CA SiteMinder®

Web Agent Installation Guide for IIS

12.52 SP1

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- CA IdentityMinder™ (formerly CA Identity Manager)
- CA SiteMinder® Web Services Security (formerly 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

No updates have been made to the 12.52 SP1 documentation, as a result of issues found in previous releases.

The following updates have been made to the 12.52 documentation, as a result of issues found in previous releases:

- Uninstall a Web Agent (see page 61)—Removed obsolete material related to installing a supported JRE and including it in the system path. A JRE is now included with the software (CQ 178969).
- How to Upgrade an Agent for IIS from Version 12.0.2 or Lower (see page 48)—Revised upgrade procedures for upgrading from versions 12.0.2 or older to 12.52 and later. Resolves CQ 170479 and STAR Issue 21402742:01.
- Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode (see page 29)—Added new instructions for verifying the ISAPI filter placement. Resolves CQ 170577 and STAR Issue 21403389:01

Contents

Chapter 1: Preparation

This section contains the following topics:

Only IIS Web Server Procedures in this Guide

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

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

- *Web Agent Installation Guide for Apache-based servers*.
- *Web Agent Installation Guide for Domino*.
- *Web Agent Installation Guide for Oracle iPlanet*.

Hardware Requirements for CA SiteMinder® Agents

Windows

agents operating on Windows require the following hardware:

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

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

This product combines all functions for Internet Information Services (IIS) into one agent.

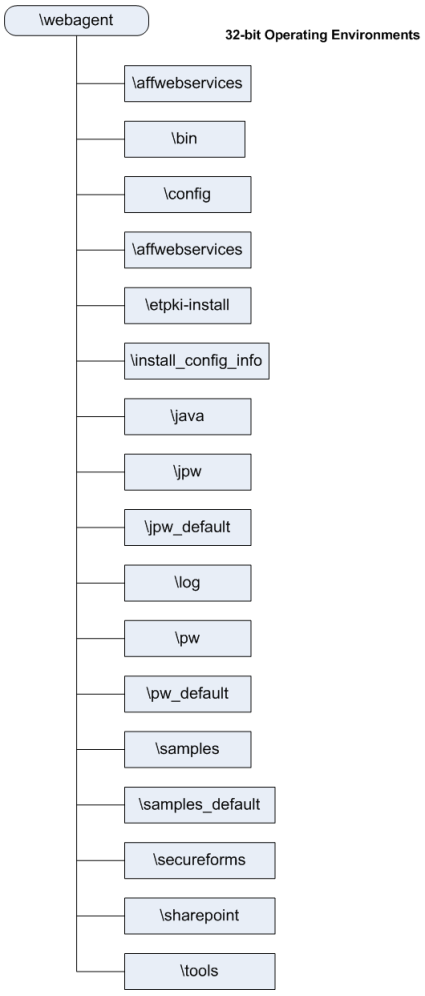
A Web Agent for IIS implemented as an ISAPI plug-in and a native HTTP module that supports the following functions:

- Application pools using Integrated or Classic pipeline mode.
- Application pools that are configured with the Enable 32-bit applications option.
- The optional IIS Application Request Routing (ARR) feature.
- Supported with IIS 7.0 and 7.5, including IIS clusters and shared configuration deployments.

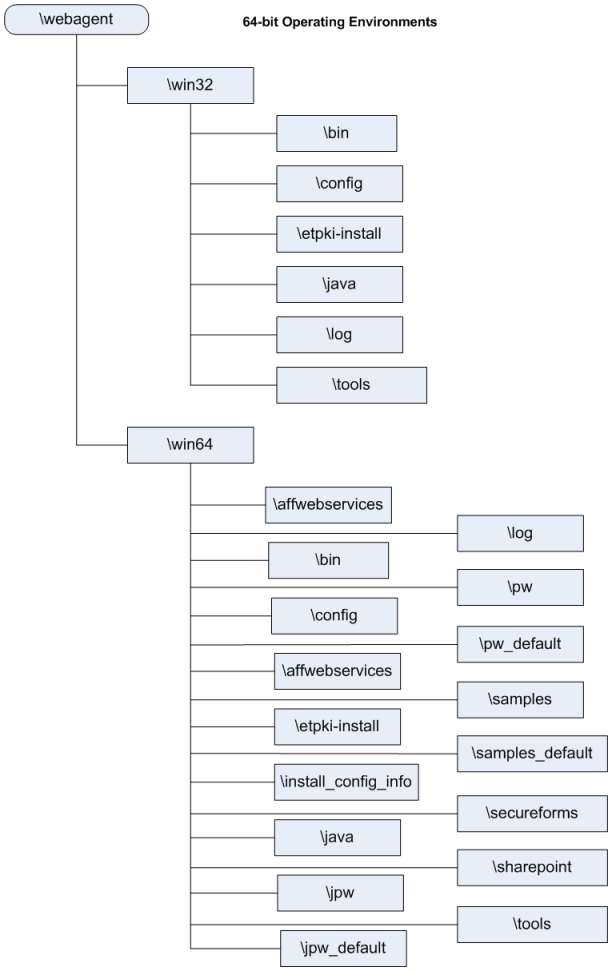
Multiple Agent for IIS Directory Structures

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:

- CA SiteMinder® Agents for IIS use the directory structure shown in the following illustration:



