CA SiteMinder®

Web Agent Installation Guide for IIS

r12.0 SP3

Fourth Edition

CA Technologies Product References

This document references the following CA Technologies products:

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

Contact CA Technologies

Contact CA Support

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

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

Providing Feedback About Product Documentation

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

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

Documentation Changes

The following documentation update have been made since the third edition of this documentation:

- Gather the Information for the Agent Configuration Program for IIS Web Servers (see page 34)—Updated with the newly added Enable Web Agent option (140141, 147841).
- Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode (see page 39)—Added new instructions for verifying the ISAPI filter placement. Resolves CQ 170574 and STAR Issue 21403389:01
- How to Prepare for a SiteMinder Web Agent or SiteMinder Agent for IIS Installation on an IIS Web Server (see page 14)—Removed reference to Visual C++ 2005 Redistributable Package (x64) prerequisite. The installer now adds this package if it does not exist. Resolves CQ171381.

Contents

Chapter 1: Preparation

This section contains the following topics:

Two Types of Agents for Internet Information Services (IIS) Web Servers

SiteMinder r12.0 SP3 now offers the following types of Agents for Internet Information Services (IIS) web servers:

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.

SiteMinder Web Agent

A SiteMinder Web Agent implemented as an ISAPI plug-in that supports the following functions:

- Application pools in Classic pipeline mode only.
- Supported with IIS 6.0, 7.0 and 7.5 standalone deployments only.

Wizard-based IIS 7 Agent Configuration Available

SiteMinder Agents for IIS can now be configured on IIS 7.0 and IIS 7.5 web servers using a wizard-based configuration program. In most situations, manual configuration steps are not necessary.

IIS 6.0 servers still require manual configuration steps.

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.

Only IIS Web Server Procedures in this Guide

This guide only contains procedures for installing or configuring one of the following Agents on IIS web servers:

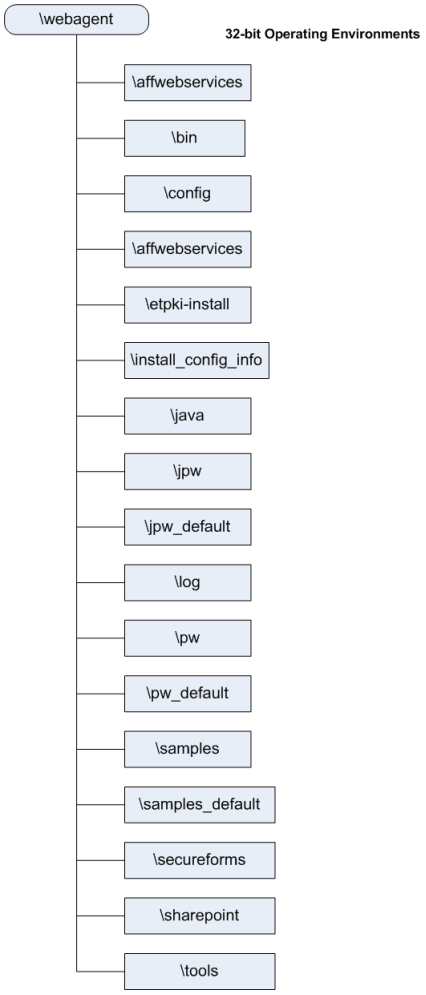
- SiteMinder Web Agent.
- SiteMinder Agent for IIS.

To install or configure a SiteMinder Web Agent on any other type of web server or operating environment (such as Apache web servers on Windows or UNIX), see the SiteMinder *Web Agent Installation Guide*.

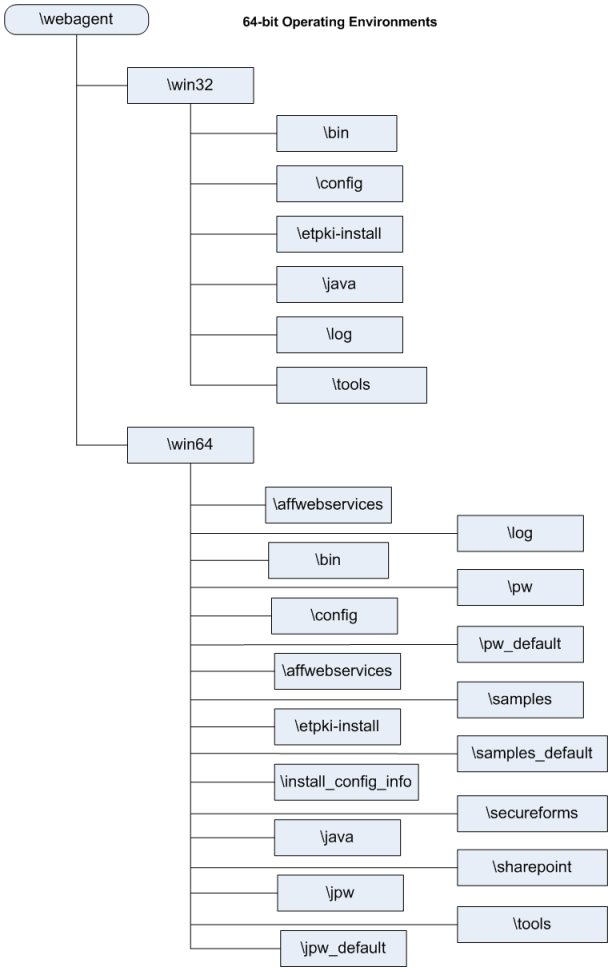
Multiple Agent for IIS Directory Structures According to Operating Environment

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:

