CA SiteMinder®

Web Agent Installation Guide for IIS
r12.5

CA Technologies Product References

This document references the following CA Technologies products:

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

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

- How to Upgrade an Agent for IIS from Version 12.0.2 or Lower (see page 46)—Revised upgrade procedures for upgrading from versions 12.0.3 or older to r12.5 to resolve CQ 170479 and STAR Issue 21402742:01.

- Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode (see page 29)—Added new instructions for verifying the ISAPI filter placement. Resolves CQ 170576 and STAR Issue 21403389:01

- How to Prepare for an Agent for IIS Installation on your web server (see page 12)—Removed reference to Visual C++ 2005 Redistributable Package (x64) prerequisite. The installer now adds this package if it does not exist. Resolves CQ171379

Contents

Chapter 4: Dynamic Policy Server Clusters   53

Chapter 5: Starting and Stopping Web Agents   55

Chapter 6: Uninstall a Web Agent   57

Chapter 7: Troubleshooting   63

Appendix A: Worksheets   69

Index   71

Chapter 1: Preparation

This section contains the following topics:

Only IIS Web Server Procedures in this Guide

This guide only contains procedures for installing or configuring the SiteMinder Agent for IIS on the Windows operating environment.

To install or configure a SiteMinder agent on any other type of web server or operating environment, see one of the following guides:

■ *Web Agent Installation Guide for Apache-based servers*.

■ *Web Agent Installation Guide for Domino*.

■ *Web Agent Installation Guide for Oracle iPlanet*.

Hardware Requirements for SiteMinder Agents

Computers hosting SiteMinder agents require the following hardware:

Windows operating environment requirements

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

■ CPU: x86 or x64

■ Memory: 2-GB system RAM.

■ Available disk space:

  – 2-GB free disk space in the installation location.

  – .5-GB free disk space in the temporary location.

Combined Functions in New Agent for Internet Information Services (IIS) Web Servers

SiteMinder r12.5 combines all functions for Internet Information Services (IIS) into one agent.

SiteMinder Agent for IIS

A SiteMinder Web Agent for IIS implemented as an ISAPI plug-in and a native HTTP module that supports the following functions:

- Application pools using Integrated or Classic pipeline mode.

- Application pools that are configured with the Enable 32-bit applications option.

- The optional IIS Application Request Routing (ARR) feature.

- Supported with IIS 7.0 and 7.5, including IIS clusters and shared configuration deployments.

Multiple Agent for IIS Directory Structures According to Operating Environment

The directory structure added to your IIS web server for your Agent files varies according to the operating environment of your IIS web server. The following directory structures exist:

- SiteMinder Web Agents and [set AGENT value for your book]s for IIS use the directory structure shown in the following illustration:

```
\webagent                          32-bit Operating Environments
    ├── \affwebservices
    ├── \bin
    ├── \config
    ├── \affwebservices
    ├── \etpki-install
    ├── \install_config_info
    ├── \java
    ├── \jpw
    ├── \jpw_default
    ├── \log
    ├── \pw
    ├── \pw_default
    ├── \samples
    ├── \samples_default
    ├── \secureforms
    ├── \sharepoint
    └── \tools
```
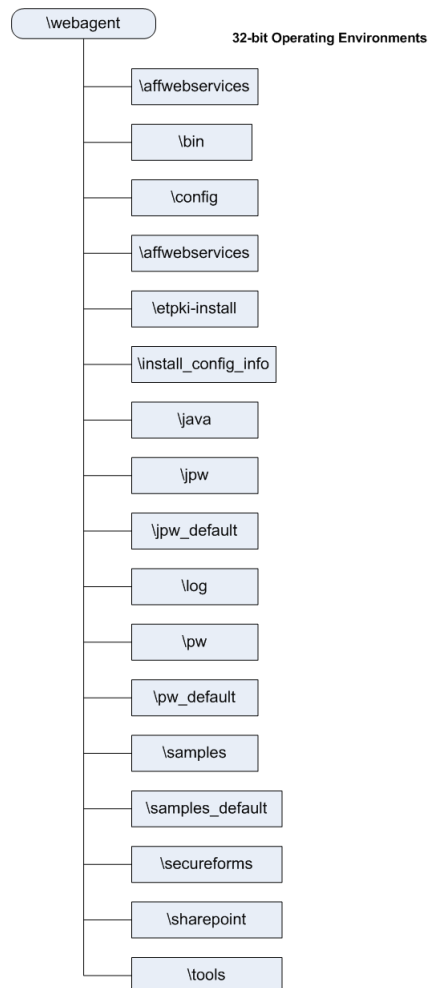
- SiteMinder Agents for IIS installed on 64-bit operating environments use the directory structure shown in the following illustration:

More information:

SiteMinder Agent Preparation Roadmap

The following illustration describes how to prepare your Windows operating environment for the SiteMinder agent for IIS:
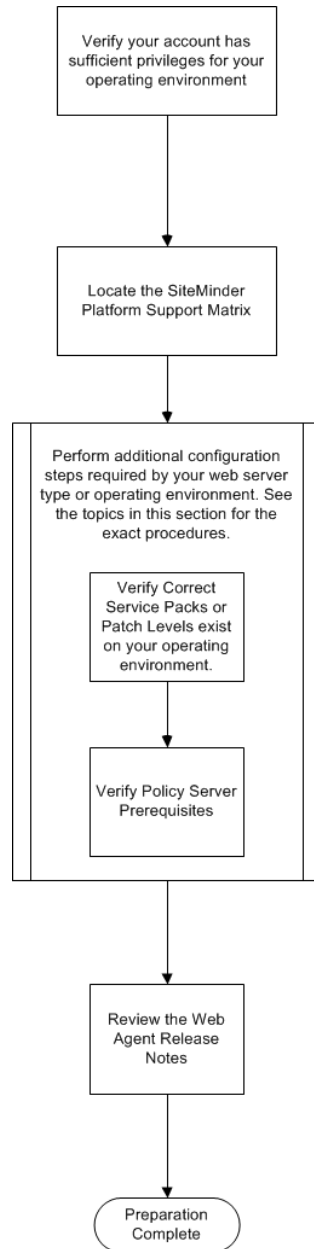
How to Prepare for an Agent for IIS Installation on your web server

To prepare for an Agent for IIS installation on a Windows operating environment, use the following process:

1. Verify that you have an account with Administrative privileges for the computer on which you want to install the agent (see page 12).

2. Verify that the IIS role, the related role services and features are installed on your Windows operating environment (see page 13).

3. Locate the SiteMinder Platform Support Matrix (see page 13). Confirm that your IIS web server meets the requirements for the agent version you want to install.

4. Verify that the Windows operating environment for your IIS web server has the proper service packs and updates installed (see page 14).

5. Confirm that your Policy Server has the prerequisites for an agent Installation (see page 14).

6. Review the *Web Agent Release Notes* for known issues (see page 16).

Verify that you have an Account with Administrative Privileges on the Windows Computer Hosting your IIS Web Server

To install or configure a SiteMinder Web Agent or SiteMinder Agent for IIS on an IIS web server, you need an account with Administrator privileges.

For Windows 2008 systems, do one of the following actions to install or configure a SiteMinder Web Agent or SiteMinder Agent for IIS:

- If you are using Windows Explorer, right-click the .exe file. Then select Run as Administrator.

- If you are using a command line, open a new console window with administrative privileges. Then run the command that you want.

Note: For more information about installing or configuring SiteMinder Web Agents or SiteMinder Agents for IIS on Windows 2008 systems, see the Web Agent Release Notes.

Verify that the IIS Role, and the Related Role Services are Installed

The IIS (web server) role is *not* enabled by default. Verify that the IIS role is installed and enabled on each Windows system, before installing the Agent for IIS.

Follow these steps:

1. Click Start, All Programs, Administrative Tools, Server Manager.

   The Server Manager appears.

2. Verify that IIS appears in the Roles list.

3. If the Web Server (IIS) role is not shown, add it using the Add Roles wizard. If you decide to use the ISAPI-filter functions of the Agent for IIS, add the following role services too:

   - ASP.NET

   - CGI

   - ISAPI Extensions

   - ISAPI Filters

   - IIS Management Console

   - Windows Authentication (for the SiteMinder Windows Authentication Scheme)

Locate the Platform Support Matrix

Use the Platform Support Matrix to verify that the operating environment and other required third-party components are supported.