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

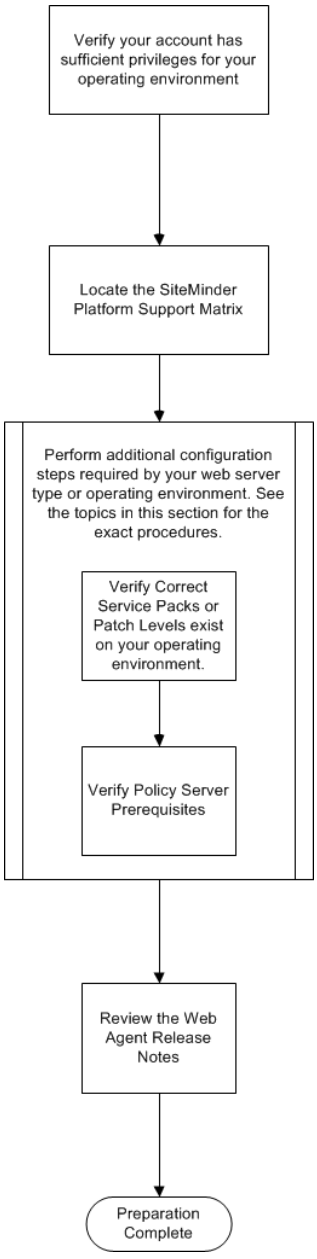


More information:

Run the Installation Wizard to Upgrade your Agent for IIS (see page 46)

CA SiteMinder® Agent Preparation Roadmap

The following illustration describes how to prepare your Windows operating environment for the CA SiteMinder® agent for IIS:



How to Prepare for an Agent for IIS Installation

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

1. Verify that you have an account with Administrative privileges for the computer on which you want to install the agent (see page 12).
2. Verify that the IIS role, the related role services and features are installed on your Windows operating environment (see page 13).
3. Locate the CA SiteMinder® Platform Support Matrix (see page 13). Confirm that your IIS web server meets the requirements for the agent version you want to install.
4. Verify that the Windows operating environment for your IIS web server has the proper service packs and updates installed (see page 14).
5. Confirm that your Policy Server has the prerequisites for an agent Installation (see page 14).
6. Review the *Web Agent Release Notes* for known issues (see page 15).

Verify that you have an Account with Administrative Privileges

To install or configure a CA SiteMinder® Web Agent or CA 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 CA SiteMinder® Web Agent or CA 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 CA SiteMinder® Web Agents or CA SiteMinder® Agents for IIS on Windows 2008 systems, see the Web Agent Release Notes.

Verify that the IIS Role and Role Services are Installed

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

Follow these steps:

1. Click Start, All Programs, Administrative Tools, Server Manager.
2. Verify that IIS appears in the Roles list.
3. If the Web Server (IIS) role is not shown, add it using the Add Roles wizard. If you decide to use the ISAPI-filter functions of the Agent for IIS, add the following role services too:
   - ASP.NET
   - CGI
   - ISAPI Extensions
   - ISAPI Filters
   - IIS Management Console
   - Windows Authentication (for the CA SiteMinder® Windows Authentication Scheme)

Locate the Platform Support Matrix

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

Follow these steps:

1. Go to the CA Support site.
2. Click Product Pages.
3. Enter the product name and click Enter.
4. Open popular links and click Informational Documentation Index.
5. Click Platform Support Matrices.

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

Technology Partners and CA Validated Products

The latest list of partners and their validated products.

Verify that the Windows IIS Web Server has the Latest Service Packs and Updates

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

Review the Policy Server Prerequisites for Agent for IIS Installations

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

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

The Administrative UI creates these 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.

Agents for IIS require the names of the following CA 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 CA 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 CA SiteMinder® Policy Server.

AgentName

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

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

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

Default: No default

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

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

Example: myagent1,192.168.0.0 (IPV4)

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

Example: myagent, www.example.com

Review the Web Agent Release Notes for Known Issues

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

Follow these steps:

1. Open a web browser and navigate to the Technical Support website.
2. Click Enterprise/Small and Medium Business.
3. Under the Get Support tab, click Product Documentation.
4. Click the field under Select a Bookshelf.
5. Type siteminder.
6. Click the bookshelf that you want from the list, and then click Go.
7. Click Release Notes.

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

This section contains the following topics:

Agent Installation Compared to Agent Configuration

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

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

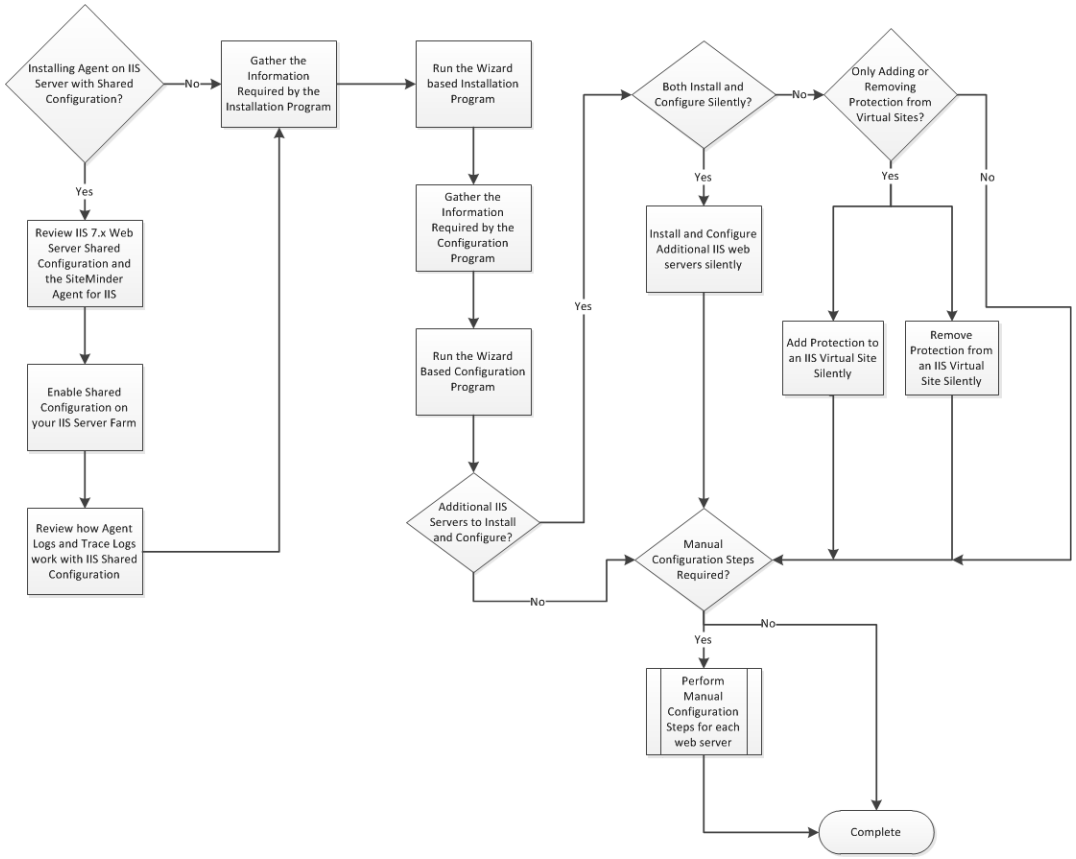
Configuration occurs after installation and means the act of preparing the CA SiteMinder® agent software for a specific web server on a computer. This preparation includes registering the agent with CA SiteMinder® Policy Servers, and creating a runtime server instance for the web server that is installed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

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

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

Agent for IIS Installation and Configuration Roadmap

The following illustration describes the process installing and configuring a CA SiteMinder® Agent for IIS:



How to Install and Configure an Agent for IIS

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

1. If you are deploying the Agent for IIS to an IIS server farm, review the following topics:
   - IIS 7.x web server shared configuration (see page 19).
   - How web agent logs and trace logs work with shared configuration (see page 21).
2. Gather the information for the installation program (see page 23).
3. Run the wizard based installation program (see page 23).
4. Gather the information for the configuration program (see page 25).
5. Run the wizard based configuration program (see page 28).
6. Verify that the ISAPI Filter is First in the List When Using Classic Pipeline Mode (see page 29)
7. (Optional) Install and configure additional Agents for IIS silently (see page 30).
8. (Optional) Add (see page 31) or remove (see page 34) CA SiteMinder® protection from virtual sites on IIS web servers silently.
9. Determine if your Agent for IIS requires any manual configuration steps (see page 39).

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

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

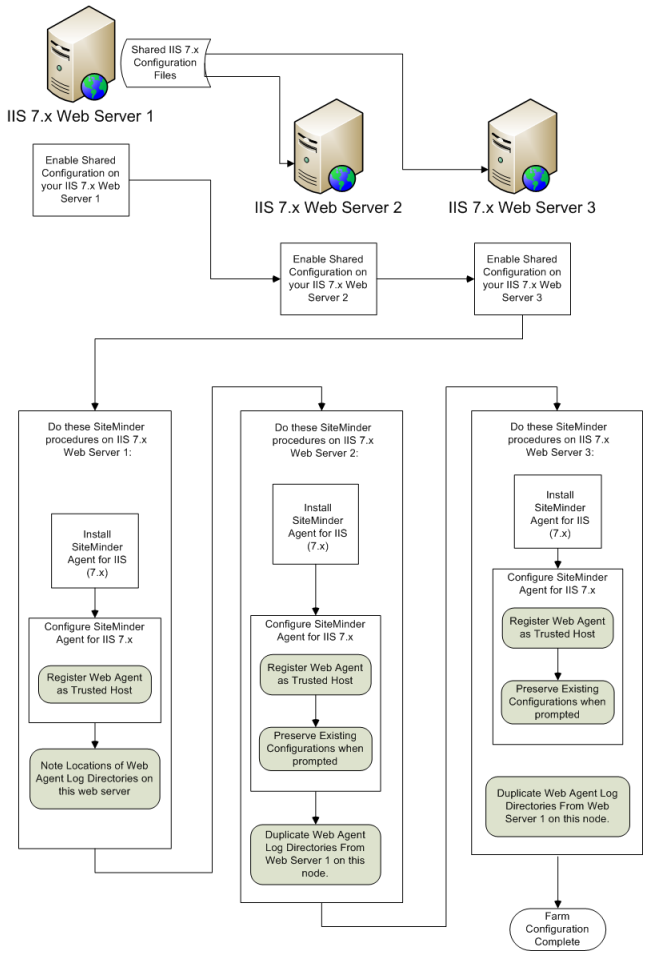
The Agent for IIS can protect resources on IIS server farms that use the shared configuration feature of IIS 7.x.