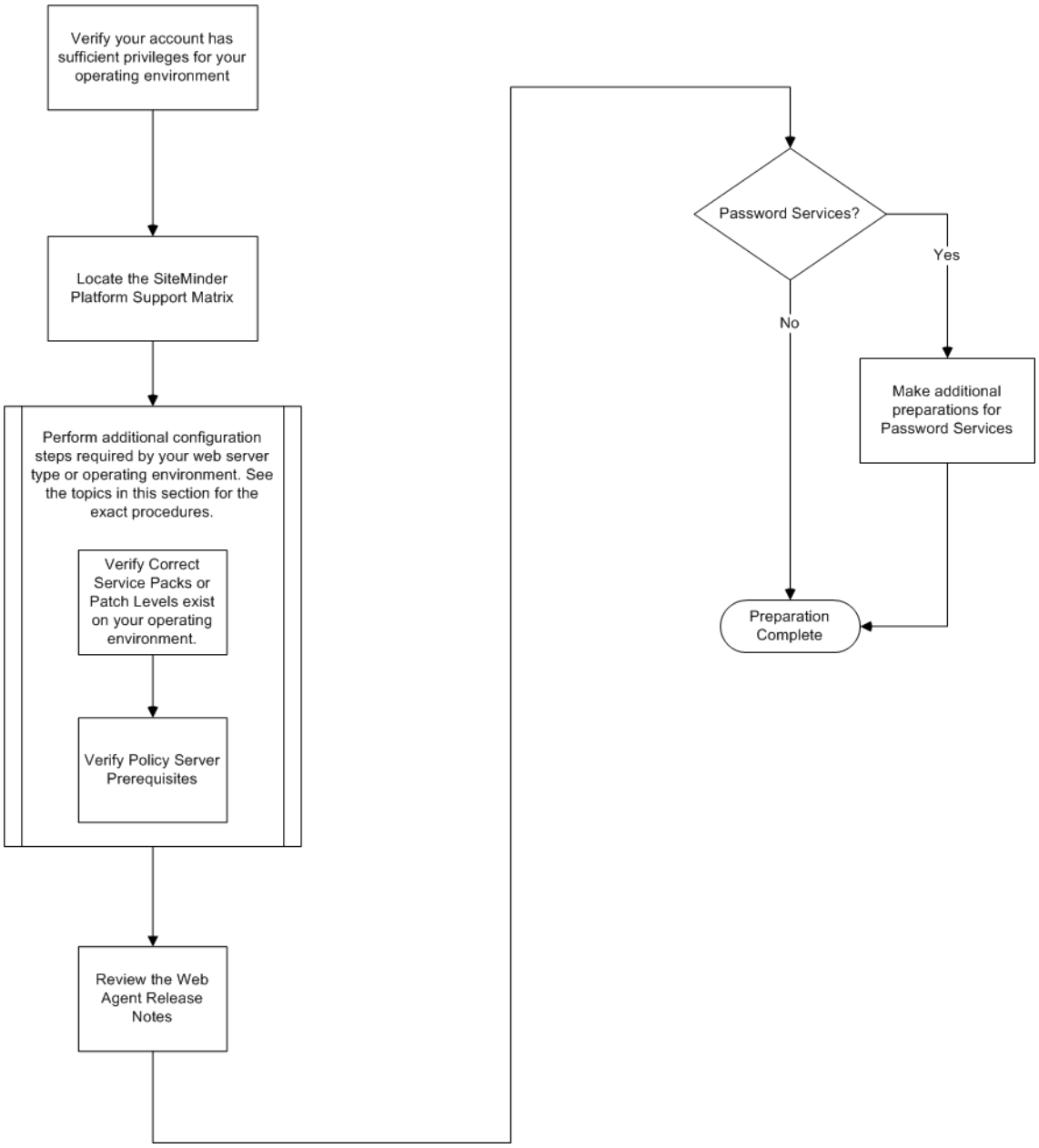


- SiteMinder Agents for IIS installed on 64-bit operating environments use the directory structure shown in the following illustration:



Web Agent Preparation Roadmap

Preparing your web server for a SiteMinder Web Agent or SiteMinder Agent for IIS installation involves several separate procedures in this section. The following diagram provides an overview of the preparation process:



How to Prepare for a SiteMinder Web Agent or SiteMinder Agent for IIS Installation on an IIS Web Server

To prepare for a Web Agent installation on an IIS web server, use the following process:

1. Verify that you have an account with Administrative privileges on the computer hosting your IIS web server (see page 14).
2. Locate the SiteMinder Platform Support Matrix (see page 15). Confirm that your IIS web server meets the requirements for the Web Agent version you want to install.
3. Verify that the Windows operating environment for your IIS web server has the proper service packs and updates installed (see page 15).
4. Confirm that your Policy Server has the prerequisites for a Web Agent Installation (see page 16).
5. Review the Web Agent Release Notes for installation considerations or known issues (see page 18).
6. (Optional) Verify that your Windows operating environment meets the prerequisites for password services (see page 18).

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.

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.

Agent Configuration Object

Specifies the name of an Agent Configuration object containing the parameter settings that your Web Agent uses. Agent configuration objects need values in at least one of the following parameters operate:

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

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

DefaultAgentName

Defines a name that the agent uses when no agent name exists in the value of the AgentName parameter.

Using a DefaultAgentName instead of defining a separate Web Agent for each web server helps you set up your SiteMinder environment quickly.

Note: If you do not specify a value for the DefaultAgentName parameter, specify every agent identity in the AgentName parameter. Otherwise, the Policy Server cannot associate policies with the Web Agent.

Default: No default

Limits: Single-value only. 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.

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.

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 19).
2. Repair the CLASSPATH used by the ServletExec application for JSP password services (see page 19).

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.

