CR6, on a 64-bit Suse 10 Linux operating system, run a script that modifies the original SiteMinder executable file *before* doing any of the following tasks:

- Installing
- Configuring
- Uninstalling

The script creates a backup (.bak) of the original SiteMinder executable file, and then creates a modified copy that you must use in place of the original file.

This script is available from Novell, at their support web site. Search for the following document number:

- 3505148

Run the script only once on each type of SiteMinder executable listed previously. For example, if you have already run the script on the installation file, you can use the modified installation file to install additional Web Agents in the future without running the script.

Uninstall the Web Agent from z/OS

You can remove the SiteMinder Web Agent from a z/OS system.

To uninstall the Web Agent from a z/OS system

1. Navigate to a directory *above* the *web_agent_home* directory.

   Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

   - For Windows installations, the default location is C:\Program Files\netegrity\webagent
   - For UNIX installations, the default location is user_home_directory/netegrity/webagent
   - For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

2. Run the following command:

   ```
   rm-rf web_agent_home_directory
   ```

3. Remove the WebAgent.conf file from the root directory of your web server.

   Note: For more information about the location of this directory, see the documentation for your web server.

4. Locate and remove the following directives from the httpd.conf file of your web server:

   - SiteMinder Web Agent initialization:

     ```
     ServerInit web_agent_home/bin/GWAPIWebAgent.so:SmInitAgent
     "path_to_WebAgent.conf"
     ```

   - SiteMinder Web Agent authorization:

     ```
     Authorization * web_agent_home/bin/GWAPIWebAgent.so:SiteMinderAgent.
     ```

   - CertOrForm and CertAndForm cert schemes:

     ```
     Service /siteminderagent/certoptional/forms/*.sfcc
     web_agent_home/bin/GWAPIWebAgent.so:SmSSLLoginFcc/samples/forms/*.sfcc
     Service /siteminderagent/certoptional/forms/*.fcc
     web_agent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/forms/*.fcc
     ```

   - Form scheme:

     ```
     Service /siteminderagent/forms/*
     web_agent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/forms/*
     ```

   - French Scheme:

     ```
     Service /siteminderagent/formsfr/*
     web_agent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/formsfr/*
     ```

   - Japanese Scheme:

```
Service /siteminderagent/formsja/*
web_agent_home/bin/GWAPIWebAgent.so:SmLoginFcc/samples/formsja/*
```

- BasicOverSSL Scheme:

```
Service /siteminderagent/nocert/*/smgetcred.scc*
web_agent_home/bin/GWAPIWebAgent.so:smGetCred/*
```

- CertOrBasic Scheme:

```
Service /siteminderagent/certoptional/*/smgetcred.scc*
web_agent_home/bin/GWAPIWebAgent.so:smGetCred/*
```

- CertAndBasic and X509Cert Schemes:

```
Service /siteminderagent/cert/*/smgetcred.scc*
web_agent_home/bin/GWAPIWebAgent.so:smGetCred/*
```

- CookieProvider:

```
Service /siteminderagent/SmMakeCookie.ccc*
web_agent_home/bin/GWAPIWebAgent.so:smMakeCookie/*
```

The Web Agent is removed from your system.

Chapter 17: Troubleshooting

This section contains the following topics:

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 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 Won't Start Following Upgrade from SiteMinder r5.x

Valid on Windows Server 2003

Symptom:

My Web Agent will not start after I upgraded from SiteMinder r5.x to r6.x and restarted my IIS web server. The Windows Event Viewer shows message descriptions similar to the following:

- Unable to load SiteMinder host configuration object or host configuration file.
- SiteMinder agent has encountered initialization errors and will not service requests.

Solution:

Verify that the NETWORK SERVICE account (or any user account that runs the IIS web server) has the following permissions for the SmHost.conf file on your IIS web server:

- Read
- Write
- Modify

"Error reinitializing event with key base 0x0.2x" Message After Upgrade from SiteMinder r5.x to r6.x

Valid on Solaris

Symptom:

After upgrading the Web Agent from r5.x to r6.x, the following message appears:

```
Error reinitializing event with key base
```

Solution:

The Web Agent uses semaphores. This error usually occurs when the semaphores used by the Web Agent are deleted. For example, if you run a chron job to delete semaphores on a regular basis, the Web Agent does not after the semaphores it was using are removed. In this situation, do *one* of the following:

- Stop running the job which removes the semaphores.
- Restart the web server on which the Web Agent runs after running the job.

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.

Connectivity and Trusted Host Registration Issues

This section contains troubleshooting information related to trusted host registration.

smreghost Command Causes Core Dump

Valid on Linux RHAS3.0

Symptom:

When I try to register a trusted host, the smreghost command fails with a core dump.

Solution:

Upgrade (to 6.x SP5 CR 24), and then re-compile, the following SiteMinder components:

- Web Agent
- Policy Server

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\netegrity\webagent

  Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

- 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 Policy Server User Interface, 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.

More Information

Fix the ServletExec CLASSPATH for DMS (see page 46)

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 nete-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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

Attempt to Access DMS Page Returns Error

Valid on Windows

Symptom:

On Windows systems, you receive a servlet DMS not found error when you access a DMS page.

Solution:

Check the ServletExec CLASSPATH and modify it if necessary.

More information:

Fix the ServletExec CLASSPATH for DMS (see page 46)

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.

"WebServer {0} , listed in properties file, could not be located on this system"

Reason:

The settings in the nete-wa-installer.properties file are not correct.

Action:

Verify the settings in the nete-wa-installer.properties file, and run the installer again.