Note: This feature works *only* with the CA SiteMinder® 12.52 SP1 Agent for IIS 7. Older versions of the CA SiteMinder® Web Agent do *not* support this feature.

IIS 7.x uses network shares to propagate the configuration information across the server farm. The CA SiteMinder® 12.52 SP1 Agent for IIS, however, *cannot* operate on network shares. Using a CA SiteMinder® 12.52 SP1 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 CA 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 CA 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:

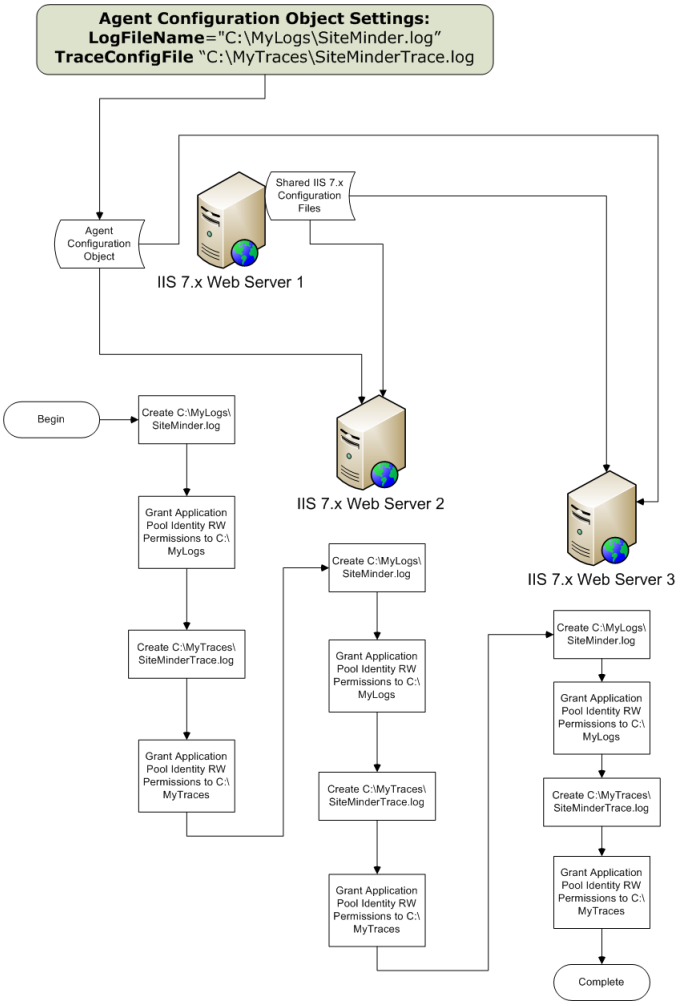
- Your Agent for IIS log and trace log directories are specified in an Agent Configuration Object on the Policy Server (*not* in a local configuration file).
- Any of the CA SiteMinder® Agents for IIS in your IIS 7.x web servers in the server farm share the same Agent Configuration object
- Your Agent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

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

Installation Directory

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

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

Shortcut Location

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

Run the Installation Program on Windows

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

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

Follow these steps:

1. Copy the Web Agent installation executable file to a temporary directory on your web server.
2. Do *one* of the following steps:
   - For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.
   - For console-based installations, open a command line window and run the executable as shown in the following example:

     ```
     executable_file_name.exe -i console
     ```
3. Use the information that you gathered previously to complete the installation.

More information:

Web Agent Install Worksheet for the Windows Operating Environment (see page 71)

Gather Information for the Agent Configuration Program for IIS Web Servers

Before configuring a CA SiteMinder® Agent on an IIS web server, gather the following information about your environment.

Host Registration

Indicates whether you want to register this agent as a trusted host with a Policy Server. Only one registration per agent is necessary. If you are installing the CA 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 CA 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 CA 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 CA 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 CA SiteMinder® Agent for IIS on an IIS web server farm, specify a *unique* name for *each* IIS server node on the farm. For example, if your farm uses six servers, specify six unique names.

Host Configuration Object

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

IP Address

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

Default: (authentication port) 44442

Example: (IPv4) 127.0.0.1,55555

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

Note: If a hardware load balancer is configured to expose Policy Servers in your environment through a single Virtual IP Address (VIP), enter the VIP.

FIPS Mode Setting

Specifies *one* of the following algorithms:

FIPS Compatibility/AES Compatibility

Uses algorithms existing in previous versions of CA SiteMinder® to encrypt sensitive data and is compatible with previous versions of CA 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, CA SiteMinder® environment continues to use existing CA 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 CA SiteMinder® environment. This setting does not interoperate with, nor is backwards-compatible with, previous versions of CA 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 CA SiteMinder® agent and the CA 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 CA 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 CA SiteMinder®.

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

Overwrite, Preserve, Unconfigure

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

- IIS 7.x websites that CA SiteMinder® 12.52 SP1 already protects on a stand-alone IIS web server.
- IIS 7.x websites that CA SiteMinder® protects on an IIS server farm using shared configuration.