Follow these steps:

1. Log in to the CA Support site.

2. Locate the Technical Support section.

3. Enter SiteMinder in the Product Finder field.

   The SiteMinder product page appears.

4. Click Product Status, SiteMinder Family of Products Platform Support Matrices.

Note: You can download the latest JDK and JRE versions at the Oracle Developer Network.

Verify that the Windows Operating Environment for your IIS Web Server has the Proper Service Packs and Updates Installed

We recommend using Windows Update to verify that your Windows operating environment contains the latest Service Packs and updates, before installing a SiteMinder Agent for IIS.

Review the Policy Server Prerequisites for Agent for IIS Installations

Your SiteMinder Agent for IIS needs the following information about the Policy Servers to which it connects:

- The IP addresses of the Policy Servers
- Certain SiteMinder object names in the Policy Server

The Administrative UI creates these SiteMinder objects in the Policy Server. We recommend creating them before installing your agent to avoid going between your web server and the Administrative UI interfaces later.

SiteMinder Agents for IIS require the names of the following SiteMinder objects stored the Policy Server:

Host Configuration Object

Contains the settings that the agent uses for subsequent connections to a Policy Server following the initial connection that the agent made.

Admin User Name

Identifies the name of a SiteMinder user with the following privileges:

- Administrative privileges
- Trusted host registration privileges

Admin Password

Identifies a password that is associated with the Admin User Name in the SiteMinder Policy Server.

AgentName

Defines the identity of the Web Agent. This identity establishes a mapping between the name and the IP address of each web server instance hosting an Agent.

When no matching value exists, the agent uses the value of from the DefaultAgentName parameter instead.

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

Default: No default

Limit: Multiple values are allowed, but each AgentName parameter has a 4,000 character limit. Create additional AgentName parameters as needed by adding a character to the parameter name. For example, AgentName, AgentName1, AgentName2.

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

Example: myagent1,192.168.0.0 (IPV4)

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

Example: myagent, www.example.com

Review the Web Agent Release Notes for Known Issues

The most-recent versions of the Web Agent Release notes are available from the CA Support website. We recommend reviewing them before installing or configuring a SiteMinder agent.

Follow these steps:

1. Open a web browser and navigate to the Technical Support website.

2. Click Enterprise/Small and Medium Business.

   The Support for Businesses and Partners page appears.

3. Under the Get Support tab, click Product Documentation.

   The documentation page appears.

4. Click the field under Select a Bookshelf.

5. Type siteminder.

   A list of SiteMinder bookshelves appears.

6. Click the bookshelf that you want from the list, and then click Go.

   The bookshelf opens (in a new window or tab, depending on your browser settings).

7. Click Release Notes.

   A list of release notes appears.

8. Click *one* of the following links to display the Release Notes in format you want:

   ■ View HTML

   ■ Download PDF

   Note: You need the Adobe Reader software to view PDF documents. Click the Download Adobe Reader link in the bookshelf.

Chapter 2: Install an Agent for IIS on Windows Operating Environments

This section contains the following topics:

Agent Installation Compared to Agent Configuration

The concepts of installation and configuration have specific meanings when used to describe SiteMinder agents.

Installation means installing the SiteMinder agent software on a computer system. For example, installing an agent creates directories and copies the SiteMinder agent software and other settings to the computer.

Configuration occurs after installation and means the act of preparing the SiteMinder agent software for a specific web server on a computer. This preparation includes registering the agent with SiteMinder Policy Servers, and creating a runtime server instance for the web server that is installed on the computer.

Use the wizard-based installation and configuration programs to install and configure your agent on your first web server. The wizard-based programs create a .properties file.

Use the .properties file and the respective executable file to install or configure the agent silently on additional web servers.

Agent for IIS Installation and Configuration Roadmap

The following illustration describes the process installing and configuring a SiteMinder Agent for IIS:
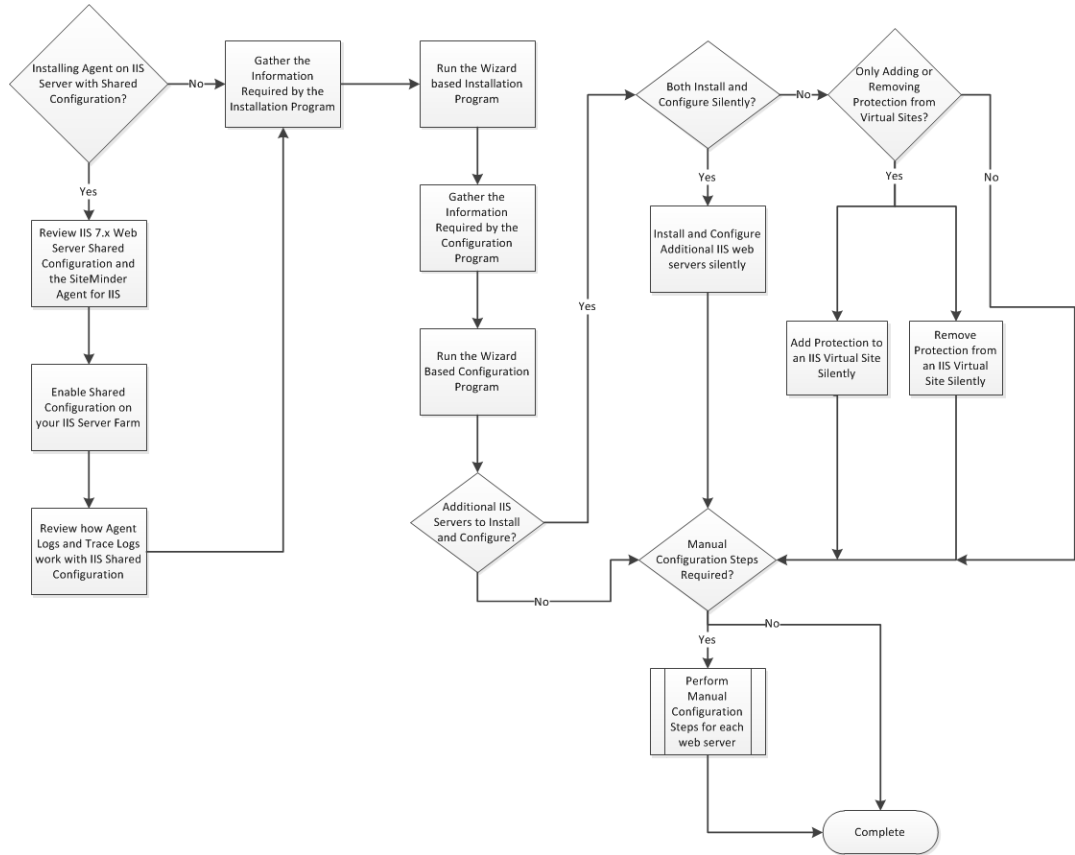
How to Install and Configure a SiteMinder Agent for IIS

Installing and configuring the SiteMinder Agent for IIS involves several separate procedures. To install and configure the Agent for IIS, use the following process:

1. If you are deploying the Agent for IIS to an IIS server farm, review the following topics:

   - IIS 7.x web server shared configuration (see page 19).

   - How web agent logs and trace logs work with shared configuration (see page 21).

2. Gather the information for the installation program (see page 23).

3. Run the wizard based installation program (see page 23).

4. Gather the information for the configuration program (see page 24).

5. Run the wizard based configuration program (see page 28).

6. Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode (see page 29)

7. (Optional) Install and configure additional Agents for IIS silently (see page 30).

8. (Optional) Add (see page 32) or remove (see page 34) SiteMinder protection from virtual sites on IIS web servers silently.

9. Determine if your Agent for IIS requires any manual configuration steps (see page 38).

IIS 7.x Web Server Shared Configuration and the SiteMinder Agent for IIS

IIS 7.x web servers support shared configurations that streamline the configuration process for an IIS a server farm.

Starting with SiteMinder r12.5, the Agent for IIS can protect resources on IIS server farms that use the shared configuration feature of IIS 7.x.

Note: This feature works *only* with the SiteMinder r12.5 Agent for IIS 7. Older versions of the SiteMinder Web Agent do *not* support this feature.

IIS 7.x uses network shares to propagate the configuration information across the server farm. The SiteMinder r12.5 Agent for IIS, however, *cannot* operate on network shares. Using a SiteMinder r12.5 Agent for IIS on an IIS server farm involves several separate procedures.