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

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

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

To repair the ServletExec classpath

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

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

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

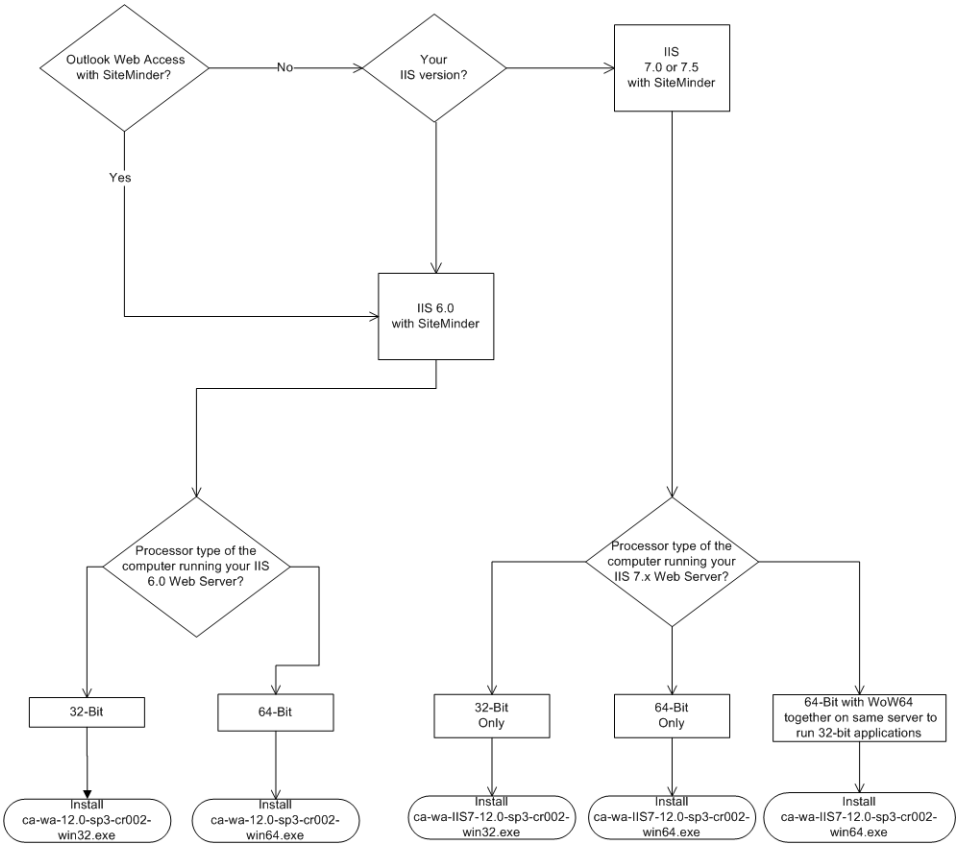
Chapter 2: Install a Web Agent on a Windows System

This section contains the following topics:

Web Agent for IIS Installation Roadmap

For SiteMinder r12.0 SP3, the Web Agent for IIS offers several installation options. These options depend on the version of IIS that you use, and the Integrated Pipeline mode of your web applications.

Use the following illustration to select the proper Web Agent for IIS installer for your situation:



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.

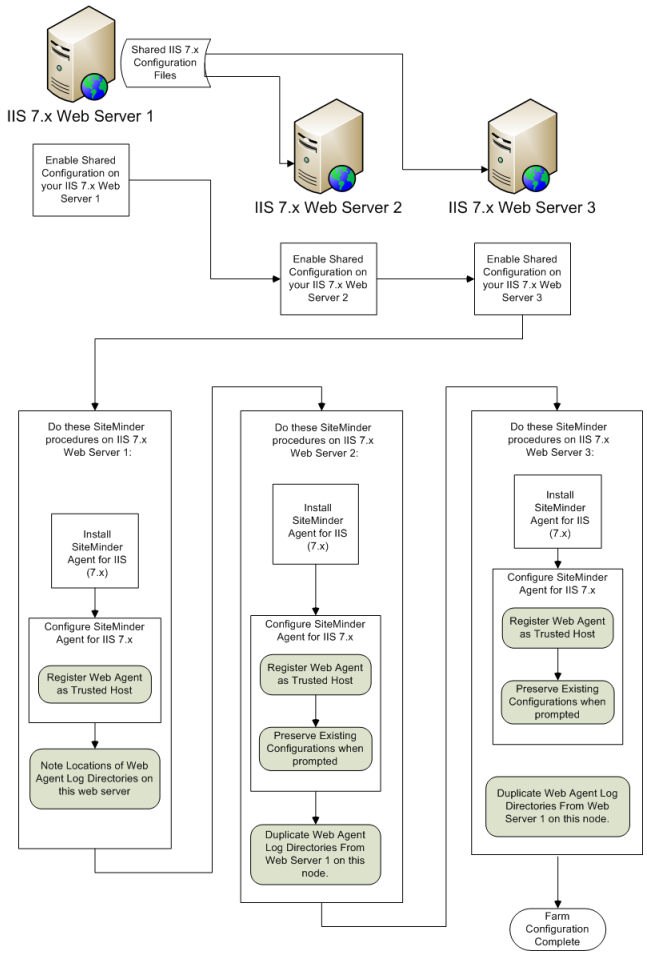
Starting with SiteMinder r12.0 SP3, the Agent for IIS can protect resources on IIS server farms that use the shared configuration feature of IIS 7.x.

Note: This feature works *only* with the SiteMinder r12.0 SP3 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 r12.0 SP3 Agent for IIS, however, *cannot* operate on network shares. Using a SiteMinder r12.0 SP3 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:

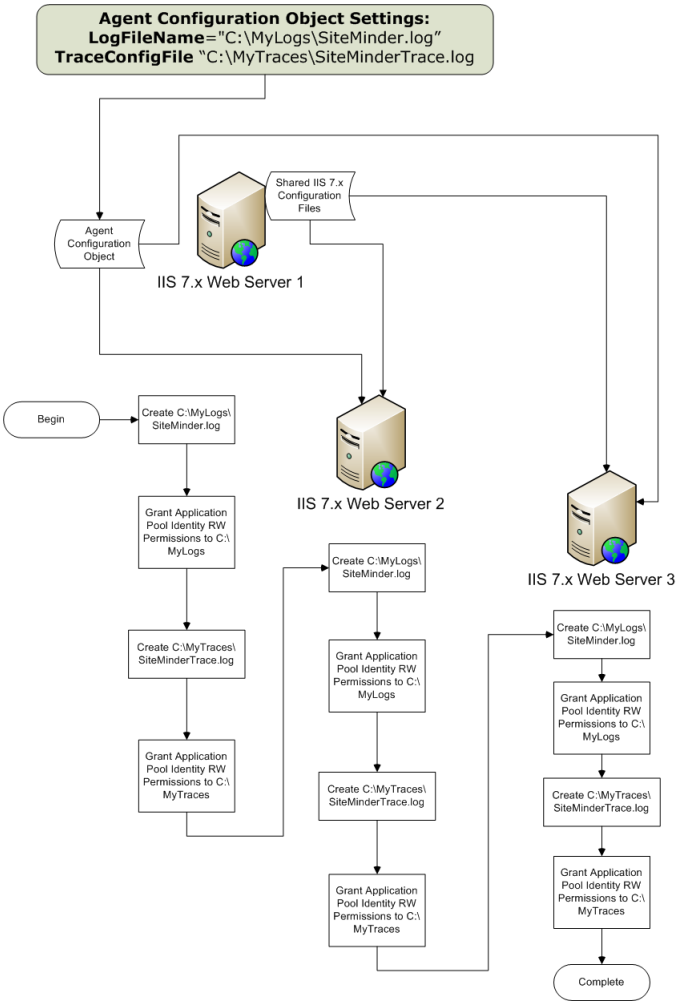
- Your Agent for IIS log and trace log directories are specified in an Agent Configuration Object on the Policy Server (*not* in a local configuration file).
- Any of the SiteMinder Agents for IIS in your IIS 7.x web servers in the server farm share the same Agent Configuration object
- Your Agent for 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.