Select *one* of the following options:

Overwrite

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

Preserve

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

Unconfigure

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

More information:

CA SiteMinder® Agent Configuration Worksheet for IIS Web Servers (see page 71)

Run the Web Agent Configuration Wizard

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

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

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

Follow these steps:

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

   The Web Agent Configuration wizard starts.

3. Complete the wizard.

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

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

Follow these steps:

1. Open IIS Manager using the following steps:
   a. Click Start, Control Panel.

      The control panel opens.

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

      IIS Manager opens.
2. Verify the ISAPI filter is first in the list using the following steps:
   a. From IIS Manager, expand the following items:
      - Your web server
      - Sites
      - Default Web Site

   b. Double-click the Handler Mappings icon.
   c. Click view ordered list.
   d. Verify that the following ISAPI filter appears in the top of the list:

      `handler-wa`
3. If the ISAPI filter from Step 2d does *not* appear first in the list, do the following steps:
   a. Click the handler-wa ISAPI filter.
   b. Click the Move up arrow until the ISAPI filter appears first in the list.

   The ISAPI filter appears first in the list.

Run a Silent Installation and Configuration on an IIS Agent

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

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

Follow these steps:

1. Run the following wizards on your first IIS web server (in the order shown):
   a. The CA SiteMinder® Web Agent Installation wizard.
   b. The CA SiteMinder® Web Agent Configuration wizard.
2. Locate the following file on your first IIS web server:

   web_agent_home\install_config_info\ca-wa-installer.properties

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

   web_agent_home

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

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

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

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with CA SiteMinder® Web Agents for IIS only]): C:\Program Files (x86)\webagent\win3
3. Perform each of the following steps on the other IIS web server nodes in your environment:

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

   a. Create a temporary directory on an IIS web server node.
   b. Copy the following files from your first IIS web server (from Steps 1 and 2) to the temporary directory on your other IIS web server:
      - The CA SiteMinder® Web Agent Installation executable file.
      - The CA SiteMinder® ca-wa-installer properties file.
   c. Open a Command Prompt window with Administrative privileges in the temporary directory.

d. Run the following command:

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

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

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

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

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

Follow these steps:

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 CA SiteMinder® Agent is installed on your web server.

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

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

Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with CA 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:

      - CA SiteMinder® Web Agent Configuration executable file (ca-wa-config.exe).
      - CA SiteMinder® ca-wa-installer properties file.

   c. Open the CA 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 CA 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.

Important! Before running a CA 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 CA SiteMinder® Web Agent for IIS is installed and configured on the node automatically.

j. (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 Web Agent Configuration from an IIS Web Server Silently

To remove the CA 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.

Follow these steps:

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 CA SiteMinder® Agent is installed on your web server.

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

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

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with CA 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 CA 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 CA 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 CA 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 CA 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 CA 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 CA 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 CA SiteMinder® Web Agent Configuration program supports a silent or unattended mode that requires no interaction from the end user.

Follow these steps:

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 CA SiteMinder® Agent is installed on your web server.

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

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

   Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with CA 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 CA 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 CA 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 CA 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 CA 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 CA 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.

Important! Before running a CA 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.

h. 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 CA SiteMinder® configuration is removed from the selected virtual sites on the node automatically.

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

How to Configure Certain Settings for the Agent for IIS Manually

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

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

- Your CA SiteMinder® Agent for IIS log files are *not* stored in the following default directory:

  web_agent_home\log

  web_agent_home

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

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

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

  Default (Windows 32-bit applications operating on 64-bit systems [Wow64 with CA 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 an authentication scheme which requests or requires client certificates.

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 CA 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"

Follow these steps:

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

   Important! Before running a CA 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 CA SiteMinder® on your IIS web server.

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 CA SiteMinder® Authentication Schemes Requiring Certificates

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

- cert
- certoptional

Follow these steps:

1. Open IIS manager.
2. Expand your web server.

The Application pools icon and Sites folder appear.

3. Expand Sites.
4. Expand the website associated with your authentication scheme that requires certificates.

   The siteminderagent virtual folder appears.
5. Expand the siteminderagent virtual folder.
6. Click the cert folder.
7. Double-click SSL Settings.
8. Select the Require SSL check box, and then click the Require option button.
9. Under Actions, click Apply
10. Click the certoptional folder.
11. Double-click SSL Settings.
12. Click the Accept option button.
13. Under Actions, click Apply.
14. Repeat Steps 3 through 14 for other websites on your IIS web server that require certificates.
15. For IIS server farms using Shared Configuration, repeat Steps 1 through 15 on each IIS web server in your farm.

    The settings are changed.

Chapter 3: Upgrade a Web Agent to 12.52 SP1

This section contains the following topics:

Agent for IIS Upgrade Roadmap

The following illustration describes the process of upgrading an Agent for IIS to r12.5:

How to Prepare for a CA SiteMinder® Agent Upgrade

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

1. Create backup copies of any customized CA SiteMinder® files on your web server. Examples of files you could have customized after installing or configuring your agent include the following files:
   - LocalConfig.conf
   - WebAgent.conf
2. Record the values of the following logging parameters in the agent configuration object of the agent that you want to upgrade:
   - LogFileName
   - TraceFileName
   - TraceConfigFile
3. Gather information for the following CA SiteMinder® programs.
   - The Agent installation wizard (see page 23).
   - (only If upgrading from version 12.0.2 or older) The Agent configuration wizard (see page 25).
4. Do *one* of the following tasks:
   - If you are upgrading from version 12.0.3 or higher to 12.52 SP1, go to Step 5.
   - If you are upgrading from version 12.0.2 or older, continue with this procedure instead (see page 48).
5. Run the installation wizard to upgrade your Agent for IIS (see page 46).
6. Add the logging parameter values (from Step 2) to your agent configuration object (see page 47).