For example, suppose you have three IIS 7.x web servers, with all of them using a shared configuration. Web server number one is your primary web server, which contains the configuration information for the farm. Web servers 2 and 3 are nodes that connect to the network share on web server one to read the configuration information.

The entire installation and configuration process for using the SiteMinder Agent for IIS on all three IIS 7.x web servers is described in the following illustration:
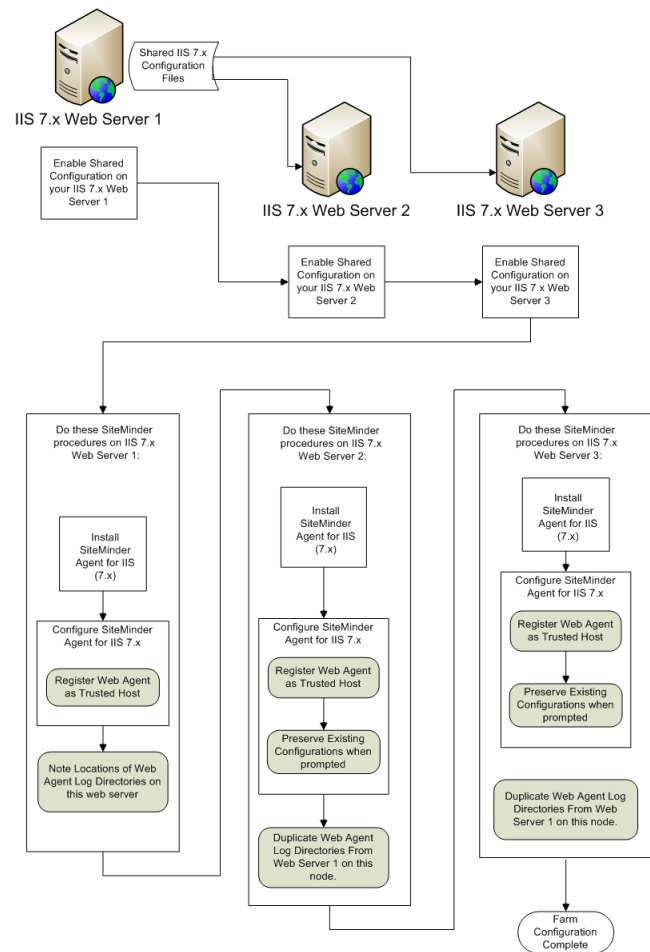
How Web Agent Logs and Trace Logs Work with IIS 7.x Web Server Shared Configuration

For SiteMinder Agents for IIS running on an IIS server farm, create duplicate log and trace file directories on each node if all the following conditions are true:

- Your Agent for IIS log and trace log directories are specified in an Agent Configuration Object on the Policy Server (*not* in a local configuration file).

- Any of the SiteMinder Agents for IIS in your IIS 7.x web servers in the server farm share the same Agent Configuration object

- Your Agent for IIS log file and trace log directories specified in the shared Agent Configuration Object are *different* than the following default settings:

    - *web_agent_home*\win32\log (for Windows IIS 7.x 32-bit)

    - *web_agent_home*\win64\log (Windows IIS 7.x 64-bit)

If all of the previous conditions exist in your server farm, use the following process to enable your Web Agent logs and trace logs:

1. Create a custom log directory on the IIS 7.x web server that contains the shared configuration for the farm.

2. Grant the application pool identities associated with your protected resources the following permissions to the custom directory on the previous IIS 7.x web server.

    - Read

    - Write

3. Create the same custom log directory on a IIS 7.x web server node in the farm.

4. Grant the application pool identities associated with your protected resources the following permissions to the custom directory on the a IIS 7.x web server node in the farm.

    - Read

    - Write

5. Repeat steps 3 and 4 on all other nodes in your server farm.

For example, suppose you have three IIS 7.x web servers, with all of them using a shared configuration. Web server number one is your primary web server, which contains the configuration information for the farm. Web servers 2 and 3 are nodes that connect to the network share on web server one to read the configuration information.

The entire process for configuring these logs is described in the following illustration:
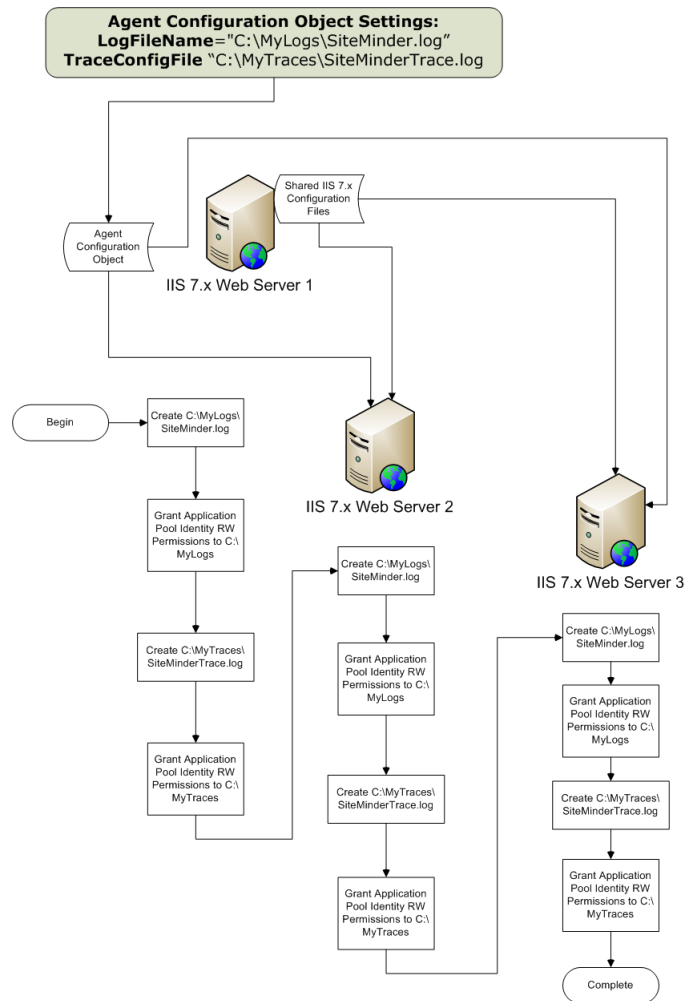
Gather the Information for the Agent Installation Program for the Windows Operating Environment

Before running the installation program for the SiteMinder Agent for IIS on the Windows operating environment, gather the following information about your web server:

Installation Directory

Specifies the location of the SiteMinder agent binary files on your web server. The *web_agent_home* variable is set to this location.

Limit: SiteMinder requires the name "webagent" for the bottom directory in the path.

Shortcut Location

Specifies the location in your Start menu for the shortcut for the Web Agent Configuration wizard.

Run the Installation Program on Windows

The installation program for the SiteMinder agent installs the agent on one computer at a time using the Windows operating environment. This installation program can be run in wizard or console modes. The wizard and console-based installation programs also create a .properties file for subsequent installations and configurations using the unattended or silent method with the same settings.

For example, suppose the Agents in your environment use the same web server version, installation directory, Agent Configuration Object and Policy Servers. Use the installation wizard or console-based installation program for your first installation. Afterwards, you could create your own script to run the installation program with the .properties file the wizard or console-based installation program created.

Follow these steps:

1. Copy the SiteMinder Web Agent installation executable file to a temporary directory on your web server.

2. Do *one* of the following steps:

   ■ For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.

   ■ For console-based installations, open a command line window and run the executable as shown in the following example:

   executable_file_name.exe -i console

3. Use the information that you gathered previously to complete the installation.

More information:

Gather the Information for the Agent Configuration Program for IIS Web Servers

Before configuring a <stmdnr> Agent on an IIS web server, gather the following information about your SiteMinder environment.

Host Registration

Indicates whether you want to register this agent as a trusted host with a SiteMinder Policy Server. Only one registration per agent is necessary. If you are installing the SiteMinder Agent for IIS 7.x on an IIS server farm, register all IIS agents in the farm as trusted hosts.

Limits: Yes, No

Admin User Name

Specifies the name of a SiteMinder user account that has sufficient privileges to create and register trusted host objects on the Policy Server.

Admin Password

Specifies the password that is associated with the SiteMinder user account that has sufficient privileges to create and register trusted host objects on the Policy Server.

Confirm Admin Password

Confirms the password that is associated with the SiteMinder user account that has sufficient privileges to create and register trusted host objects on the Policy Server.

