CA SiteMinder® Web Services Security

WSS Agent Guide for IIS Web Servers

12.52

CA Technologies Product References

This document references the following CA Technologies products:

- CA SiteMinder®
- 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.

Contents

Chapter 1: CA SiteMinder® Web Services Security Agent for Web Servers Introduction 9

Chapter 2: Preparation 13

Chapter 3: Install an Agent for IIS on Windows Operating Environments 23

Chapter 4: Upgrade a SOA Agent to a 12.52 WSS Agent 51

Chapter 5: Advanced Configuration 55

Chapter 6: Dynamic Policy Server Clusters 61

Chapter 7: Starting and Stopping SiteMinder WSS Agents 63

Chapter 8: Uninstall a SiteMinder WSS Agent 69

Chapter 9: SiteMinder WSS Agent Logging 71

Chapter 10: Troubleshooting 99

Appendix A: Worksheets 103

Chapter 1: CA SiteMinder® Web Services Security Agent for Web Servers Introduction

This section contains the following topics:

Overview

The SiteMinder Web Services Security (WSS) Agent for Web Servers is an XML-enabled version of the CA SiteMinder Web Agent that operates with a web server to handle XML messages sent to web service implementations.

When a web consumer (client) application sends an XML message to a URL that is bound to a web service, the SiteMinder WSS Agent intercepts these messages and communicates with the Policy Server to process authentication and authorization requests before the XML message is passed on to the web service. In addition, the Policy Server can provide information that the SiteMinder WSS Agent adds to the XML message, such as a SAML assertion based on the originating client application's identity.

Note: If you have purchased CA SiteMinder®, you can also use the core Web Agent functionality of the SiteMinder WSS Agent to protect other resources on a Web server. For more information about this functionality, see the CA SiteMinder® documentation—the remainder of this chapter deals specifically with use of the SiteMinder WSS Agent to protect web services.

SiteMinder WSS Agent Functions

The SiteMinder WSS Agent performs the following tasks:

- Intercept posted XML messages to protected Web services and work with the Policy Server to determine whether or not a client application should have access.

- Ensure a client application’s ability to access Web services quickly and securely. The SiteMinder WSS Agent stores contextual information about client application access privileges in a session cache. You can optimize performance by modifying the cache configuration settings.
- Support multistep and chain authentication service models by generating and consuming SAML Session Tickets and WS-Security tokens.

The SiteMinder WSS Agent and the Policy Server

To enforce web service access control, the SiteMinder WSS Agent interacts with the Policy Server, where all authentication and authorization decisions are made.

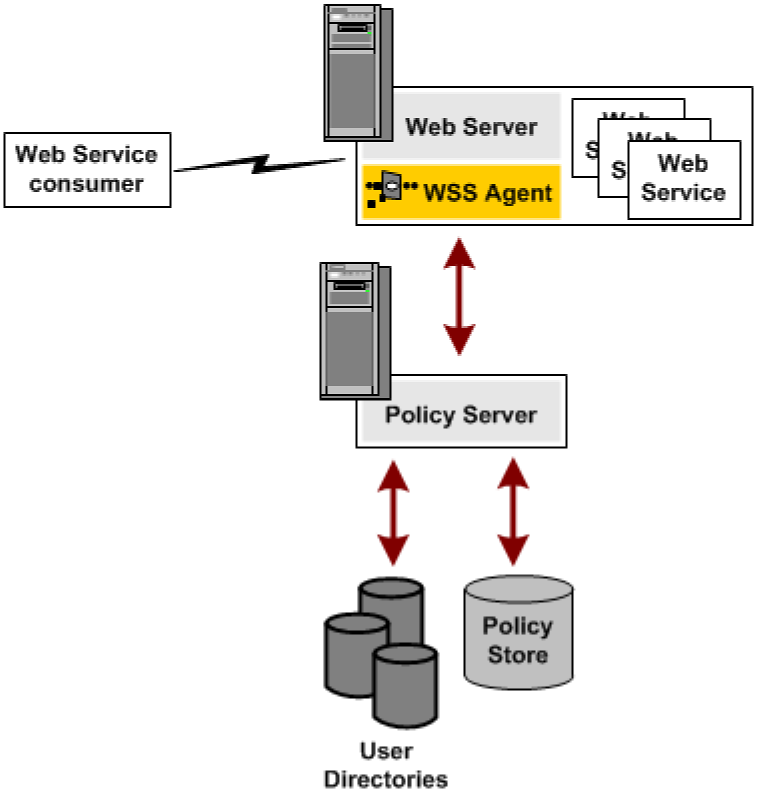
The SiteMinder WSS Agent intercepts XML messages posted to a web server and checks with the Policy Server to see if the requested resource is protected. If the resource is unprotected, the access request proceeds directly to the web server. If the resource is protected, the following occurs:

- The SiteMinder WSS Agent checks which authentication method is required for this resource. Typical credentials are a name and password, but other credentials, such as a certificate or SAML assertion, may be required.
- The SiteMinder WSS Agent obtains credentials from the transport, header, or body of the XML message.
- The SiteMinder WSS Agent passes the credentials to the Policy Server, which determines if the credentials are sufficient for the authentication method.
- If the posted XML message passes the authentication phase, the Policy Server determines if the message is authorized to access the resource. If a policy uses policy expressions as part of the authorization process, the SiteMinder WSS Agent may need to resolve the variables used in these expressions if the Policy Server cannot resolve them.
- Once the Policy Server grants access, the SiteMinder WSS Agent allows the access request to proceed to the Web service.