Web Agent for IIS Installation Options

The installation program for the SiteMinder Web Agent for IIS offers the following installation options:

Wizard based

Installs the SiteMinder Web Agent using a wizard-based program. This installation program automatically creates a ca-wa-installer.properties file that lets you install subsequent Web Agents on other computers using the unattended or silent method. The same settings you used in the wizard are in the ca-wa-installer.properties file.

Unattended or Silent Installation

Installs the SiteMinder Web Agent using a command line interface. Settings from the ca-wa-installer.propterties file are used. This installation option lets you create your own customized script to install and configure the SiteMinder Web Agent automatically. This method supports silmultaneous installation and configuration of a SiteMinder Web Agent.

Limits: A ca-wa-installer.properties file is required for this option.

Run the Wizard based Installation Program for your Web Agent or Agent for IIS

The wizard based installation program for the SiteMinder Web Agent or SiteMinder Web Agent for IIS installs the Agent on one computer at a time using the Windows operating environment. The wizard based installation program also creates a .properties file for subsequent installations 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.

To run the installation program for your Web Agent or Agent for IIS

1. Copy SiteMinder Web Agent installation executable file to a temporary directory on your IIS web server.
2. Right-click the installation executable file, 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.
3. Use the information from your Agent Installation worksheet to complete the wizard.

More information:

Web Agent Install Worksheet for the Windows Operating Environment (see page 109)

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 saves time if you have a large SiteMinder environment that uses many Web 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.

This section is meant for installing and configuring a SiteMinder Web Agent or Agent for IIS in a single process. Separate configuration of a SiteMinder Web Agent is also supported (see page 41).

Note: A reboot is required between installation and configuration.

To run the unattended or silent installation program for your Web Agent or Agent for IIS

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 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 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:
      - SiteMinder Web Agent Installation executable file.
      - SiteMinder ca-wa-installer properties file.

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

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.

d. Run the following command:

```
agent_executable -f properties_file -i silent
```

Example: ca-wa-IIS7-12.0-sp3-cr002-win64.exe -f ca-wa-installer.properties -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 IIS web server node in your SiteMinder environment that uses the configuration specified by the settings in your ca-wa-installer.properties file.

Chapter 3: Configure a SiteMinder Agent for IIS or Web Agent on an IIS Web Server

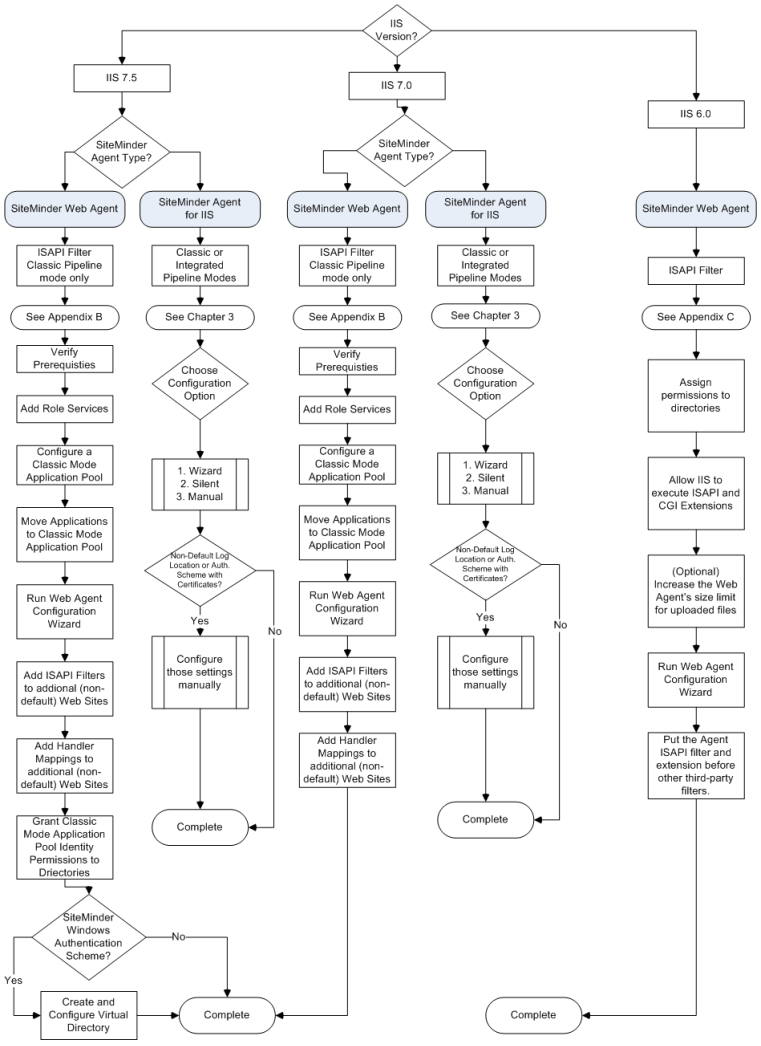
This section contains the following topics:

SiteMinder Agent for IIS and Web Agent Configuration Overview

Because SiteMinder r12.0 SP3 now offers two types of Agents for IIS web servers, the procedures for configuring your SiteMinder Agent for are different for each type of Agent.

For example, the configuration procedures for the SiteMinder r12.0 SP3 Agent for IIS differ from the configuration procedures for the SiteMinder Web Agent.

Use the following illustration to locate the proper configuration procedures for your type of SiteMinder Agent:



SiteMinder Web Agent Configuration Methods

The SiteMinder Web Agent supports the following configuration methods:

Wizard based configuration

Configures the SiteMinder Web Agent using a wizard-based program. This configuration program automatically modifies the ca-wa-installer.properties file that lets you configure subsequent Web Agents on other computers using the unattended or silent method. The same settings you used in the wizard are in the ca-wa-installer.properties file.