Enable Shared Secret Rollover

Indicates whether the Policy Server generates a new shared secret when the agent is registered as a trusted host.

Trusted Host Name

Specifies a unique name for the host you are registering. After registration, this name appears in the list of Trusted Hosts in the Administrative UI. When configuring a SiteMinder Agent for IIS on an IIS web server farm, specify a *unique* name for *each* IIS server node on the farm. For example, if your farm uses six servers, specify six unique names.

Host Configuration Object

Indicates the name of the Host Configuration Object that exists on the Policy Server.

IP Address

Specifies the IP addresses of any Policy Servers to which the agent connects. Add a port number if you are *not* using the default port for the authentication server. Non-default ports are used for all three Policy Server connections (authentication, authorization, accounting).

Default: (authentication port) 44442

Example: (IPv4) 127.0.0.1,55555

Example: (IPv6) [2001:DB8::/32][:55555]

Note: If a hardware load balancer is configured to expose Policy Servers in your environment through a single Virtual IP Address (VIP), enter the VIP. For more information, see the *Policy Server Administration Guide*.

FIPS Mode Setting

Specifies *one* of the following algorithms:

FIPS Compatibility/AES Compatibility

Uses algorithms existing in previous versions of SiteMinder to encrypt sensitive data and is compatible with previous versions of SiteMinder. If your organization does *not* require the use of FIPS-compliant algorithms, use this option.

FIPS Migration/AES Migration

Allows a transition from FIPS-compatibility mode to FIPS-only mode. In FIPS-migration mode, SiteMinder environment continues to use existing SiteMinder encryption algorithms as you reencrypt existing sensitive data using FIPS-compliant algorithms.

FIPS Only/AES Only

Uses *only* FIPS-compliant algorithms to encrypt sensitive data in the SiteMinder environment. This setting does *not* interoperate with, *nor* is backwards-compatible with, previous versions of SiteMinder.

Default: FIPS Compatibility/AES Compatibility

Note: FIPS is a US government computer security standard that accredits cryptographic modules which meet the Advanced Encryption Standard (AES).

Important! Use a compatible FIPS/AES mode (or a combination of compatible modes) for both the SiteMinder agent and the SiteMinder Policy Server.

Name

Specifies the name of the SmHost.conf file which contains the settings the Web Agent uses to make initial connections to a SiteMinder Policy Server.

Default: SmHost.conf

Location

Specifies the directory where the SmHost.conf file is stored. On Windows 64-bit operating environments, the configuration program creates two separate files. One file supports 64-bit applications, and the other file supports 32-bit applications running on the same web server.

Default: (Windows IIS 7.x 32-bit) *web_agent_home*\win32\bin\IIS

Default: (Windows IIS 7.x 64-bit) *web_agent_home*\win64\bin\IIS

Virtual Sites

Lists the web sites on the IIS 7.x web server that you can protect with SiteMinder.

Overwrite, Preserve, Unconfigure

Appears when the SiteMinder Agent configuration wizard detects *one* of the following situations:

- IIS 7.x websites that SiteMinder r12.5 already protects on a stand-alone IIS web server.

- IIS 7.x websites that SiteMinder protects on an IIS server farm using shared configuration.

Select *one* of the following options:

Overwrite

Replaces the previous configuration of the SiteMinder Agent with the current configuration.

Preserve

Keeps the existing configuration of your SiteMinder Agent. No changes are made to this web server instance. Select this setting for *each* web server node if you are configuring the SiteMinder Agent for IIS 7.x on an IIS server farm.

Unconfigure

Removes the existing configuration of a SiteMinder Agent from the web server. Any resources are left unprotected by SiteMinder.

Default: Preserve

Important! Do not configure and unconfigure virtual sites at the same time. Run the wizard once to configure the sites you want, and then run the wizard again to unconfigure the sites you want.

Agent Configuration Object Name

Specifies the name of an Agent Configuration Object (ACO) already defined on the Policy Server. IIS web servers in a server farm using shared configuration support sharing a single ACO name with all IIS servers in the farm.

Default: AgentObj

Note: We recommend printing a copy of the SiteMinder Agent Configuration Worksheet to record this information for future reference.

More information:

Run the Web Agent Configuration Wizard

After gathering the information for your Agent Configuration worksheet, run the Agent Configuration wizard. The configuration wizard creates a runtime instance of the Agent for IIS on your IIS web server.

Running the configuration wizard once creates a properties file. Use the properties file to run unattended configurations on other computers with same operating environment and settings.

Note: The configuration wizard for this version of the Agent for IIS does *not* support console mode.

Follow these steps:

1. Click Start, All Programs, CA, SiteMinder.

   A shortcut to the Web Agent Configuration wizard appears.

2. Right-click the shortcut, and then select Run as administrator.

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

   The Web Agent Configuration wizard starts.

3. Complete the wizard.

Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode

Applications running in classic pipeline mode require that the ISAPI filter appears first in the list of ISAPI filters. Verify the position of the ISAPI filter in the list of ISAPI filters on your IIS web server before continuing.

Follow these steps:

1. Open IIS Manager using the following steps:

    a. Click Start, Control Panel.

    The control panel opens.

    b. Click Administrative Tools, Internet Information Services (IIS) Manager.

    IIS Manager opens.

2. Verify the ISAPI filter is first in the list using the following steps:

    a. From IIS Manager, expand the following items:

    - Your web server

    - Sites

    - Default Web Site

    b. Double-click the Handler Mappings icon.

    c. Click view ordered list.

    d. Verify that the following ISAPI filter appears in the top of the list:

    `handler-wa`

3. If the ISAPI filter from Step 2d does *not* appear first in the list, do the following steps:

    a. Click the handler-wa ISAPI filter.

    b. Click the Move up arrow until the ISAPI filter appears first in the list.

    The ISAPI filter appears first in the list.

Run the Unattended or Silent Installation and Configuration Programs for your Web Agent or Agent for IIS

The unattended or silent installation option can help you automate the installation and configuration process. This method saves time if you have a large SiteMinder environment that uses many agents with identical settings.

For example, suppose the Agents in your environment use the same web server version, installation directory, Agent Configuration Object and Policy Servers. Use the installation wizard or console-based installation program for your first installation. Afterwards, you could create your own script to run the installation program with the .properties file the wizard or console-based installation program created.

Follow these steps:

1. Run the following wizards on your first IIS web server (in the order shown):

   a. The SiteMinder Web Agent Installation wizard.

   b. The SiteMinder Web Agent Configuration wizard.

2. Locate the following file on your first IIS web server:

   web_agent_home\install_config_info\ca-wa-installer.properties

   Note: If the path contains spaces, surround it with quotes.

   > *web_agent_home*
   >
   > Indicates the directory where the SiteMinder Agent is installed on your web server.
   >
   > **Default** (Windows 32-bit installations of SiteMinder IIS Web Agents only): C:\Program Files\CA\webagent
   >
   > **Default** (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64
   >
   > **Default** (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

3. Perform each of the following steps on the other IIS web server nodes in your environment:

   Note: To automate this process, create your own customized script to execute these files on your systems. Use any scripting language that you want.

   a. Create a temporary directory on an IIS web server node.

   b. Copy the following files from your first IIS web server (from Steps 1 and 2) to the temporary directory on your other IIS web server:

      ■ The SiteMinder Web Agent Installation executable file.

      ■ The SiteMinder ca-wa-installer properties file.

      c.   Open a Command Prompt window with Administrative privileges in the temporary directory.

      d.   Run the following command:

          `agent_executable -f properties_file -i silent`

          The SiteMinder Web Agent for IIS is installed and configured on the node automatically.

      e.   (Optional) Delete the temporary directory from your web server node.

4.   Repeat Step 3 for each additional web server in your SiteMinder environment that uses the configuration that the settings in your ca-wa-installer.properties file specify.

Add SiteMinder Protection to Additional Virtual Sites on IIS Web Servers Silently

If your IIS web server already has a Web Agent for IIS installed, you can protect any additional virtual websites on the web server. For example, if you add two new virtual sites named Example2 and Example3 to your IIS server, you can protect them with SiteMinder.

If you do not want to run configuration wizard, or if you have many IIS web servers in a server farm, use the silent mode.

The SiteMinder Web Agent Configuration program supports a silent or unattended mode that requires no interaction from the end user.