The SiteMinder WSS Agent can also receive message-specific attributes, in the form of *responses,* to be passed on to the Web service. A response is a personalized message or other message-specific information returned to the SiteMinder WSS Agent from the Policy Server after authorizing the message. A response consists of name-value attribute pairs that instruct the SiteMinder WSS Agent to generate SAML Session Tickets and WS-Security tokens.

SiteMinder WSS Agent Support for Web Servers

To protect Web services hosted on a web server, you deploy a SiteMinder WSS Agent on that web server (as shown in the following illustration). You then configure authentication and authorization policies for the web service resources hosted on that web server.



For a list of Web server platforms on which the SiteMinder WSS Agent is supported, see the CA SiteMinder® Web Services Security Platform Support matrix on the Technical Support site at http://ca.com/support.

Chapter 2: 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

Computers hosting CA SiteMinder® agents require the following hardware:

Windows operating environment requirements

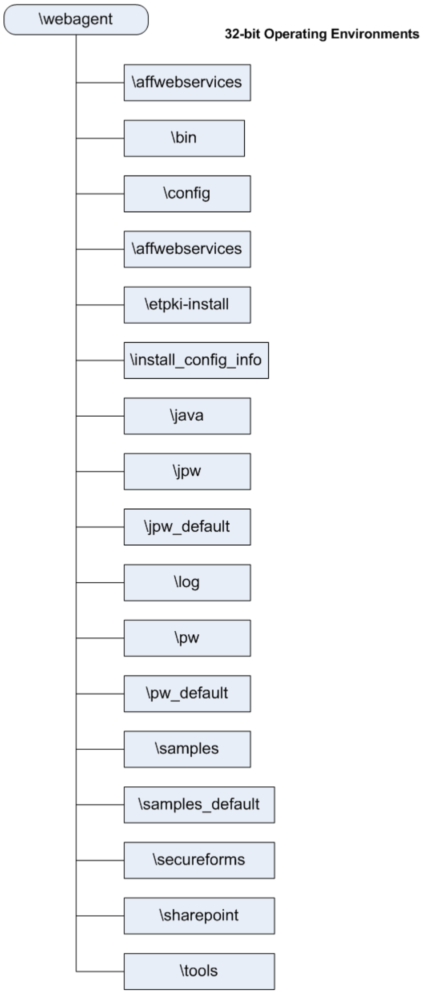
CA SiteMinder® agents operating on Windows operating environments require the following hardware:

- 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.

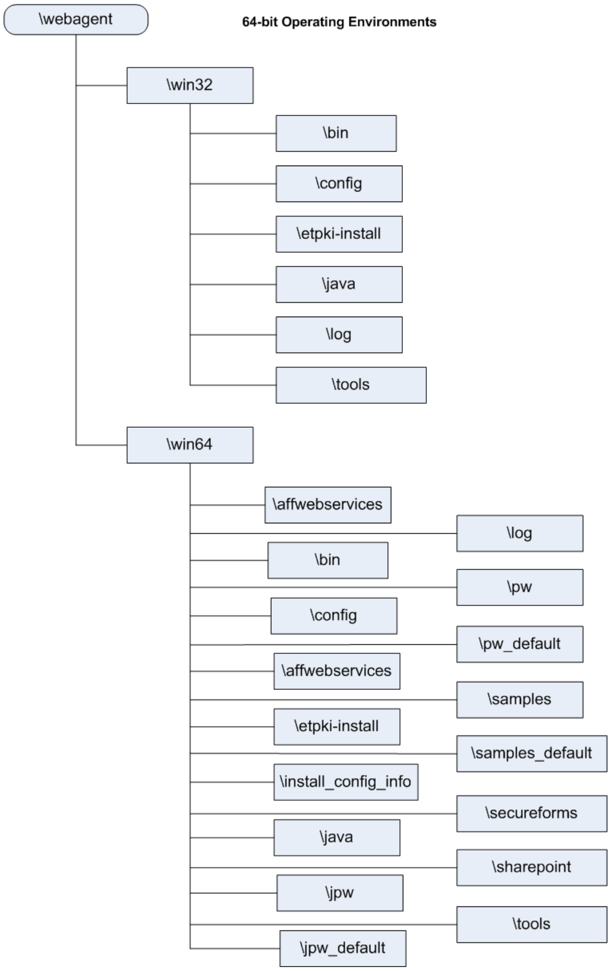
Multiple Agent for IIS Directory Structures According to Operating Environment

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:

- CA SiteMinder® Web Agents and SiteMinder WSS 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:



How to Prepare for a WSS Agent for IIS Installation on Your Web Server

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

1. Set the JRE in the Path variable (see page 16).
2. Verify that you have an account with Administrative privileges for the computer on which you want to install the agent.
3. Verify that the IIS role, the related role services and features are installed on your Windows operating environment (see page 17).
4. Locate the CA SiteMinder® Platform Support Matrix (see page 18). Confirm that your IIS web server meets the requirements for the agent version you want to install.
5. Verify that the Windows operating environment for your IIS web server has the proper service packs and updates installed (see page 18).
6. For 64-bit Windows operating environments, verify that the Microsoft C++ redistributable package is installed (see page 18).
7. Confirm that your Policy Server has the prerequisites for an agent Installation (see page 19).
8. Review the *CA SiteMinder® Web Services Security Release Notes* for known issues (see page 20).

Set the JRE in the Path Variable

Set the Java Runtime Environment (JRE) in the Windows path variable.

Follow these steps:

1. Open the Windows Control Panel.
2. Double-click System.
3. Add the location of the JRE to the Path system variable in the Environment Variables dialog.

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

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

On Windows 2008 systems, do one of the following actions to install or configure a SiteMinder WSS Agent:

- 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 WSS Agents on Windows 2008 systems, see the CA SiteMinder® Web Services Security Release Notes.