Source the Environment Script on UNIX and Linux Operating Environments

If you are upgrading a Web Agent on a UNIX or Linux system, source the environment script that is available in the following directory:

CA SiteMinder® 6.0

web_agent_home/nete_wa_env.sh

CA SiteMinder® 12.0 and later

web_agent_home/ca_wa_env.sh

web_agent_home

Indicates the directory where the CA SiteMinder® Agent is installed.

Default: /opt/ca/webagent

Run the Installation Wizard to Upgrade your Agent for IIS

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

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

Follow these steps:

1. Copy the Web Agent installation executable file to a temporary directory on your web server.
2. Do *one* of the following steps:
   - For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.
   - For console-based installations, open a command line window and run the executable as shown in the following example:

     executable_file_name.exe -i console
3. Use the information that you gathered previously to complete the installation.

More information:

Multiple Agent for IIS Directory Structures (see page 9)

Add the logging parameter values to your agent configuration object

Occasionally, certain logging parameters are not copied correctly to the new version during an Agent for IIS upgrade. Complete the upgrade by adding the values of the logging parameters from the old version to the agent configuration object.

Update the values of the following parameters:

LogFileName

Specifies the full path (including the file name) of the log file.

Default: No

Example: (Windows) *web_agent_home*\log\WebAgent.log

Example: (UNIX/LInux)
/export/iPlanet/servers/https-jsmith/logs/WebAgent.log

TraceFileName

Specifies the full path to the trace log file.

Default: No default

Limits: Specify the file name in this parameter.
Example: *web_agent_home*\log\trace.log

TraceConfigFile

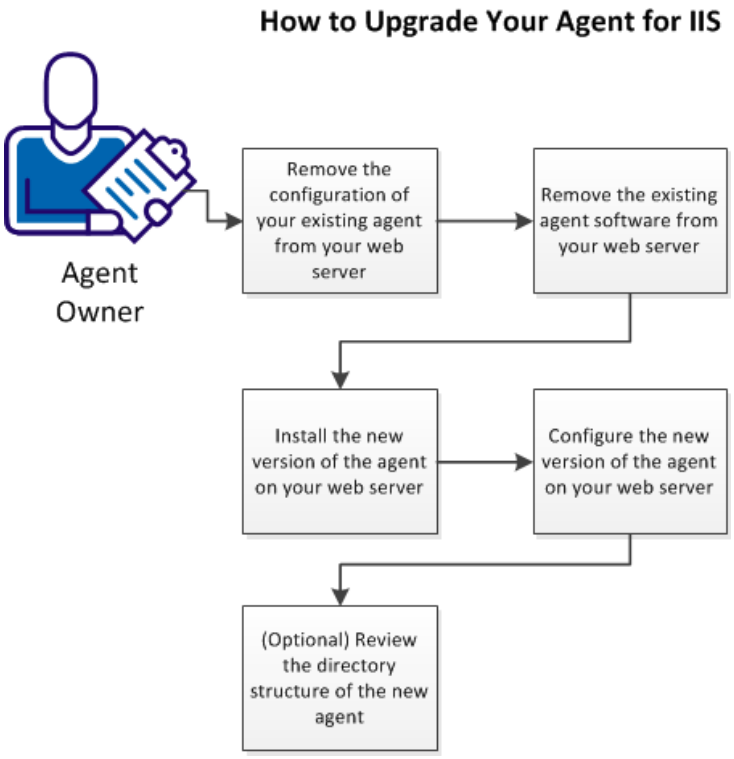
Specifies the location of the WebAgentTrace.conf configuration file that determines which components and events to monitor.

Default: No default

Example: *web_agent_home*\config\WebAgentTrace.conf

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

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



Follow these steps:

1. Remove the configuration of your existing agent from your web server (see page 49).
2. Remove the existing agent software from your web server (see page 50).
3. Install the new version of the agent on your web server (see page 52).
4. Configure the new version of the agent on your web server (see page 53).
5. (Optional) Review the directory structure of the new agent (see page 54).

Remove the configuration of your existing agent from your web server

Before upgrading your agent to 12.0.3 or higher, remove the server configuration from the previous version of your agent using the configuration wizard. For example, if you are upgrading from 6.x to 12.52 SP1, remove the server configuration for the 6.x version of your agent using the configuration wizard.

Follow these steps:

1. Start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, CA SiteMinder®, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure differs slightly.

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

2. Skip to the next step. You do *not* need to register a trusted host.
3. Clear the check boxes of the web server instances from which you want to remove the configuration.
4. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance, then click Next.

   This name must match an Agent Configuration Object that already defined at the Policy Server.

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

   The Web Agent files are installed.

6. Click Done when the installation is complete.
7. Reboot the computer.

Remove the existing agent software from your web server

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

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.

Follow these steps:

1. Stop the web server.
2. Remove the configuration settings for the agents on your server with *one* of the following procedures:
   - To un-configure the agent with the wizard, go to Step 3.
   - To un-configure the agent with the console-based program, go to Step 6.
3. Click Start, All Programs, CA, CA SiteMinder®.