To add SiteMinder protection to additional virtual sites on IIS web servers silently

1. Locate the following file on your first IIS web server.

    web_agent_home\install_config_info\ca-wa-installer.properties

    Note**: In this context, the first server refers to the IIS web server in a farm where the shared configuration information is stored. A node refers to any other IIS web servers in the farm which read the shared configuration from the first server.***web_agent_home*

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

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

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

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

2. Perform each of the following steps on the IIS web servers to which you want to protect the additional virtual sites:

    Note: To automate this process, create your own customized script to execute these files on your systems. Use any scripting language that you want.

    a. Create a temporary directory on an IIS web server node.

    b. Copy the following files from your first IIS web server (from Steps 1 and 2) to the temporary directory on your IIS web server node:

        ■ SiteMinder Web Agent Configuration executable file (ca-wa-config.exe).

        ■ SiteMinder ca-wa-installer properties file.

    c. Open the SiteMinder ca-wa-installer properties file with a text editor.

    d. Locate the following parameter:

        CONFIGURE_SITES=

Specifies the names of IIS 7.x web sites to protect on an IIS 7.x web server. Verify that these names match those names shown in under the Sites folder in the Internet Information Services (IIS) Manager of your web server. Separate multiple website names with commas.

For more information, see the comments in the ca-wa-installer.properties file.

Example: Default Web Site,Example1,Example2

e. Add the names of the web sites you want to configure to the previous parameter. Remove the names of any other sites on the web server that you want to leave unchanged.

f. Locate the following parameter:

HOST_REGISTRATION_YES=

Specifies if the agent configuration program registers the agent with a Policy Server. Each web server requires only one trusted host registration is required. Set the value of this parameter to 0 if you have previously registered a web server with the Policy Server as a trusted host.

Default: 1 (yes)

Limits: 0 (no registration), 1 (registration)

g. If the IIS web *server* is *already* registered as a trusted host with the SiteMinder Policy Server, change the value of the previous parameter to 0. Otherwise, the configuration program registers the web server as a trusted host.

h. Open a Command Prompt window with Administrative privileges in the temporary directory.

i. **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.

j. Run the following command:

```
agent_configuration_executable -f properties_file -i silent
```

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

The SiteMinder Web Agent for IIS is installed and configured on the node automatically.

k. (Optional) Delete the temporary directory from your web server node.

3. Repeat Step 2 for each additional IIS web server node in your environment that uses the configuration specified by the settings in your <flilename>-wa-installer.properties file.

Remove a SiteMinder Web Agent Configuration from an IIS Web Server Silently

To remove the SiteMinder protection from all the websites on an IIS web server without the Web Agent Configuration wizard, use silent or unattended mode. This mode requires no interaction from the end user.

To remove a SiteMinder Web Agent configurations from an IIS web server silently

1. Locate the following file on your first IIS web server.

   web_agent_home\install_config_info\ca-wa-installer.properties

   Note: In this context, the first server refers to the IIS web server in a farm where the shared configuration information is stored. A node refers to any other IIS web servers in the farm which read the shared configuration from the first server.

   ### *web_agent_home*

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

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

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

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

2. Perform each of the following steps on the IIS web servers to which you want to remove protection from virtual sites:

   Note: To automate this process, create your own customized script to execute these files on your systems. Use any scripting language that you want.

   a. Open the following directory on an IIS web server node.

      web_agent_home\install_config_info

   b. Copy the SiteMinder ca-wa-installer properties file from your first IIS web server (from Step 1) to the install_config_info directory on your IIS web server node.

   c. Open the SiteMinder ca-wa-installer properties file with a text editor.

   d. Locate the following parameter:

      UNCONFIGURE_SITES=

      Specifies the names of IIS 7.x web sites from which to remove SiteMinder protection on an IIS 7.x web server. Verify that these names match those names shown in under the Sites folder in the Internet Information Services (IIS) Manager of your web server. Separate multiple website names with commas.

Removing the SiteMinder Web Agent configuration from a website leaves its resources *unprotected*.

For more information, see the comments in the ca-wa-installer.properties file.

Example: Default Web Site,Example4,Example5

e. Enter the names of the websites you want to unconfigure in the previous parameter.

f. Locate the following parameter:

CONFIGURE_SITES=

Specifies the names of IIS 7.x web sites to protect on an IIS 7.x web server. Verify that these names match those names shown in under the Sites folder in the Internet Information Services (IIS) Manager of your web server. Separate multiple website names with commas.

For more information, see the comments in the ca-wa-installer.properties file.

Example: Default Web Site,Example1,Example2

g. Verify that the previous parameter contains no website names.

h. Open a command prompt window with Administrative privileges.

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.

i. Run the following command:

`agent_configuration_executable -f properties_file -i silent`

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

The websites are unconfigured on the node automatically.

3. Repeat Step 2 for each additional IIS web server node in your environment that uses the configuration specified by the settings in your <flilename>-wa-installer.properties file.

Remove SiteMinder Protection From Some Virtual Sites on IIS Web Servers Silently

If your IIS web server already has a Web Agent for IIS installed, you can remove protection from some virtual websites on the web server. For example, suppose you want to remove protection from only two of the virtual sites named Example4 and Example5 from to your IIS server. Modify the ca-wa-installer.properties file to remove the configuration from those two virtual websites while leaving the protection for the other websites unchanged.

If you do not want to run the configuration wizard, or if you have many IIS web servers in a server farm, use the silent mode.

The SiteMinder Web Agent Configuration program supports a silent or unattended mode that requires no interaction from the end user.

To remove SiteMinder protection from additional virtual sites on IIS web servers silently

1. Locate the following file on your first IIS web server.

    web_agent_home\install_config_info\ca-wa-installer.properties

    Note**: In this context, the first server refers to the IIS web server in a farm where the shared configuration information is stored. A node refers to any other IIS web servers in the farm which read the shared configuration from the first server.***web_agent_home*

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

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

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

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

2. Perform each of the following steps on the IIS web servers from which you want to remove the protection of the additional virtual sites:

    Note: To automate this process, create your own customized script to execute these files on your systems. Use any scripting language that you want.

    a. Copy the SiteMinder ca-wa-installer properties file from your first IIS web server (from Step 1) to the install_config_info directory on your IIS web server node:

    b. Open the SiteMinder ca-wa-installer properties file with a text editor.

    c. Locate the following parameter:

        UNCONFIGURE_SITES=

Specifies the names of IIS 7.x web sites from which to remove SiteMinder protection on an IIS 7.x web server. Verify that these names match those names shown in under the Sites folder in the Internet Information Services (IIS) Manager of your web server. Separate multiple website names with commas.

Removing the SiteMinder Web Agent configuration from a website leaves its resources *unprotected*.

For more information, see the comments in the ca-wa-installer.properties file.

Example: Default Web Site,Example4,Example5

d. Add the names of the web sites from which you want to remove the configuration to the previous parameter. Remove the names of any other sites on the web server that you want to leave unchanged.

e. Locate the following parameter:

HOST_REGISTRATION_YES=

Specifies if the agent configuration program registers the agent with a Policy Server. Each web server requires only one trusted host registration is required. Set the value of this parameter to 0 if you have previously registered a web server with the Policy Server as a trusted host.

Default: 1 (yes)

Limits: 0 (no registration), 1 (registration)

f. If the IIS web *server* is *already* registered as a trusted host with the SiteMinder Policy Server, set the previous parameter to 0. Otherwise, the configuration program registers the web server as a trusted host.

g. Open a Command Prompt window with Administrative privileges in the temporary directory.

h. **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.

i. Run the following command:

`agent_configuration_executable` -f `properties_file` -i silent

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

The SiteMinder configuration is removed from the selected virtual sites on the node automatically.

3. Repeat Step 2 for each additional IIS web server node in your environment that uses the configuration specified by the settings in your <flilename>-wa-installer.properties file.

How to Configure Certain Settings for the SiteMinder Agent for IIS Manually

In some situations, the SiteMinder Agent configuration programs *cannot* add the proper settings to all the IIS web server directories which need them.

Configure the SiteMinder Agent for IIS settings manually in *any* of the following situations:

- Your SiteMinder Agent for IIS log files are *not* stored in the following default directory (see page 39):

  web_agent_home\log

  > **web_agent_home**
  >
  > Indicates the directory where the SiteMinder Agent is installed on your web server.
  >
  > **Default** (Windows 32-bit installations of SiteMinder IIS Web Agents only): C:\Program Files\CA\webagent
  >
  > **Default** (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64
  >
  > **Default** (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32

  For example, suppose that you store your log files in the C:\My Logs\SiteMinder directory. Grant this directory permissions.