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

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

Follow these steps:

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

   The Server Manager appears.

2. Verify that IIS appears in the Roles list.

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

   - ASP.NET
   - CGI
   - ISAPI Extensions
   - ISAPI Filters
   - IIS Management Console
   - Windows Authentication (for the 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. Log in to the CA Support site.
2. Locate the Technical Support section.
3. Enter CA SiteMinder® in the Product Finder field.

   The CA SiteMinder® product page appears.
4. Click Product Status, CA 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 CA SiteMinder® Agent for IIS.

Verify that the Microsoft Visual C++ 2005 Redistributable Package (x64) is Installed

Before installing an 12.52 CA SiteMinder® Agent on a Windows 64-bit platform, download and install the Microsoft Visual C++ 2005 Redistributable Package (x64). Go to the Microsoft downloads page, and then search for "Microsoft Visual C++ 2005 Redistributable Package (x64)."

Review the Policy Server Prerequisites for Agent for IIS Installations

Your CA SiteMinder® 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 CA 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.

CA SiteMinder® 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 CA SiteMinder® Web Services Security Release Notes for Known Issues

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

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

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

7. Click Release Notes.

   A list of release notes appears.

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

   ■ View HTML

   ■ Download PDF

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

Chapter 3: 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.

Apply the Unlimited Cryptography Patch to the JRE

Patch the Java Runtime Environment (JRE) used by the Agent to support unlimited key strength in the Java Cryptography Extension (JCE) package. The patches for all supported platforms are available from the Oracle website.

The files that need to be patched are:

- local_policy.jar
- US_export_policy.jar

The local_policy.jar and US_export_policy.jar files can found be in the following locations:

- Windows

  jre_home\lib\security

- UNIX

  jre_home/lib/security

jre_home

Defines the location of your Java Runtime Environment installation.

Configure the JVM to Use the JSafeJCE Security Provider

The SiteMinder WSS Agent XML encryption function requires that the JVM is configured to use the JSafeJCE security provider.

Follow these steps:

1. Add a security provider entry for JSafeJCE (com.rsa.jsafe.provider.JsafeJCE) to the java.security file located in the following location:

   - *JVM_HOME*\jre\lib\security (Windows)
   - *JVM_HOME*/jre/lib/security (UNIX)

   JVM_HOME

   Is the installed location of the JVM used by the application server.

In the following example, the JSafeJCE security provider entry has been added as the second security provider:

```
security.provider.1=sun.security.provider.Sun
security.provider.2=com.rsa.jsafe.provider.JsafeJCE
security.provider.3=sun.security.rsa.SunRsaSign
security.provider.4=com.sun.net.ssl.internal.ssl.Provider
security.provider.5=com.sun.crypto.provider.SunJCE
security.provider.6=sun.security.jgss.SunProvider
security.provider.7=com.sun.security.sasl.Provider
```

Note: If using the IBM JRE, always configure the JSafeJCE security provider immediately after (that is with a security provider number one higher than) the IBMJCE security provider (com.ibm.crypto.provider.IBMJCE)

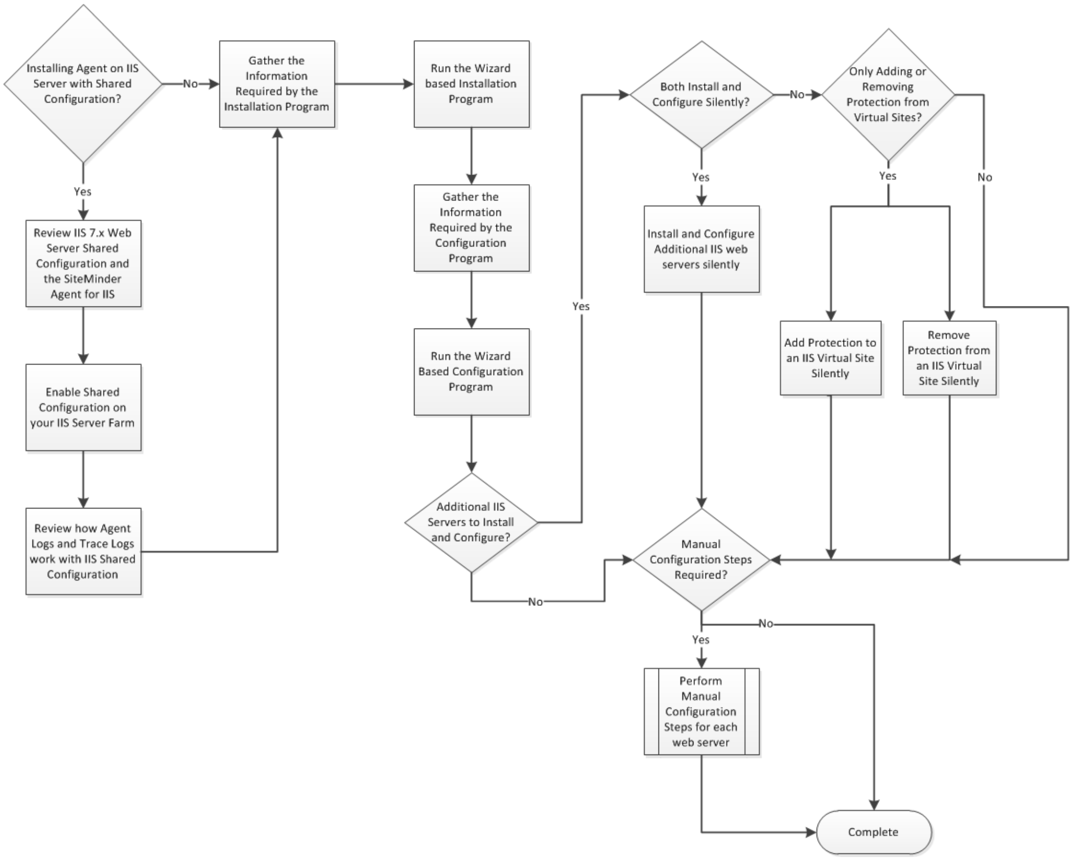
2. Add the following line to *JVM_HOME*\jre\lib\security\java.security (Windows) or *JVM_HOME/*jre/lib/security/java.security (UNIX) to set the *initial* FIPS mode of the JsafeJCE security provider:

   ```
   com.rsa.cryptoj.fips140initialmode=NON_FIPS140_MODE
   ```

   Note: The initial FIPS mode does not affect the final FIPS mode you select for the SiteMinder WSS Agent.

Agent for IIS Installation and Configuration Roadmap

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


Installing Agent on IIS Server with Shared Configuration?
No
Yes
Gather the Information Required by the Installation Program
Run the Wizard based Installation Program
Review IIS 7.x Web Server Shared Configuration and the SiteMinder Agent for IIS
Enable Shared Configuration on your IIS Server Farm
Review how Agent Logs and Trace Logs work with IIS Shared Configuration
Gather the Information Required by the Configuration Program
Run the Wizard Based Configuration Program
Additional IIS Servers to Install and Configure?
Yes
No
Both Install and Configure Silently?
Yes
No
Install and Configure Additional IIS web servers silently
Only Adding or Removing Protection from Virtual Sites?
Yes
No
Add Protection to an IIS Virtual Site Silently
Remove Protection from an IIS Virtual Site Silently
Manual Configuration Steps Required?
Yes
No
Perform Manual Configuration Steps for each web server
Complete

How to Install and Configure a SiteMinder WSS Agent for IIS

Installing and configuring the SiteMinder WSS 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 27).
   - How web agent logs and trace logs work with shared configuration (see page 29).
2. Gather the information for the installation program (see page 31).
3. Gather the information for the configuration program (see page 31).
4. Run the CA SiteMinder® Web Services Security installation program (see page 35).
5. Run the wizard based configuration program (see page 37).
6. (Optional) Install and configure additional Agents for IIS silently (see page 38).
7. (Optional) Add (see page 39) or remove (see page 42) CA SiteMinder® Web Services Security protection from virtual sites on IIS web servers silently.
8. Determine if your Agent for IIS requires any manual configuration steps (see page 46).

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

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

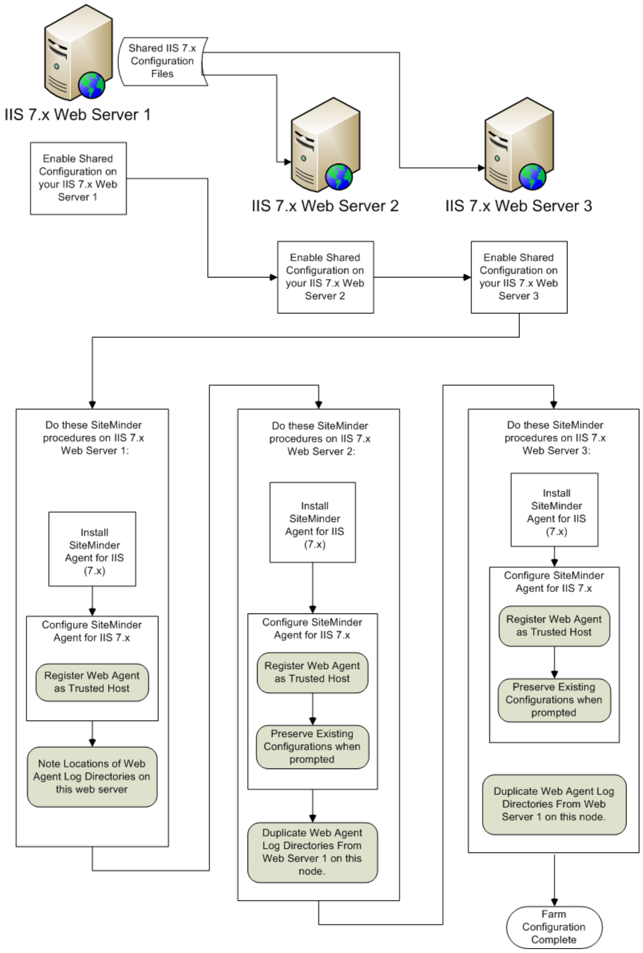
Starting with CA SiteMinder® 12.52, the Agent for IIS can protect resources on IIS server farms that use the shared configuration feature of IIS 7.x.

Note: This feature works *only* with the CA SiteMinder® 12.52 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 Agent for IIS, however, *cannot* operate on network shares. Using a CA SiteMinder® 12.52 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:


Shared IIS 7.x Configuration Files
IIS 7.x Web Server 1
IIS 7.x Web Server 2
IIS 7.x Web Server 3
Enable Shared Configuration on your IIS 7.x Web Server 1
Enable Shared Configuration on your IIS 7.x Web Server 2
Enable Shared Configuration on your IIS 7.x Web Server 3
Do these SiteMinder procedures on IIS 7.x Web Server 1:
Install SiteMinder Agent for IIS (7.x)
Configure SiteMinder Agent for IIS 7.x
Register Web Agent as Trusted Host
Note Locations of Web Agent Log Directories on this web server
Do these SiteMinder procedures on IIS 7.x Web Server 2:
Install SiteMinder Agent for IIS (7.x)
Configure SiteMinder Agent for IIS 7.x
Register Web Agent as Trusted Host
Preserve Existing Configurations when prompted
Duplicate Web Agent Log Directories From Web Server 1 on this node.
Do these SiteMinder procedures on IIS 7.x Web Server 3:
Install SiteMinder Agent for IIS (7.x)
Configure SiteMinder Agent for IIS 7.x
Register Web Agent as Trusted Host
Preserve Existing Configurations when prompted
Duplicate Web Agent Log Directories From Web Server 1 on this node.
Farm Configuration Complete