Silent or Unattended Configuration

Configures the SiteMinder Web Agent using a command line interface. Settings from the ca-wa-installer.propterties file are used. This configuration option lets you create your own customized script to configure the SiteMinder Web Agent automatically.

Limits: A ca-wa-installer.properties file is required for this option.

How to Configure a SiteMinder Web Agent or Agent for IIS using a Wizard

Configuring a SiteMinder Web Agent or Agent for IIS using the wizard based option involves several separate procedures. To configure a SiteMinder Web Agent or Agent for IIS using a wizard, use the following process:

1. Gather the information for the Web Agent configuration program (see page 34).
2. Run the web Agent Configuration Wizard (see page 38).

   Note: To configure the SiteMinder Agent for IIS from a server farm, run the configuration program on each node in the farm. Start by configuring the Agent for IIS on the first web server in the farm, and then configure the Agent for IIS on 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.
3. Verify that the ISAPI filter is first in the list when using classic pipeline mode (see page 39).

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

Before configuring a Web 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]

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 r12.0 SP3 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

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

Webagent Enable option

Indicates if the configuration wizard enables (starts) the agent automatically. This setting produces the same results as editing the EnableWebAgent parameter value in the WebAgent.conf file with a text editor.

Default: No (clear check box)

Note: We recommend printing a copy of the Web Agent Installation worksheet to record this information for future reference.

More information:

SiteMinder Agent Configuration Worksheet for IIS Web Servers (see page 109)

Run the Web Agent Configuration Wizard

After gathering the information for your Web Agent Configuration worksheet, run the Web Agent Configuration wizard to create a Web Agent runtime instance for the web servers running on your computer.

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.

To run the Web Agent Configuration wizard

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.

   Your SiteMinder Web Agent or Agent IIS is configured.

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.

How to Configure a SiteMinder Web Agent or Agent for IIS Silently

The SiteMinder Web Agent Configuration Wizard creates or modifies the following file each time it runs on a web server:

web_agent_home\install_config_info\ca-wa-installer.properties

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 ca-wa-installer.properties file contains the settings you chose when running the Web Agent Configuration Wizard. Use this file to configure a SiteMinder Web Agent on other web servers in your SiteMinder environment that use 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.

To configure a SiteMinder Web Agent or Agent for IIS silently, perform any of the following procedures:

- Configure a SiteMinder Web Agent for a web server silently (see page 41).
- Configure a SiteMinder Agent for additional virtual websites on a server (see page 43).

To remove a SiteMinder Web Agent or Agent for IIS configuration silently, perform any of the following procedures:

- Remove a SiteMinder Web Agent configuration from a web server silently (see page 45).
- Remove a SiteMinder Web Agent configuration from some virtual websites on a server (see page 47).

Configure a SiteMinder Web Agent or Agent for IIS Silently

If your IIS web server already has a Web Agent or Agent for IIS installed, you can change any of the configuration settings the Agent uses. The SiteMinder Web Agent Configuration program supports a silent or unattended mode that requires no interaction from the end user.

This section is meant for configuring a SiteMinder Agent that has already been installed on a web server. Simultaneous Installation and configuration of a SiteMinder Agent is also supported.

To configure a SiteMinder Web Agent or Agent for IIS silently

1. Run the following wizards on your first IIS web server (in the order shown):
   - The SiteMinder Web Agent Configuration wizard.
2. Locate the following file on your first 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
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 IIS web server node:
      - SiteMinder Web Agent Configuration executable file (ca-wa-config.exe).
      - SiteMinder ca-wa-installer properties file.

   c. Open a command prompt window with Administrative privileges in the temporary directory.

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.

d. 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.

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

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

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.

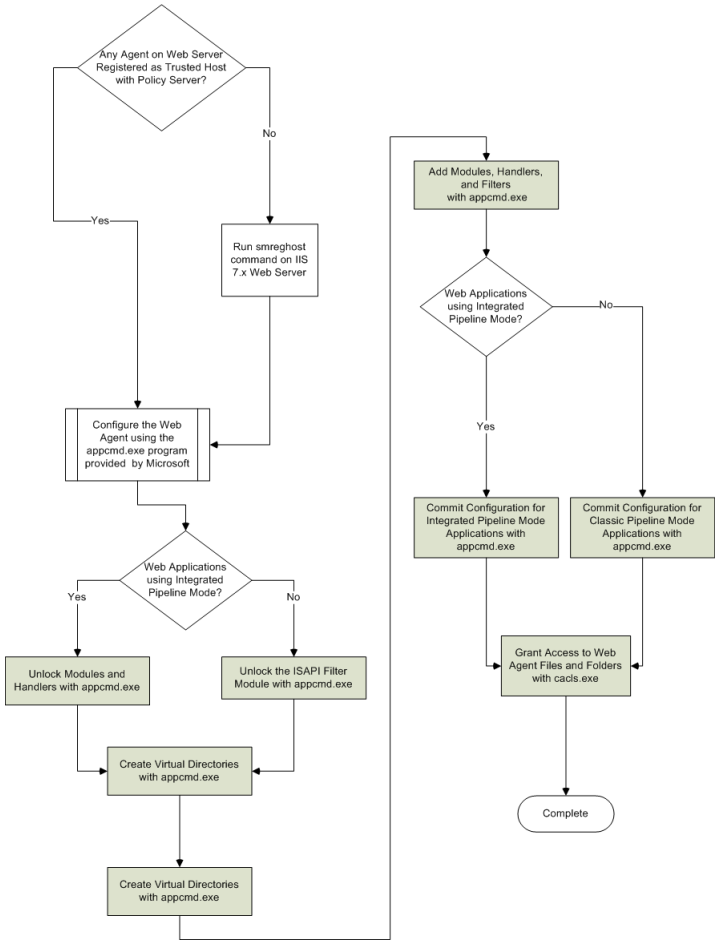
3. Repeat Step 2 for each additional IIS web server node in your environment that uses the configuration specified by the settings in your <flilename>-wa-installer.properties file.

Manual Web Agent Configuration Roadmap

Several tools from third-party vendors are available to configure the SiteMinder Web Agent for IIS manually without using any of the following programs:

- The Web Agent Configuration wizard.
- A Silent or Unattened Web Agent Configuration (using a ca-ca-installer.properties file.