- You use a SiteMinder authentication scheme which requests or requires client certificates (see page 40).

Set Permissions Manually for Non-Default Log Locations

If you decide to store your agent log files in a non default directory, grant your application pools permissions to the directory. For example, if you want to store your log files in a directory named C:\MyLogFiles, grant permissions for all your application pool identities to C:\MyLogFiles.

Microsoft provides a command line utility, icacls.exe you can use to set the appropriate permissions. This procedure provides one possible example of a way to set permissions using tools or utilities provided by third-party vendors.

Important! CA provides this information only as an example of one possible method of configuring SiteMinder without using the programs and utilities tested and approved by CA. Microsoft provides the icacls.exe command as part of the Windows operating environment. You may choose to use the following examples as a guide to grant file permissions for the agent for IIS. This command and the syntax shown are subject to change by Microsoft at any time and without notice. For more information, go to the Microsoft Support website, and search for "icacls".

To set permissions manually for non default log locations

1. Open a Command Prompt Window on your IIS web server.

   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.

2. Run the icacls command. Use the following example as a guide:

   `icacls log_directory /grant IIS AppPool\application_pool_identity`

   log_directory

   Specifies the non default log directory to which you must grant permissions.

   application_pool_identity

   Specifies the identity of the application pool associated with the application protected by SiteMinder on your IIS web server.

   Note: For more information about Application Pool Identities, see the IIS website.

3. Repeat Step 2 for each application pool identity on your IIS web server. For example, if you have two application pools, grant permissions to both.

4. If you have an IIS server farm using Shared Configuration, repeat Steps 1 through 3 for each IIS web server in the farm.

   The permissions are set.

Change IIS Settings Manually for SiteMinder Authentication Schemes Requiring Certificates

If you use SiteMinder authentication schemes that request or require certificates, change the settings manually on your IIS web server for the following virtual directories:

- cert

- certoptional

To change IIS settings manually for SiteMinder authentication schemes requiring certificates

1. Open IIS manager.

2. Expand your web server.

3. The Application pools icon and Sites folder appear.

4. Expand Sites.

   A list of web sites appears.

5. Expand the website associated with your authentication scheme that requires certificates.

   The siteminderagent virtual folder appears.

6. Expand the siteminderagent virtual folder.

   A list of subfolders appears.

7. Click the cert folder.

   The settings icons appear.

8. Double-click SSL Settings.

   The SSL Settings page appears.

9. Select the Require SSL check box, and then click the Require option button.

10. Under Actions, click Apply.

    The changes are applied.

11. Click the certoptional folder.

    The settings icons appear.

12. Double-click SSL Settings.

    The SSL Settings page appears.

13. Click the Accept option button.

14. Under Actions, click Apply.

    The changes are applied.

15. Repeat Steps 3 through 14 for other websites on your IIS web server that require certificates.

16. For IIS server farms using Shared Configuration, repeat Steps 1 through 15 on each IIS web server in your farm.

    The settings are changed.

Chapter 3: Upgrade a Web Agent to r12.5

This section contains the following topics:

How to Prepare for a SiteMinder Agent Upgrade

Upgrading a SiteMinder agent involves several separate procedures. To prepare for an upgrade of your agent, follow these steps:

1. Create backup copies of any customized SiteMinder files on your web server. Examples of files you could have customized after installing or configuring your agent include the following files:

    ■ LocalConfig.conf

    ■ WebAgent.conf

2. Gather information for the following SiteMinder programs.

    ■ Agent installation wizard (see page 23).

    ■ Agent configuration wizard (see page 24).

3. Do *one* of the following tasks:

    ■ If you are upgrading from version 12.0.3 or higher to r12.5, go to Step 4.

    ■ If you are upgrading from version 12.0.2 or older, continue with this procedure instead (see page 46).

4. Run the installation wizard to upgrade your Agent for IIS (see page 44).

5. Run the configuration wizard to configure the upgraded Agent for IIS (see page 45).

Run the Installation Wizard to Upgrade your Agent for IIS

The installation program for the SiteMinder agent installs the agent on one computer at a time using the Windows operating environment. This installation program can be run in wizard or console modes. The wizard and console-based installation programs also create a .properties file for subsequent installations and configurations using the unattended or silent method with the same settings.

For example, suppose the Agents in your environment use the same web server version, installation directory, Agent Configuration Object and Policy Servers. Use the installation wizard or console-based installation program for your first installation. Afterwards, you could create your own script to run the installation program with the .properties file the wizard or console-based installation program created.

Follow these steps:

1. Copy the SiteMinder Web Agent installation executable file to a temporary directory on your web server.

2. Do *one* of the following steps:

   ■ For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.

   ■ For console-based installations, open a command line window and run the executable as shown in the following example:

   executable_file_name.exe -i console

3. Use the information that you gathered previously to complete the installation.

More information:

Multiple Agent for IIS Directory Structures According to Operating Environment (see page 9)

Run the Configuration Wizard on your Upgraded Agent for IIS

After gathering the information for your Agent Configuration worksheet, run the Agent Configuration wizard. The configuration wizard creates a runtime instance of the Agent for IIS on your IIS web server.

Running the configuration wizard once creates a properties file. Use the properties file to run unattended configurations on other computers with same operating environment and settings.

Note: The configuration wizard for this version of the Agent for IIS does *not* support console mode.

Follow these steps:

1. Click Start, All Programs, CA, SiteMinder.

    A shortcut to the Web Agent Configuration wizard appears.

2. Right-click the shortcut, and then select Run as administrator.

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

    The Web Agent Configuration wizard starts.

3. Complete the wizard.

How to Upgrade an Agent for IIS from Version 12.0.2 or Lower

Upgrading an agent for IIS to version 12.0.3 or higher requires removing the older version of the agent before installing the newer version. Some directory changes were introduced in 12.0.3 which also apply to the subsequent versions of the product. Running the new installation program without removing the previous version sometimes causes problems.

How to Upgrade Your Agent for IIS
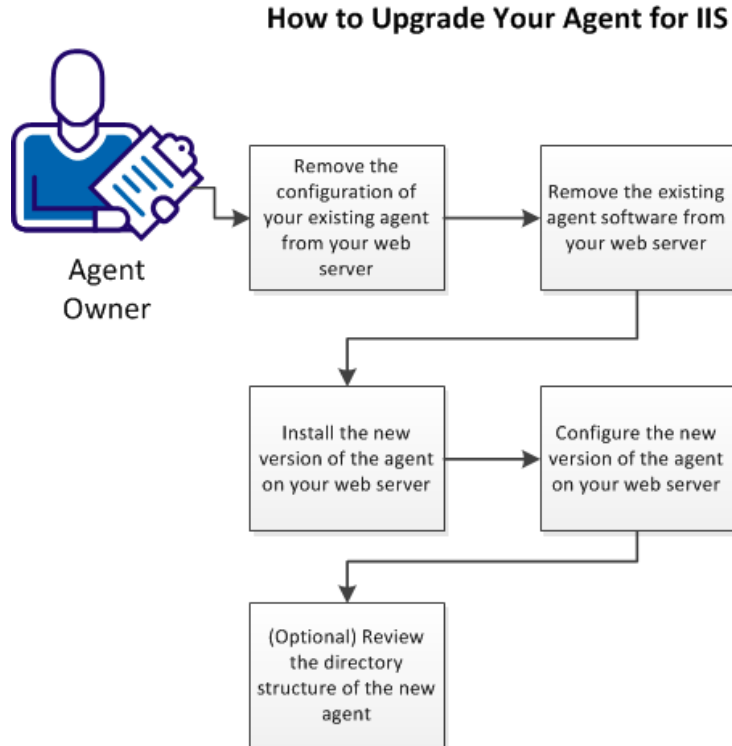
Follow these steps:

1. Remove the configuration of your existing agent from your web server (see page 47).

2. Remove the existing agent software from your web server (see page 48).

3. Install the new version of the agent on your web server (see page 49).

4. .Configure the new version of the agent on your web server (see page 50).

5. (Optional) Review the directory structure of the new agent (see page 51).