   A shortcut to the Web Agent Configuration wizard appears.
4. 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 CA SiteMinder® component.

   The Web Agent Configuration wizard starts.
5. Clear the check boxes from the agent instances configured on your web server, and complete the wizard.
6. Open a Command Prompt window with root privileges.
7. Navigate to the ca-wa-config.exe file, and then run it with the following switch:

   ```
   -i console
   ```
8. Un-configure the agent instances configured on your web server. Wait for the configuration program to finish, then go to Step 9.
9. Choose *one* of the following procedures:
   - To remove the Web Agent using the wizard, go to Step 10.
   - To remove the Web Agent using the console-based program, go to Step 15.
10. Click Start, Control Panel, Programs and Features.

A list of installed programs appears.

11. Click CA CA SiteMinder® Web Agent *version_number*.
12. Click Uninstall/Change.

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

    The wizard removes the web agent.
14. Wait for the wizard to finish, then go to Step 17.
15. Open a command-line window.
16. Navigate to the following directory.

    web_agent_home

    web_agent_home

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

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

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

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

    ```
    ca-wa-uninstall.cmd -i console
    ```
18. Wait for the un–installation program to finish, then go to Step 19.
19. Start the web server.

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

Install the new version of the agent on your web server

After unconfiguring and removing the older version of your agent, install version 12.52 SP1 on your web server.

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

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

Follow these steps:

1. Copy the Web Agent installation executable file to a temporary directory on your web server.
2. Do *one* of the following steps:
   - For wizard-based installations, right-click the installation executable file, and then select Run as Administrator.
   - For console-based installations, open a command line window and run the executable as shown in the following example:

     ```
     executable_file_name.exe -i console
     ```

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

Configure the new version of the agent on your web server

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

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

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

Follow these steps:

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

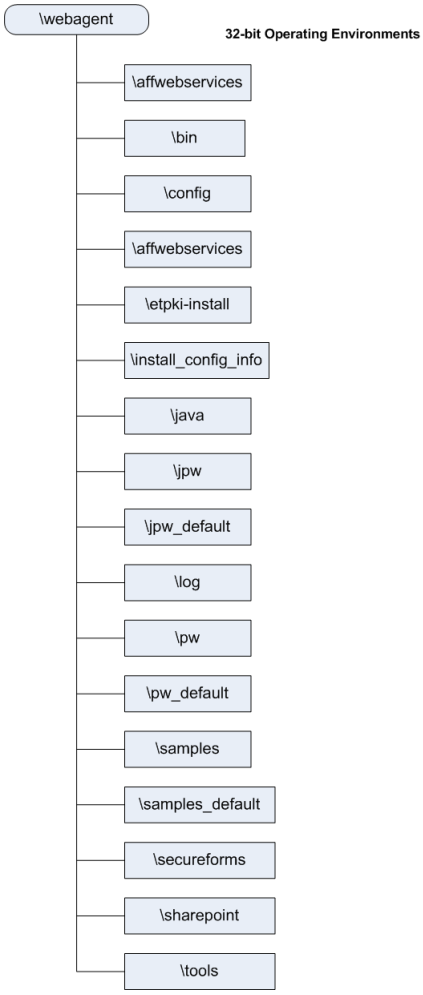
   The Web Agent Configuration wizard starts.

   Complete the wizard.

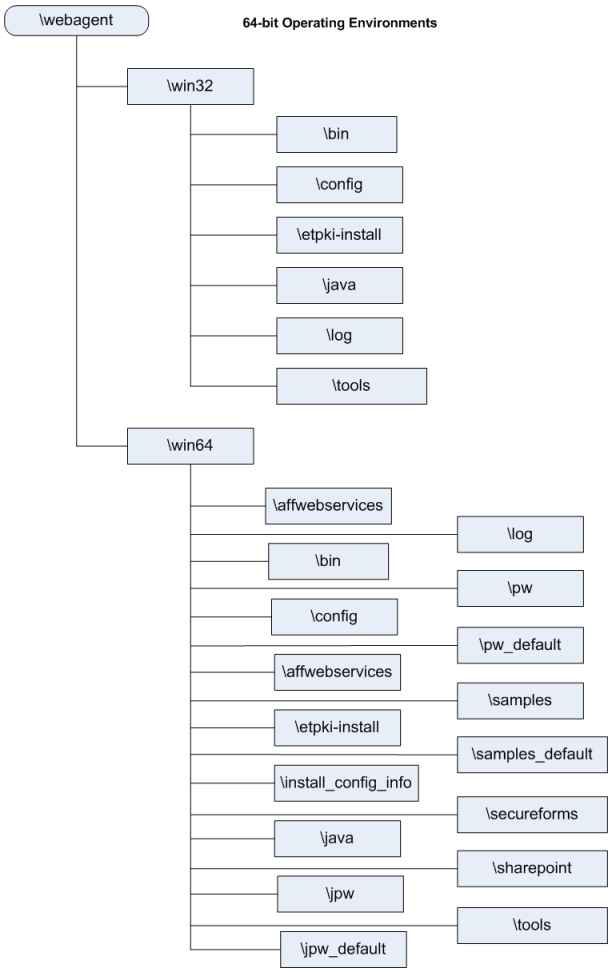
(Optional) Review the directory structure of the new agent

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

- CA SiteMinder® Agents for IIS use the directory structure shown in the following illustration:



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



Chapter 4: Dynamic Policy Server Clusters

Earlier versions of CA 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.