Manual configuration of a SiteMinder Web Agent involves several separate procedures. Those procedures are described in the following illustration:



How to Configure a SiteMinder Agent for IIS Manually

The appcmd.exe command offers one possible way to configure a SiteMinder Agent for IIS manually. This option bypasses the Web Agent Configuration wizard, and the silent or unattended mode.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

To configure a SiteMinder Agent manually, use the following multiple-step process:

1. Run the smreghost.command (see page 51).
2. Unlock the appropriate modules and handlers sections of the IIS configuration file for the applications on your IIS 7.x web server:
   - Integrated Pipeline mode (see page 54).
   - Classic Pipeline mode (see page 55).
3. Create virtual directories (see page 56).
4. Add the appropriate modules, handlers and filters for the applications on your IIS 7.x web server:
   - Integrated Pipeline mode (see page 58).
   - Classic Pipeline mode (see page 60).
5. Grant access to Web Agent files and folders (see page 62).
6. To configure SiteMinder Web Agents on an IIS server farm manually using shared configuration, perform the previous steps on your first IIS web server. Then repeat them on each IIS web server node.

   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.

Run the smreghost.exe Command on your IIS 7.x Web Server

The SiteMinder Web Agent Configuration wizard, and the silent/unattended configuration mode register Web Agents as trusted hosts with SiteMinder Policy Servers.

For manual configurations of SiteMinder Web Agents, run the following command to register a trusted host:

web_agent_home\bin\smreghost.exe

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

To run the smreghost.exe command on your IIS 7.x web server

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.

2. Run the smreghost command. Use the information from your Web Agent Configuration worksheet as values for the following arguments:

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

   -i *policy_server_IP_ address:port*

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

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

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

   Default: (ports) 44441,44442,44443

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

Example: (IPv4 default ports) -i 127.0.0.1

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

Example: (IPv6 default ports) -i [2001:DB8::/32]

-u *administrator_username*

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

-p *Administrator_password*

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

-hn *hostname_for_registration*

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

-hc *host_config_object*

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

-sh *shared_secret*

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

-rs

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

-f *path_to_host_config_file*

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

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

-cf *FIPS mode*

Specifies one of the following FIPS modes:

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

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

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

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

Default: COMPAT

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

-o

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

Your Web Agent is registered as a trusted host.

Unlock Modules and Handlers for Integrated Pipeline Mode Applications with appcmd.exe

The first step for configuring a SiteMinder Web Agent for IIS manually is unlocking the modules and handlers of the IIS 7.x web server. The appcmd.exe command (provided by Microsoft) provides one possible example of how to unlock modules and handlers for configuring a Web Agent manually.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

This procedure describes an example of unlocking the IIS module and handlers for applications using Integrated pipeline mode on an IIS 7.x server. Evaluate your particular implementation and modify any steps accordingly.

To unlock modules and handlers for Integrated Pipeline Mode applications with appcmd.exe

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. Unlock the handler section of the configuration file with the following command:

   ```
   appcmd/commit unlock config-section:system.webServer/handlers
   ```

3. Unlock the modules section of the configuration file with the following command:

   ```
   appcmd/commit unlock config-section:system.webServer/modules
   ```

4. Add the SiteMinder module for IIS 7.x with the following command:

   ```
   appcmd/commit install module
   /name:CASiteMinderWebagentModule/image:"web_agent_home\bin\IIS7WebAgent.dll"
   /preCondition:integratedMode
   ```

   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 modules and handlers for Integrated Pipeline Mode applications are unlocked.

Unlock the ISAPI Filters Module for Classic Mode Applications with appcmd.exe

The first step for configuring a SiteMinder Web Agent for IIS manually is unlocking the modules and handlers of the IIS 7.x web server. The appcmd.exe command (provided by Microsoft) provides one possible example of how to unlock modules and handlers for configuring a Web Agent manually.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

This procedure describes an example of unlocking the IIS module and handlers for applications using Classic pipeline mode on an IIS 7.x server. Evaluate your particular implementation and modify any steps accordingly.

To unlock the ISAPI Filters module for Classic Pipeline Mode applications with appcmd.exe

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. Unlock the IsapiFilters section of the configuration file with the following command:

   ```
   appcmd unlock config/section:system.webServer/isapiFilters
   ```

   The IsapiFilters section of the configuration file is unlocked.

Create Virtual Directories for your Agent for IIS with appcmd.exe

The second step for configuring a SiteMinder Agent for IIS manually is creating the virtual directories for SiteMinder on each website of your IIS 7.x web server. The appcmd.exe command (provided by Microsoft) provides a possible example of how to create virtual directories for a Web Agent manually.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

This procedure describes an example of creating virtual directories for SiteMinder an IIS 7.x server. These directories are normally created by the Configuration wizard. Evaluate your particular implementation and modify any steps accordingly.

Create virtual directories with appcmd.exe

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. Create the siteminderagent virtual directory with the following command:

   ```
   appcmd/commit add vdir/app.name:"your_web_site_name/"
   /path:/siteminderagent/physicalPath:"web_agent_home\samples
   ```

   your_web_site_name

   Specifies the name of your website, as defined in the IIS Manager.

   Default: Default Web Site

   Limits: If the name contains spaces, enclose 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. Create the pw virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/pw /physicalPath:"web_agent_home\pw"
```

4. Create the pwcgi virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/pwcgi/physicalPath:"web_agent_home\pw"
```

5. Create the jpw virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/jpw/physicalPath:"web_agent_home\jpw"
```

6. Create the redirectjsp directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/redirectjsp/physicalPath:"web_agent_home\affwebservice
s\redirectjsp"
```

7. Create the cert virtual directory with the following comand:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/cert /physicalPath:"web_agent_home\samples"
```

8. Create the nocert virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/nocert/physicalPath:"web_agent_home\samples"
```

9. Create the certoptional virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/certoptional/physicalPath:"web_agent_home\samples"
```

10. Create the ntlm virtual directory with the following command:

```
appcmd/commit add vdir/app.name:"your_web_site_name/"
/path:/siteminderagent/ntlm/physicalPath:"web_agent_home\samples"
```

The virtual directories are created.

Add Modules, Handlers and Filters for Integrated Pipeline Mode Applications with Appcmd.exe

The third step for configuring a SiteMinder Web Agent for IIS manually is adding the modules, handlers and filters for SiteMinder on each website of your IIS 7.x web server. The appcmd.exe command (provided by Microsoft) provides a possible example of how to configure a Web Agent manually.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

This procedure describes an example of adding the module and handlers used by SiteMinder for applications using Integrated pipeline mode on an IIS 7.x server. Evaluate your particular implementation and modify any steps accordingly.

To add modules, handlers, and filters for integrated pipeline mode applications with appcmd.exe

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. Add the module with the following command:

   ```
   appcmd/commit add module
   /name:CASiteMinderWebagentModule/app.name:"your_web_site_name/"
   /preCondition:integratedMode
   ```

   your_web_site_name

   Specifies the name of your website, as defined in the IIS Manager.

   Default: Default Web Site

   Limits: If the name contains spaces, enclose it with quotes.

3. Add the kcc handler with the following command:

   ```
   appcmd/commit set config"your_web_site_name/"
   /section:system.webServer/handlers/+[name='CASiteMinderWebAgentHandler-kcc',p
   ath='*.kcc',verb='*',modules='CASiteMinderWebagentModule',resourceType='Unspe
   cified',preCondition='integratedMode']
   ```

4. Add the scc handler with the following command:

```
appcmd/commit set config"your_web_site_name/"
/section:system.webServer/handlers
/+[name='CASiteMinderWebAgentHandler-scc',path='*.scc',verb='*',modules='CASi
teMinderWebagentModule',resourceType='Unspecified',preCondition='integratedMo
de']
```

5. Add the ccc handler with the following command:

```
appcmd/commit set config"your_web_site_name/"
/section:system.webServer/handlers
/+[name='CASiteMinderWebAgentHandler-ccc',path='*.ccc',verb='*',modules='CASi
teMinderWebagentModule',resourceType='Unspecified',preCondition='integratedMo
de']
```

6. Add the ntc handler with the following command:

```
appcmd/commit set config"your_web_site_name/"
/section:system.webServer/handlers
/+[name='CASiteMinderWebAgentHandler-ntc',path='*.ntc',verb='*',modules='CASi
teMinderWebagentModule',resourceType='Unspecified',preCondition='integratedMo
de']
```

7. Add the fcc handler with the following command:

```
appcmd/commit set config"your_web_site_name/"
/section:system.webServer/handlers
/+[name='CASiteMinderWebAgentHandler-fcc',path='*.fcc',verb='*',modules='CASi
teMinderWebagentModule',resourceType='Unspecified',preCondition='integratedMo
de']
```

8. Set the configuration with the following command:

```
appcmd/commit set config"your_web_site_name" /section:system.web/identity
/impersonate:"false"
```

   The modules, handlers and filters for Integrated Pipeline mode applications are added.

Add the Wildcard Mapping and Handlers for Classic Pipeline Mode Applications with Appcmd.exe

The third step for configuring a SiteMinder Web Agent for IIS manually is adding the modules, handlers and filters for SiteMinder on each website of your IIS 7.x web server. The appcmd.exe command (provided by Microsoft) provides a possible example of how to configure a Web Agent manually.

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 appcmd.exe command as part of the IIS web server. You may choose to use the following examples as a guide to configure your SiteMinder Web 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 IIS website, and search for "appcmd".

This procedure describes an example adding a wildcard mapping and a handler used by SiteMinder for applications using Classic pipeline mode on an IIS 7.x server. Evaluate your particular implementation and modify any steps accordingly.

To add the wildcard mapping and handler for classic pipeline mode applications with appcmd.exe

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. Add the wildcard mapping with the following command:

   ```
   appcmdset config"your_web_site_name/"
   /section:system.webServer/isapiFilters/+[name='"SiteMinderAgent"',path='"web_
   agent_home\bin\ISAPI6WebAgent.dll"',enabled='true',preCondition='classicMode'
   ]
   ```

   your_web_site_name

   Specifies the name of your website, as defined in the IIS Manager.

   Default: Default Web Site

   Limits: If the name contains spaces, enclose 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. Add the handler with the following command:

```
appcmdset config"your_web_site_name/" /section:system.webServer/handlers
/+[name='handler-wa',path='*',verb='*',modules='IsapiModule',scriptProcessor=
'"web_agent_home\bin\ISAPI6WebAgent.dll"',resourceType='Unspecified',requireA
ccess='None',preCondition='classicMode']
```

4. Set the configuration with the following command:

```
appcmdset
config-section:system.webServer/security/isapiCgiRestriction/+"[path='web_age
nt_home\bin\ISAPI6WebAgent.dll',allowed='True',groupId='Webagent',description
='Webagent']" /commit:apphost
```

The wildcard mapping and handlers for Classic Pipeline Mode Applications are set.

Grant Access to Agent for IIS Files and Folders with cacls.exe

The final step for configuring a SiteMinder Agent for IIS manually is granting permissions to the SiteMinder files and folders on your IIS 7.x web server. The cacls command (provided by Microsoft) provides a possible example of how to set these permissions manually.

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 cacls.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 SiteMinder Web 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 "cacls".

This procedure describes an example of granting the SiteMinder Agent for IIS permissions to certain access files and folders on an IIS 7.x web server. Perform this procedure for *all* manual configurations, regardless of the pipeline mode used by your application pools.

To grant access to Agent for IIS files and folders with cacls.exe

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. Grant permissions to the SmHost.conf file with the following command:

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

3. Grant permissions to the log file with the following command:

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

4. Grant permissions to the WebAgent.conf file with the following command:

   ```
   cacls"C:\Program Files\CA\webagent\bin\IIS\WebAgent.conf" /T /E /G
   "NetworkService":R
   ```

   Access to the Web Agent files and folders is granted.

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 64):

  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 65).

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.

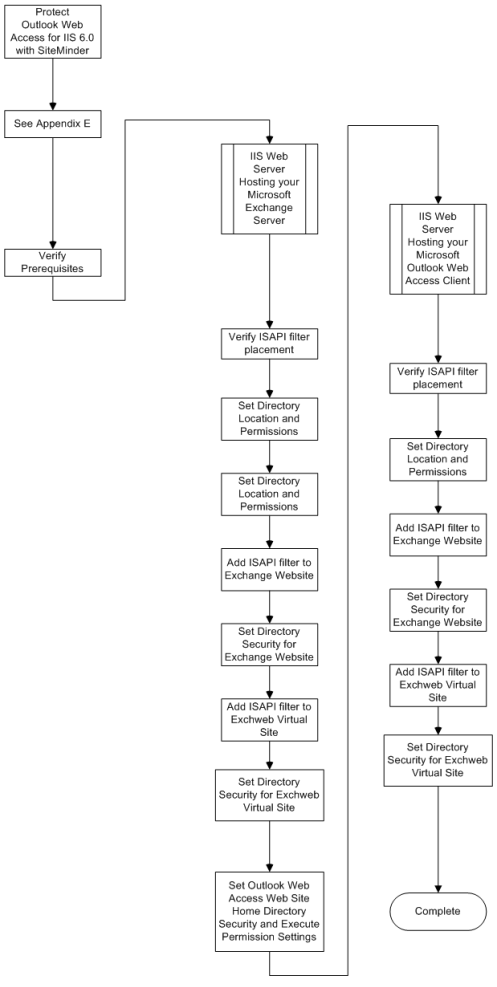
    The changes are applied.

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.

SiteMinder Protection of Outlook Web Access Overview

If your Microsoft Outlook Web Access operates on IIS 6.0 web servers, and you want to protect it with SiteMinder, use the following illustration to locate the configuration procedures:



Chapter 4: Configurations Available for All Web Agents

This section contains the following topics:

Chapter 5: Dynamic Policy Server Clusters

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

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

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

- 192.168.2.100
- 192.168.2.101
- 192.168.2.103
- 192.168.2.104

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

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

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

Connect a Web Agent to a Dynamic Policy Server Cluster

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

Follow these steps:

1. Open the following file with a text editor:

   web_agent_home\config\SmHost.conf

   web_agent_home

   Indicates the directory where the SiteMinder Agent is installed.

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

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

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

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

2. Do *one* of the following tasks:

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

     ```
     enableDynamicHCO="YES"
     ```

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

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

4. Restart your web server.

   The Web Agent is connected to dynamic Policy Server clusters.

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.

How to Set Up Additional Agent Components

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

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

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

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

- Configuring an Agent as a forms credential collector

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

- Configuring an Agent as an SSL credential collector

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

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

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

Chapter 6: Password Services

This section contains the following topics:

Password Services Implementations

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

The following mechanisms are available for implementing password management:

Password Services CGI

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

FCC-based Password Services

Implements Password Services using SiteMinder forms.

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

Password Services servlet

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

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

How to Set Up Your Environment for JSP Password Services

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

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

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

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

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

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

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

More Information

How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server (see page 74)

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\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

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.

Chapter 7: Starting and Stopping Web Agents

This section contains the following topics:

Enable a Web Agent

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

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

Follow these steps:

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

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

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

   The Web Agent is enabled.

Disable a Web Agent

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

Follow these steps:

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

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

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

   The Web Agent is disabled.

Chapter 8: Uninstall a Web Agent

This section contains the following topics:

How to Migrate from an ISAPI-Only SiteMinder Web Agent on IIS 7.x to a SiteMinder r12.0 SP3 Web Agent for IIS 7.x

Web Agent versions *older* than SiteMinder r12.0 SP3 (such as r12.0 SP3 CR1 and earlier) offered only ISAPI-based protection for IIS web servers 7.0 and 7.5. These older Web Agents extended the IIS 6.0 behavior for Classic Mode IIS 7.x applications.

Upgrading from the previous ISAPI-only versions (which also supported IIS 6.0) is *not* supported.

To migrate from the ISAPI-only version to r12.0 SP3 of the Web Agent for IIS, use the following process:

1. Remove the ISAPI-only Web Agent for IIS from your web servers (see page 81).
2. Install the SiteMinder Web Agent for IIS (see page 22).
3. Configure your SiteMinder Web Agent.

Notes About Uninstalling Web Agents

Be aware of the following:

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

Set JRE in PATH Variable Before Uninstalling the SiteMinder Agent

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

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

Follow these steps:

On Windows

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

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

On UNIX

Run the following commands:

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

   JRE

   Specifies the location of your JRE.

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

Uninstall a Web Agent from a Windows Operating Environment

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

Follow these steps:

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

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

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

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

   web_agent_home

   web_agent_home

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

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

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

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

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

12. Start the web server.

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

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 9: Troubleshooting

This section contains the following topics:

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.

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.

500 Error after Configuring Agent for IIS

Symptom:

I configured the Agent for IIS, but I get a 500 error when I try to access a protected resource.

Solution:

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:

- *web_agent_home*\bin directories
- The SmHost.conf file
- The /log directory

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:

      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.

13. Navigate to (but do *not* open) the following directory:

    web_agent_home\bin

14. Right-click the previous directory, and then select Properties.

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

15. Repeat Steps 3 through 9.

    The application pool identities are granted permissions for the SiteMinder SmHost.conf file, \log directory, and \bin directories.

Appendix A: Configure an SiteMinder Web Agent on an IIS 6.0 Web Server

This section contains the following topics:

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\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

   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)

IIS 6.0 Web Agents and Third-Party Software on the Same Server

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.

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\ca\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.

If you decide later to change the directory containing your protected resources on your IIS web server, run the agent configuration wizard again to protect these resources with SiteMinder.

Example:

If you originally configured your web agent to protect resources in the default IIS location C:\inetpub\wwwroot, and you later move those resources to C:\internetfiles, run the configuration wizard again to protect the resources in C:\internetfiles.

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. Use these permissions even if you are logged in to the system as an administrator. For more information, see the release notes for your SiteMinder component.

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

2. If you have 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

Install a Web Agent on a Windows System (see page 21)

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\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

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 Windows 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 Windows challenge and response for credentials.

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

Appendix B: Protect Microsoft Outlook Web Access with SiteMinder and IIS 6.0

This section contains the following topics:

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 r12.0 SP3 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 (r12.0 SP3) 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\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

■

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.

Appendix C: 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	

More information:

Run the Wizard based Installation Program for your Web Agent or Agent for IIS (see page 28)

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	

Information Needed	Your Value
IP Address	
FIPS Mode Setting	
SmHost.conf file Name	
SmHost.conf file Locations	
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 27)

Index

I

J

L

M

N

O

P

R

S

T

U

V

W