Remove the configuration of your existing agent from your web server

Before upgrading your agent to 12.0.3 or higher, remove the server configuration from the previous version of your agent using the configuration wizard. For example, if you are upgrading from 6.x to r12.5, remove the server configuration for the 6.x version of your agent using the configuration wizard.

Follow these steps:

1. 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 differs slightly.

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

2. Skip to the next step. You do *not* need to register a trusted host.

3. Clear the check boxes of the web server instances from which you want to remove the configuration.

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 that already defined at the Policy Server.

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

    The Web Agent files are installed.

6. Click Done when the installation is complete.

7. Reboot the computer.

Remove the existing agent software from your web server

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

Follow these steps:

1. Stop the web server.

2. Choose *one* of the following procedures:

   - To remove the Web Agent using the wizard, go to Step 3.

   - To remove the Web Agent using the console-based program, go to Step 8.

3. Click Start, Control Panel, Programs and Features.

   A list of installed programs appears.

4. Click CA SiteMinder Web Agent *version_number*.

5. Click Uninstall/Change.

   The uninstallation wizard appears.

6. Review the information in the Uninstall SiteMinder Web Agent dialog, then click Uninstall.

   The wizard removes the web agent.

7. Wait for the wizard to finish, then go to Step 12.

8. Open a command-line window.

9. Navigate to the following directory.

   web_agent_home

   web_agent_home

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

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

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

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

10. Run the following command:

    `ca-wa-uninstall.cmd -i console`

11. Wait for the un–installation program to finish, then go to Step 12.

12. Start the web server.

Important! Delete the ZeroG registry file from the following location after uninstalling the Web Agent: C:\Program Files\ZeroG Registry\com.zerog.registry.xml

Install the new version of the agent on your web server

After unconfiguring and removing the older version of your agent, install version r12.5 on your web server.

The installation program for the SiteMinder agent installs the agent on one computer at a time using the Windows operating environment. This installation program can be run in wizard or console modes. The wizard and console-based installation programs also create a .properties file for subsequent installations and configurations using the unattended or silent method with the same settings.

For example, suppose the Agents in your environment use the same web server version, installation directory, Agent Configuration Object and Policy Servers. Use the installation wizard or console-based installation program for your first installation. Afterwards, you could create your own script to run the installation program with the .properties file the wizard or console-based installation program created.

Follow these steps:

1. Copy the SiteMinder Web Agent installation executable file to a temporary directory on your web server.

2. Do *one* of the following steps:

    ■   For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.

    ■   For console-based installations, open a command line window and run the executable as shown in the following example:

    executable_file_name.exe -i console

    Use the information that you gathered previously to complete the installation.

Configure the new version of the agent on your web server

After gathering the information for your Agent Configuration worksheet, run the Agent Configuration wizard. The configuration wizard creates a runtime instance of the Agent for IIS on your IIS web server.

Running the configuration wizard once creates a properties file. Use the properties file to run unattended configurations on other computers with same operating environment and settings.

Note: The configuration wizard for this version of the Agent for IIS does *not* support console mode.

Follow these steps:

1. Click Start, All Programs, CA, SiteMinder.

    A shortcut to the Web Agent Configuration wizard appears.

2. Right-click the shortcut, and then select Run as administrator.

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

    The Web Agent Configuration wizard starts.

    Complete the wizard.

(Optional) Review the directory structure of the new agent

The directory structure added to your IIS web server for your Agent files varies according to the operating environment of your IIS web server. The following directory structures exist:

- SiteMinder Web Agents and [set AGENT value for your book]s for IIS use the directory structure shown in the following illustration:

```
\webagent                    32-bit Operating Environments
   ├── \affwebservices
   ├── \bin
   ├── \config
   ├── \affwebservices
   ├── \etpki-install
   ├── \install_config_info
   ├── \java
   ├── \jpw
   ├── \jpw_default
   ├── \log
   ├── \pw
   ├── \pw_default
   ├── \samples
   ├── \samples_default
   ├── \secureforms
   ├── \sharepoint
   └── \tools
```
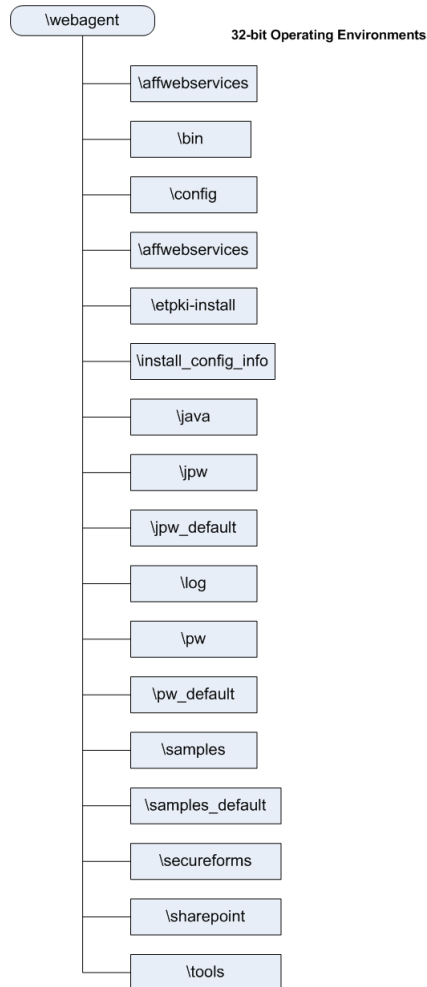
■ SiteMinder Agents for IIS installed on 64-bit operating environments use the directory structure shown in the following illustration:
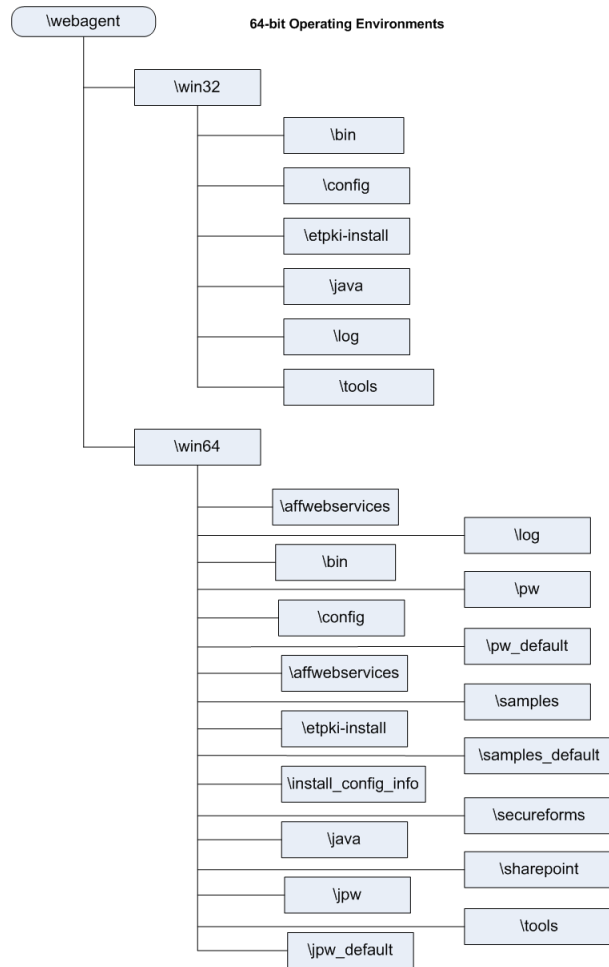
Chapter 4: Dynamic Policy Server Clusters

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

SiteMinder r12.5 supports dynamic Policy Server clusters. Agents automatically discover Policy Servers that are added or removed from an existing cluster when dynamic Policy Server Clusters are enabled.

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

- 192.168.2.100
- 192.168.2.101
- 192.168.2.103
- 192.168.2.104

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

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

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

Connect a Web Agent to a Dynamic Policy Server Cluster

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

Follow these steps:

1. Open the following file with a text editor:

   web_agent_home\config\SmHost.conf

   > **web_agent_home**
   >
   >> Indicates the directory where the SiteMinder Agent is installed.
   >>
   >> **Default** (Windows 32-bit installations of SiteMinder Web Agents only): C:\Program Files\CA\webagent
   >>
   >> **Default** (Windows 64-bit installations [SiteMinder Web Agents for IIS only]): C:\Program Files\CA\webagent\win64
   >>
   >> **Default** (Windows 32-bit applications operating on 64-bit systems [Wow64 with SiteMinder Web Agents for IIS only]): C:\Program Files (x86)\webagent\win32
   >>
   >> **Default** (UNIX/Linux installations): /opt/ca/webagent

2. Do *one* of the following tasks:

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

     enableDynamicHCO="YES"

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

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

4. Restart your web server.

   The Web Agent is connected to dynamic Policy Server clusters.