How SiteMinder WSS Agent Logs and Trace Logs Work with IIS 7.x Web Server Shared Configuration

For SiteMinder WSS 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 WSS 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 default setting:

  `agent_home\log`

  agent_home

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

  Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

  Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

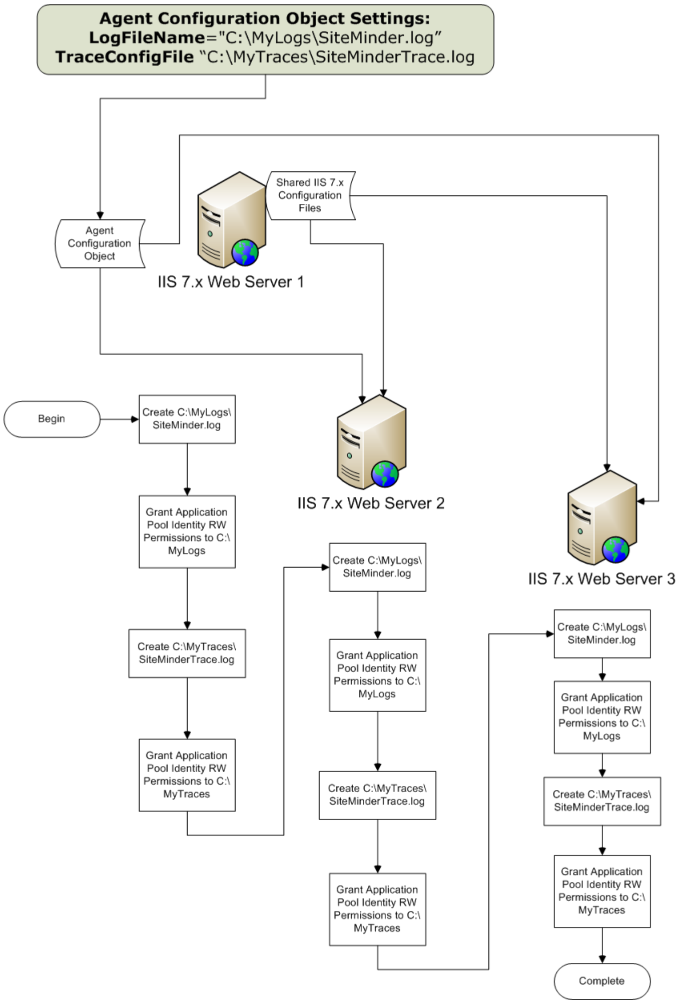
  Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

If all of the previous conditions exist in your server farm, use the following process to enable your SiteMinder WSS 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:


Agent Configuration Object Settings:
LogFileName="C:\MyLogs\SiteMinder.log"
TraceConfigFile "C:\MyTraces\SiteMinderTrace.log
Agent Configuration Object
Shared IIS 7.x Configuration Files
IIS 7.x Web Server 1
Begin
Create C:\MyLogs\SiteMinder.log
Grant Application Pool Identity RW Permissions to C:\MyLogs
Create C:\MyTraces\SiteMinderTrace.log
Grant Application Pool Identity RW Permissions to C:\MyTraces
IIS 7.x Web Server 2
Create C:\MyLogs\SiteMinder.log
Grant Application Pool Identity RW Permissions to C:\MyLogs
Create C:\MyTraces\SiteMinderTrace.log
Grant Application Pool Identity RW Permissions to C:\MyTraces
IIS 7.x Web Server 3
Create C:\MyLogs\SiteMinder.log
Grant Application Pool Identity RW Permissions to C:\MyLogs
Create C:\MyTraces\SiteMinderTrace.log
Grant Application Pool Identity RW Permissions to C:\MyTraces
Complete

Gather the Information for the Agent Installation Program for the Windows Operating Environment

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.

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

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

Host Registration

Indicates whether you want to register this agent as a trusted host with a CA SiteMinder® 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. For more information, see the *Policy Server Administration Guide*.

FIPS Mode Setting

Specifies *one* of the following algorithms:

FIPS Compatibility/AES Compatibility

Uses algorithms existing in previous versions of 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) *agent_home*\win32\bin\IIS

Default: (Windows IIS 7.x 64-bit) *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®.

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 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

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

Agent Configuration Object Name

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

Default: AgentObj

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

More information:

CA SiteMinder® Agent Configuration Worksheet for IIS Web Servers (see page 103)

Run the Installer to Install a SiteMinder WSS Agent

Install the SiteMinder WSS Agent using the CA SiteMinder® Web Services Security installation media on the Technical Support site.

Follow these steps:

1. Exit all applications that are running.
2. Navigate to the installation material.
3. Double-click ca-sm-wss-12.52-*cr*-win32.exe.

   cr

   Specifies the cumulative release number. The base 12.52 release does not include a cumulative release number.

   The CA SiteMinder® Web Services Security installation wizard starts.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the CA SiteMinder® Web Services Security Release Notes.