More information:

nete-wa-installer.properties File (see page 229)
Verify the Properties File Settings for Apache Web Agent Installations (UNIX) (see page 231)

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 194)
How to Tune the Solaris 10 Resource Controls (see page 196)

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 made by the Agent configuration to the obj.conf were applied. Re-configure the Web Agent.

Sun Java System Web Server Fails at Runtime

Symptom:

Oracle iPlanet web server is failing at run time.

Solution:

Increase the StackSize setting in the Oracle iPlanet server's magnus.conf file to a value of 256 KB. The magnus.conf file is located in:

Sun_Java_System_home/*web_server_instance*/config

More Information

Tune the Shared Memory Segments (see page 194)

Apache Web Agent Issues

This section lists troubleshooting information for the Apache Web Agent.

More Information

Tune the Shared Memory Segments (see page 194)

Apache Server Starts But Web Agent Is Not Enabled

Symptom:

The Apache Agent is not enabled even though the web server has started.

Solution:

Do the following tasks:

- Open the WebAgent.conf file, and then set EnableWebAgent to yes.
- Compile the Apache web server to include the mod_so Apache module .
- Modify the httpd.conf file so it to loads the mod_sm SiteMinder Agent Module.
- Modify the httpd.conf file to initialize the Agent, using the SmInitFile entry.
- For Apache Agents on HP-UX systems, modify the httpd.conf file to add the mod-hpaCCso.c SiteMinder Agent Module.

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.

CGI Password Services Return an Error

Valid on UNIX

Symptom:

My Apache web server log shows a 500 error, and SiteMinder displays a diagnostic page when I try to access CGI password services.

Solution:

Add the library path to the Global Environment section of the httpd.conf file of your Apache web server. For example:

```
PassEnv LD_LIBRARY_PATH <web_agent_home>/lib
```

Note: The *web_agent_home* variable indicates the installed location of the Web Agent, as shown in the following examples:

- For Windows installations, the default location is C:\Program Files\netegrity\webagent
- For UNIX installations, the default location is user_home_directory/netegrity/webagent
- For z/OS installations, the default location is /siteminder/v_*number_of_version*/webagent/

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 158)

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.

Appendix A: Set Up the nete-wa-installer.properties File

This section contains the following topics:

nete-wa-installer.properties File

The nete-wa-installer.properties file is generated during a Web Agent installation and configuration. It contains all of the parameters, paths, and passwords entered during the installation and configuration.

During an unattended installation and configuration, this properties file provides the settings that would be entered by an end-user in a GUI or Console mode installation. Be default, the nete-wa-installer.properties file contains the settings from the initial installation. You can use the default properties file to run installations with the same settings or use the file as a template that you modify to suite your environment.

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 web server, and then properties file to run an unattended installation 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\\netegrity\\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

Verify the Properties File Settings for Apache Web Agent Installations (UNIX)

Before running an unattended installation of a SiteMinder Web Agent on an Apache web server for the UNIX operating environment, verify that the nete-wa-installer.properties file contains values for the following settings:

APACHE_SELECTED=1

Specifies an Apache web server installation.

Limit: 1

APACHE_WEBSERVER_ROOT=*directory_path*

Specifies the /conf subdirectory located in the root directory of the Apache web server.

Example: /opt/IBM/HTTPServer/conf

APACHE_SPECIFIC_PATH_YES=*number*

Uses a number to indicate *one* of the following types of Apache web server:

- Original Apache web sever. Set the value of this parameter to zero.
- Apache-based web server (an Apache web server customized for and available from a third-party vendor, such as Oracle, IBM, and others). Set the value of this parameter to one.

Limits: 0, 1

Example: 1

APACHE_VENDOR_TYPE=*server_type*

Specifies the third-party vendor of the Apache-based web server. Choose from the following:

- HP_APACHE—HP Apache server.
- HTTP_APACHE—HTTP Apache server.
- IBM_HTTP—IBM HTTP server.

Default: None

APACHE_VERSION=*number.number*

Specifies the version of the Apache or Apache-based web server being installed.

Limits: 1.0, 2.0

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\\netegrity\\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 235)

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 B: 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/netegrity/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/netegrity/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\netegrity\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 C: 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:

Library Path for the Web Server is Set for UNIX Systems

The library path for the Apache web server is required because it enables the Apache server to load libraries correctly on a UNIX system. For example:

export LD_LIBRARY_PATH *web_agent_home*/bin

The library path variable depends on the operating system—it should always point to *web_agent_home*/bin.

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

The following table lists the variables.

Operating System	Path Variable
Solaris	LD_LIBRARY_PATH

Operating System	Path Variable
HP-UX	SHLIB_PATH
LINUX	LD_LIBRARY_PATH
AIX	LIBPATH

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\netegrity\webagent

Default (UNIX/Linux installations): user_home_directory/netegrity/webagent

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

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

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.

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

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

Appendix D: 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

Appendix E: Worksheets

This section contains the following topics:

Web Agent Installation Worksheet

Use this worksheet to gather the required information before running the Web Agent installer.

Information Needed	Your Value
Web Agent installation location (if not using the default)	

Web Agent Configuration Worksheet

Use this worksheet to gather the required information before configuring the SiteMinder Web Agent.

Information Needed	Your Value
(Optional) PKCS11 DLL File location	
(Optional) Token Label	
(Optional) Token Passphrase	
Admin User Name	
Admin Password	
Enable Shared Secret Rollover	
Trusted Host Name	
Host Configuration Object	
Policy Server IP Address	
Policy Server Port Numbers (if not using the default)	

Information Needed	Your Value
SmHost.conf file location (if not using the default)	

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W

X