CA SiteMinder® 12.52 SP1 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 CA SiteMinder® Agent is installed.

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

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

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

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

2. Do *one* of the following tasks:

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

     enableDynamicHCO="YES"

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

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

4. Restart your web server.

   The Web Agent is connected to dynamic Policy Server clusters.

Chapter 5: Starting and Stopping Web Agents

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 CA SiteMinder® Policy Server.

Follow these steps:

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

   Note: Agents for IIS installed on 64-bit operating environments have *two* WebAgent.conf files. One file for 32-bit Windows applications. The other file is for 64-bit Windows applications. Modify *both* WebAgent.conf files when starting or stopping the Agent for IIS.

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: Agents for IIS installed on 64-bit operating environments have *two* WebAgent.conf files. One file for 32-bit Windows applications. The other file is for 64-bit Windows applications. Modify *both* WebAgent.conf files when starting or stopping the Agent for IIS.

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

   The Web Agent is disabled.

Chapter 6: Uninstall a Web Agent

This section contains the following topics:

Notes About Uninstalling Web Agents

Be aware of the following:

- All Web Agents for all installed web servers will be uninstalled.
- The Password Services and Forms directories, (pw_default, jpw_default, samples_default) will be removed. However, the non-default copies of these directories (pw, jpw, samples) are not removed because these directories may contain customized files.

Uninstall an IIS Agent

Before you remove the CA SiteMinder® Web Agent from a Windows operating environment, consider making backup copies of your registry settings and Web Agent configuration settings.

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.

Note: To remove the CA SiteMinder® Web Agent for IIS from a server farm, run the uninstall program on *each* node in the farm. Start by removing the Web Agent from the first web server in the farm, and then remove the Web Agent from all other nodes. The first server refers to the IIS web server where the shared configuration information is stored. A node refers to any IIS web servers which read the shared configuration from the first server.

Follow these steps:

1. Stop the web server.
2. Run the configuration wizard to remove the configuration settings of the agents that you want to remove.
3. 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.
4. Click Start, Control Panel, Programs and Features.
5. Click CA CA SiteMinder® Web Agent *version*.
6. Click Uninstall/Change.
7. Review the information in the Uninstall CA SiteMinder® Web Agent dialog, then click Uninstall.
8. Wait for the wizard to finish, then go to Step 12.
9. Open a command-line window.

10. Navigate to the following directory.

    web_agent_home

    web_agent_home

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

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

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

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

11. Run the following command:

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

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

13. 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 an IIS Agent

The CA SiteMinder® Agent supports an unattended mode that uninstalls the agent. 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 CA 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 configuration wizard to remove the configuration settings of the agents that you want to remove.
4. 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 CA SiteMinder® Agent is installed on your web server.

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

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

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

   The agent is removed from the web server.
5. For IIS server farms, repeat Steps 1 though 3 for each web server in your farm.

Chapter 7: Troubleshooting

This section contains the following topics:

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

When you install and configure the CA 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\Wow6432Node\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 CA SiteMinder® Agent for IIS. Use this setting to control when the CA SiteMinder® module executes.

Follow these steps:

1. Open the Windows Registry Editor on your IIS web server.
2. Expand the following keys:

   ```
   HKLM\SOFTWARE\Wow6432Node\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 CA 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 CA 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 CA 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 CA 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 CA 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 CA SiteMinder® agent. Now the resources in the new document root folder are unprotected.

Solution:

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

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

Symptom:

The CA SiteMinder® Agent does not start or shut down.

Solution:

Do the following tasks:

- Run the Low Level Agent Worker Process (LLAWP) separately to isolate the problem.
- For the Windows operating environment Windows, see the Application Log in the Event Viewer.

Event Viewer Message Describes lack of Permissions on Host Configuration File

Valid on IIS

Symptom:

I see the following messages in my event viewer:

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

Solution:

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

- The SmHost.conf file

Follow these steps:

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

   web_agent_home\config\SmHost.conf

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

   The SmHost.conf Properties dialog appears.

3. Click the Security tab.

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

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

   The Permissions for SmHost.conf dialog appears.

5. Click Add.

   The Select Users, Computers, or Groups dialog appears.

6. Do the following steps:

   a. Click Locations.

      The Locations dialog appears.

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

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

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

   `IIS AppPool\Application_Pool_Name`

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

   `IIS AppPool\DefaultAppPool`

d. Click Check Names, and then click OK.

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

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

   The Permissions for SmHost.conf dialog closes.

9. Click OK.

   The SmHost.conf Properties dialog closes. The application pool identities are granted permission for the CA SiteMinder® SmHost.conf file.

Appendix A: Worksheets

This section contains the following topics:

Web Agent Install Worksheet for the Windows Operating Environment

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

Information Needed	Your Value
Installation Directory	
Shortcut Location	

CA SiteMinder® Agent Configuration Worksheet for IIS Web Servers

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

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

Information Needed	Your Value
SmHost.conf file Locations	
Select Servers	
Overwrite, Preserve, Unconfigure	
Agent Configuration Object Name	
Webagent Enable Option	

More information:

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

Index