4. Use gathered system and component information to install the SiteMinder WSS Agent. Consider the following points when running the installer:

   - When prompted to select which CA SiteMinder® Web Services Security Agents to install, select **CA SiteMinder® Web Services Security Agent for Web Servers**.
   - When prompted to select the Java version, the installer lists all Java executables present on the system. Select a supported 32-bit Java Runtime Environment (refer to the Platform Support Matrix on the Technical Support site).
   - If you enter path information in the wizard by cutting and pasting, enter (and delete, if necessary) at least one character to enable the Next button.
   - If the installer detects the presence of an existing CA SiteMinder® Web Agent, it displays a warning dialog stating that the install will upgrade the Web Agent. Click Continue to upgrade the Web Agent to a SiteMinder WSS Agent. If you proceed, the software upgrade occurs in the installed location of the existing Web Agent.

5. Review the information that is presented on the Pre-Installation Summary page, then click Install.

   Note: If the installation program detects that newer versions of certain system DLLs are installed on your system, it asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The SiteMinder WSS Agent files are copied to the specified location.

6. On the CA SiteMinder® Web Services Security Configuration screen, click one of the following options and click Next:

   - Yes. I would like to configure CA SiteMinder® Web Services Security Agents now.
   - No. I will configure CA SiteMinder® Web Services Security Agents later.

   If the installation program detects that there are locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system automatically or later on your own.

   Important! For SiteMinder WSS Agents for Web Servers installed on IIS servers, reboot your system after installation; it is not sufficient to restart the IIS service. Also, do not configure the Agent immediately after installation; there are some tasks you must do before configuring the Agent.

7. Click Done.

   If you selected the option to configure SiteMinder WSS Agents now, the installation program prepares the CA SiteMinder® Web Services Security Configuration Wizard and begins the trusted host registration and configuration process. Use the information that you gathered earlier to complete the wizard.

   If you did not select the option to configure SiteMinder WSS Agents now, or if you are required to reboot the system after installation, run the configuration wizard manually later.

Installation Notes:

- After installation, you can review the installation log file in *WSS_HOME*\install_config_info. The file name is: CA_SiteMinder_Web_Services_Security_Install_*install-date-and-time*.log

  WSS_Home

  Specifies the path to where CA SiteMinder® Web Services Security is installed.

  Default: C:\Program Files\CA\Web Services Security

  install-date-and-time

  Specifies the date and time that the SiteMinder WSS Agent was installed.

  The Agent cannot communicate properly with the Policy Server until the trusted host is registered.

More information:

Gather the Information for the Agent Installation Program for the Windows Operating Environment (see page 31)

Run the WSS 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. Open the following directory on your web server:

   WSS_Home\install_config_info

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

2. Right-click ca-pep-config.exe, 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 WSS Agent Configuration wizard starts.

3. Use the information you gathered earlier to complete the wizard.

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

The unattended or silent installation option can help you automate the installation and configuration process. This method saves time if you have a large CA SiteMinder® Web Services Security 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 Services Security Installation wizard.
   b. The CA SiteMinder® Web Services Security Configuration wizard.
2. Locate the following file on your first IIS web server:

   ```
   WSS_home\install_config_info\ca-wss-installer.properties
   ```

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

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

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

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

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

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

      - The SiteMinder WSS Agent Installation executable file.
      - The ca-pepconfig-installer.properties file.

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

   d. Run the following command:

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

      The SiteMinder WSS 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-wss-installer.properties file specify.

Add CA SiteMinder® Web Services Security Protection to Additional Virtual Sites on IIS Web Servers Silently

If your IIS web server already has a SiteMinder WSS 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 web services on them with CA SiteMinder® Web Services Security.

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 Services Security 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.

   `WSS_Home\install_config_info\ca-wss-installer.properties`

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

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.

   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.

   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 WSS Agent configuration executable file (ca-pep-config.exe).
      - SiteMinder WSS Agent ca-wss-installer.properties file.

   c. Open the ca-wss-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-wss-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.

i. **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.

j. Run the following command:

```
ca-pep-config.exe -f ca-wss-installer.properties -i silent
```

   The SiteMinder WSS 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 ca-wss-installer.properties file.

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

To remove the CA SiteMinder® Web Services Security protection from all the websites on an IIS web server without using the CA SiteMinder® Web Services Security 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.

   WSS_Home\install_config_info\ca-wa-installer.properties

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

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.

   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.

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

      WSS_Home\install_config_info

   b. Copy the ca-wss-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-wss-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® Web Services Security 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 WSS Agent configuration from a website leaves its resources *unprotected*.

      For more information, see the comments in the ca-soasm-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-wss-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:

```
ca-pep-config.exe -f properties_file -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 ca-wss-installer.properties file.

Remove CA SiteMinder® Web Services Security Protection From Some Virtual Sites on IIS Web Servers Silently

If your IIS web server already has a SiteMinder WSS 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-wss-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 Services Security 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.

   `*WSS_Home*\install_config_info\ca-wa-installer.properties`

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

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.

   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.

   a. Copy the ca-wss-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-wss-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® Web Services Security 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 WSS Agent configuration from a website leaves its resources *unprotected*.

      For more information, see the comments in the ca-soasm-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.

h. **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:

```
ca-pep-config.exe -f ca-wss-installer.properties -i silent
```

The CA SiteMinder® Web Services Security 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 ca-wss-installer.properties file.

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

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

Configure the SiteMinder WSS 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 (see page 47):

  WSS_agent_home\log

  agent_home

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

  Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

  Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

  Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\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 CA SiteMinder® Web Services Security authentication scheme which requests or requires client certificates (see page 48).

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".

To set permissions manually for non default log locations

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.

   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 CA SiteMinder® Web Services Security Authentication Schemes Requiring Certificates

If you use CA SiteMinder® Web Services Security authentication schemes that request or require certificates, change the settings for the following virtual directories:

- cert
- certoptional

Follow these steps:

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 that is associated with your authentication scheme that requires certificates.

   The siteminderagent virtual folder appears.
6. Expand the siteminderagent virtual folder.

   A list of subfolders appears.
7. Click the cert folder.

   The settings icons appear.
8. Double-click SSL Settings.

   The SSL Settings page appears.
9. Select the Require SSL check box, and then click the Require option button.
10. Under Actions, click Apply.

    The changes are applied.
11. Click the certoptional folder.

    The settings icons appear.
12. Double-click SSL Settings.

    The SSL Settings page appears.
13. Click the Accept option button.

14. Under Actions, click Apply.

    The changes are applied.

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

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

    The settings are changed.

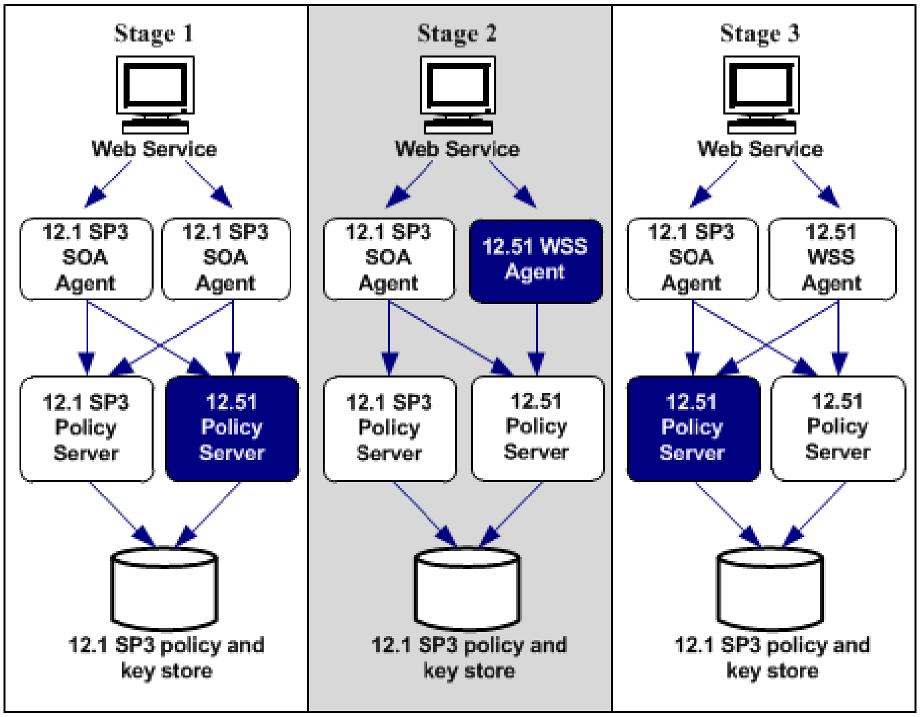
Chapter 4: Upgrade a SOA Agent to a 12.52 WSS Agent

This section contains the following topics:

How to Upgrade a SOA Agent

Upgrading a SOA Agent to a 12.52 WSS Agent involves several separate procedures. To upgrade your agent, Follow these steps::

1. Verify that you are in the proper step of the upgrade process for an agent upgrade. You upgrade to 12.52 from r12.1 SP3 at stage two of the CA SiteMinder® Web Services Security upgrade process, as shown in the following illustration:



2. Create backup copies of any customized agent-related 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
3. Gather information for the following CA SiteMinder® programs.
   - Agent installation wizard.
   - Agent configuration wizard.
4. Run the installation wizard to upgrade your agent (see page 53).
5. Run the configuration wizard to configure the upgraded agent (see page 54).

Run the Installation Wizard to Upgrade your Agent for Web Servers

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

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

Follow these steps:

1. Copy the SiteMinder WSS 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
     ```

     Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the CA SiteMinder® Web Services Security Release Notes.

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

Note: The software upgrade occurs in the installed location of the existing SOA Agent.

More information:

Multiple Agent for IIS Directory Structures According to Operating Environment (see page 14)

Run the Configuration Wizard on your Upgraded SiteMinder WSS Agent

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 Web Servers on your 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. Open the following directory on your web server:

   ```
   WSS_Home\install_config_info
   ```

   WSS_Home

   Specifies the path to where CA SiteMinder® Web Services Security is installed.

   Default: C:\Program Files\CA\Web Services Security

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, even if you are logged into the system as an Administrator. For more information, see the CA SiteMinder® Web Services Security Release Notes.

   The agent configuration wizard starts.

3. Complete the wizard.

Chapter 5: Advanced Configuration

This section contains the following topics:

SiteMinder WSS Agent Configuration Parameters

The following table lists configuration parameters for the SiteMinder WSS Agent.

Parameter Name	Value	Description
IgnoreXMLSDK	yes or no	If this parameter is added to the Agent Configuration Object and is set to Yes, the SiteMinder WSS Agent is disabled. This means that the Agent behaves as a Web Agent for all incoming requests. If added to the Agent Configuration Object and set to No (or not added to to the Agent Configuration Object at all), the SiteMinder WSS Agent is enabled. That is, the Agent uses the XML SDK to process incoming HTTP requests under these conditions: ■ HTTP action is POST ■ HTTP MIME type is “text/xml” or, if the XMLSDKMimeTypes parameter is configured, any one of the MIME types specified by that parameter. ■ HTTP content is an XML document

Parameter Name	Value	Description
XMLSDKMimeTypes	String	A comma-delimited list of MIME types that the SiteMinder WSS Agent will accept for processing by CA SiteMinder® Web Services Security. All POSTed requests having one of the listed MIME types are processed. Examples: ■ text/xml ■ application/octet-stream ■ text/xml,multipart/related If you do not add this parameter to the Agent Configuration Object, the SiteMinder WSS Agent defaults to accepting only the text/xml MIME type.