Chapter 5: Starting and Stopping Web Agents

This section contains the following topics:

Enable a Web Agent

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

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

Follow these steps:

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

    Note: SiteMinder r12.5 Agents for IIS installed on 64-bit Windows operating environments have *two* WebAgent.conf files. One file is associated with 32-bit Windows applications. The other file is associated with 64-bit Windows applications. Modify *both* WebAgent.conf files to start or stop the SiteMinder Agent for IIS on all 32-bit *and* 64-bit applications on a particular IIS web server.

2. Change the value of the EnableWebAgent parameter to yes.

3. Save and close the WebAgent.conf file.

4. Restart the web server (the web server itself, not the computer on which it runs).

    The Web Agent is enabled.

Disable a Web Agent

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

Follow these steps:

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

   Note: SiteMinder r12.5 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.

Chapter 6: Uninstall a Web Agent

This section contains the following topics:

Notes About Uninstalling Web Agents

Be aware of the following:

- All Web Agents for all installed web servers will be uninstalled.

- The Password Services and Forms directories, (pw_default, jpw_default, samples_default) will be removed. However, the non-default copies of these directories (pw, jpw, samples) are not removed because these directories may contain customized files.

- Make sure that the JRE is installed on the Web Agent system, as it is needed for uninstallation. For a supported version, see the SiteMinder r12.5 Platform Matrix at Technical Support.

Set JRE in PATH Variable Before Uninstalling the SiteMinder Agent

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

- "Could not find a valid Java virtual machine to load. You need to reinstall a supported Java virtual machine."

- "No Java virtual machine could be found from your PATH environment variable. You must install a VM prior to running this program."

Follow these steps:

On Windows

1. Go to the Control Panel.

2. Double-click System.

3. In the Environment Variables dialog, add the location of the JRE to the PATH system variable.

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

On UNIX

Run the following commands:

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

    JRE

    Specifies the location of your JRE.

    For example, /usr/bin/j2sdk*version_number*/jre

2. export PATH

Uninstall a Web Agent from a Windows Operating Environment

Before you unˉinstall 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 the 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.

Follow these steps:

1. Stop the web server.

2. Choose *one* of the following procedures:

   ■   To remove the Web Agent using the wizard, go to Step 3.

   ■   To remove the Web Agent using the console-based program, go to Step 8.

3. Click Start, Control Panel, Programs and Features.

   A list of installed programs appears.

4. Click CA SiteMinder Web Agent *version*.

5. Click Uninstall/Change.

   The uninstallation wizard appears.

6. Review the information in the Uninstall SiteMinder Web Agent dialog, then click Uninstall.

   The wizard removes the web agent.

7. Wait for the wizard to finish, then go to Step 12.

8. Open a command-line window.

9. Navigate to the following directory.

   web_agent_home

   web_agent_home

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

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

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

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

10. Run the following command:

```
ca-wa-uninstall.cmd -i console
```

11. Wait for the un–installation program to finish, then go to Step 12.

12. Start the web server.

Important! Delete the ZeroG registry file from the following location after uninstalling the Web Agent: C:\Program Files\ZeroG Registry\com.zerog.registry.xml

Silently Remove a SiteMinder Web Agent from a Windows Operating Environment

The SiteMinder Web Agent supports an unattended or silent removal mode which uninstalls a SiteMinder Web Agent from a web server. This option does not require any interaction from the end user.

1. Log in to your web server.

2. Open a Command Prompt window with Administrative privileges.

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

3. Run the following command:

    web_agent_home\install_config_info\ca-wa-uninstall\uninstall.exe -f
    installvariables.properties -i silent

    Note: If the path contains spaces, surround it with quotes.

    web_agent_home

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

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

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

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

    The SiteMinder Web Agent is removed from the web server.

4. For IIS server farms, repeat Steps 1 though 3 for each web server in your farm.

Chapter 7: Troubleshooting

This section contains the following topics:

I need to execute another IIS 7.x Module Before the SiteMinder Web Agent for IIS

When you install and configure the SiteMinder Agent for IIS on an IIS web server, the Agent for IIS executes before any other modules. If your IIS environment requires another module to execute first, you can change the number set the following location in the Windows Registry:

HKLM\Software\Netegrity\SiteMinder Web Agent\Microsoft IIS\RequestPriority

For example, suppose another module in your IIS 7.x web server (like UrlScan) is assigned the same execution priority as the SiteMinder Agent for IIS. Use this setting to control when the SiteMinder module executes.

Follow these steps:

1. Open the Windows Registry Editor on your IIS web server.

2. Expand the following keys:

   HKLM\Software\Netegrity\SiteMinder Web Agent\Microsoft IIS

3. Locate the following value:

   RequestPriority

4. Change the value of RequestPriority to the number which corresponds to the following value you want:

   PRIORITY_ALIAS_FIRST

   Executes the SiteMinder Agent for IIS before any other modules on your IIS web server. This setting is the default.

   Example: 0 (First)

   Default: 0

   PRIORITY_ALIAS_HIGH

   Executes the SiteMinder Agent for IIS module after any modules set to execute first, but before any modules set to execute with medium, low or last priority.

   Example: 1 (High)

   PRIORITY_ALIAS_MEDIUM

   Executes the SiteMinder Agent for IIS module after modules set to execute first and high, but before modules set to execute with low or last priority.

   Example: 2 (Medium)

   PRIORITY_ALIAS_LOW

   Executes the SiteMinder Agent for IIS module after modules set to execute first, high, and medium, but before modules set to execute with last priority.

Example: 3 (Low)

PRIORITY_ALIAS_LAST

Executes the module for the SiteMinder Agent for IIS *after* all other modules.

Example: 4 (Last)

5. Save your changes and close the registry editor.

6. Test your settings and verify that the module you want executes before the Agent for IIS module executes.

Changing Document Root Folder after Agent Configuration Leaves Resources Unprotected

Symptom:

I changed the location of the document root folder on my web server after I configured my SiteMinder agent. Now the resources in the new document root folder are unprotected.

Solution:

If you change the location of the document root folder on your web server, run the agent configuration program again.

Diagnose Agent Start-Up/Shutdown Issues (Framework Agents Only)

Symptom:

The SiteMinder Agent does not start or shut down.

Solution:

Do the following tasks:

■ Run the Low Level Agent Worker Process (LLAWP) separately to isolate the problem.

■ For the Windows operating environment Windows, see the Application Log in the Event Viewer.

Event Viewer Message Describes lack of Permissions on Host Configuration File

Valid on IIS

Symptom:

I see the following messages in my event viewer:

- Siteminder Web Agent not having read permissions on host configuration file. Permission denied. Please assign read privileges to the user DefaultAppPool for the file C:\Program Files\CA\webagent\config\SmHost.conf.

- Siteminder Web Agent not having read permissions on host configuration file. Permission denied. Please assign read privileges to the user DefaultAppPool for the file C:\Program Files\CA\webagent\config\SmHost.conf.

Solution:

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

- The SmHost.conf file

Follow these steps:

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 text:

    `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. The application pool identities are granted permission for the SiteMinder SmHost.conf file.

Appendix A: Worksheets

This section contains the following topics:

Web Agent Install Worksheet for the Windows Operating Environment

Use the following table to record the information that the Agent for IIS Installation program requires for the Windows operating environment:

Information Needed	Your Value
Installation Directory	
Shortcut Location	

SiteMinder Agent Configuration Worksheet for IIS Web Servers

Use the following table to record the information that the SiteMinder Agent Configuration program requires for IIS web servers:

Information Needed	Your Value
Host Registration (Yes/No)	
Admin User Name	
Admin Password	
Enable Shared Secret Rollover	
Trusted Host Name (unique for each server)	
Host Configuration Object	
IP Address	
FIPS Mode Setting	
SmHost.conf file Name	
SmHost.conf file Locations	

Information Needed	Your Value
Select Servers	
Overwrite, Preserve, Unconfigure	
Agent Configuration Object Name	
Webagent Enable Option	

More information:

Gather the Information for the Agent Installation Program for the Windows Operating Environment (see page 23)

Index

R

S

T

U

V

W