ServerProductName	String	Description of the product name—for example, iPlanet Web Server. Provides a value for the SiteMinder WSS Agent variable property Server Product Name. **Note:** For more information about setting this variable, see the *CA SiteMinder® Web Services Security Policy Configuration Guide*.
ServerVendor	String	Description of the Web Server vendor—for example, Sun. Provides a value for the SiteMinder WSS Agent Variable property Server Vendor. **Note:** For more information about setting this variable, see the *CA SiteMinder® Web Services Security Policy Configuration Guide*.
ServerVersion	String	Description of the product version—for example, 6.0 SP2). Provides a value for the SiteMinder WSS Agent Variable property Server Version. **Note:** For more information about setting this variable, see the *CA SiteMinder® Web Services Security Policy Configuration Guide*.

Parameter Name	Value	Description
MaxXmlSdkRetries	Number	Defines the number of times the SiteMinder WSS Agent tries to contact the XML SDK server when it receives requests. The default is 3. The Agent does not continually retry the server for the same request. If a request comes in and the Agent cannot contact the SDK server, that request is dropped and the Agent tries again when a subsequent request is made. The Agent attempts to connect for each new request until it reaches the number specified in this parameter. If the SiteMinder WSS Agent does not connect to the XML SDK server, the Agent assumes the server is not running and stops trying to process CA SiteMinder® Web Services Security-specific requests. **Note:** For the SiteMinder WSS Agent on Apache Web servers, this value applies to each process.
XMLSDKResourceIdentification	yes or no	Determines if the SiteMinder WSS Agent should identify the web service operation being requested by an incoming XML message as well as the resource identifier (that is, perform fine-grain resource identification). The default is No. **Note:** You must set this option to Yes if you want to use the Administrative UI to configure policies to protect resources with the SiteMinder WSS Agent.
XMLSDKAcceptSMSessionCookie	yes or no	Determines whether or not the SiteMinder WSS Agent accepts an CA SiteMinder session cookie to authenticate a client. The default is no. If set to yes, the SiteMinder WSS Agent uses information in a session cookie sent as an HTTP header in the request as a means of authenticating the client. If set to no, session cookies are ignored and the SiteMinder WSS Agent requests credentials required by the configured authentication scheme.

Parameter Name	Value	Description
SAMLSessionTicketLogoffi	yes or no	Determines whether the SiteMinder WSS Agent should attempt to log off session tickets in SAML assertions. The default is yes.
XMLAgentSoapFaultDetails	yes or no	Determines whether or not the SiteMinder WSS Agent should insert the authentication/authorization rejection reason (if provided by the Policy Server) into the SOAP fault response sent to the Web service consumer. The default is no.

Configure a SiteMinder WSS Agent to Enable Fine-Grain Resource Identification

By default, the SiteMinder WSS Agent identifies incoming requests for web service resources as follows:

[*URL*][*Web Service Name*]

However, the SiteMinder WSS Agent can be configured to provide fine-grain resource identification, additionally identifying the requested web service operation name, so that requests are identified as:

[*URL*][*Web Service Name*][*Web Service Operation*]

This allows you to define fine-grain policies that include the web service operation in authorization decisions, but may adversely affect transaction performance.

Note: For more information on configuring fine-grain authorization policies, see the *CA SiteMinder® Web Services Security Policy Configuration Guide*.

Follow these steps:

1. Ensure that the XMLSDKResourceIdentification Agent configuration parameter is present and set to Yes for the target SiteMinder WSS Agent.
2. Edit the XmlToolkit.properties file located in *agent_home*\java to ensure that the WSDMResourceIdentification entry is present and set to "Yes".

3. Save and close the XmlToolkit.properties file.
4. Restart the target SiteMinder WSS Agent.

Note: You must enable fine-grain resource identification to use the Administrative UI to generate policies for web service resources protected by the SiteMinder WSS Agent from their associated WSDL files.

Configure the Username and Password Digest Token Age Restriction

By default, the WS-Security authentication scheme imposes a 60-minute restriction on the age of Username and Password Digest Tokens to protect against replay attacks.

To configure a different value for the token age restriction for a SiteMinder WSS Agent for Web Servers, add the WS_UT_CREATION_EXPIRATION_MINUTES parameter to the XmlToolkit.properties file for that agent.

Follow these steps:

1. Navigate to a*gent_home*\java*.*
2. Open XmlToolkit.properties in a text editor.
3. Add the following line:

   ```
   WS_UT_CREATION_EXPIRATION_MINUTES=token_age_limit
   ```

   token_age_limit

   Specifies the token age limit restriction in minutes.
4. Save and close the XmlToolkit.properties file.
5. Restart the SiteMinder WSS Agent.

Configure the SiteMinder WSS Agent to Process Large XML Messages

By default, the SiteMinder WSS Agent can process XML messages up to 2000 KB in size. However, if you need to process larger files, you can increase this size limit by editing the conapi.conf file on each system hosting a SiteMinder WSS Agent.

The conapi.conf is located in:

- *agent_home*\config (Windows)
- *agent_home*/config (UNIX)

agent_home

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

Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

To increase the maximum message size, uncomment the nete.conapi.service.xmlsdk.maxpacketsize entry and change its value to the maximum message size (in KB) you want the SiteMinder WSS Agent to be able to process. For example:

```
nete.conapi.service.xmlsdk.maxpacketsize=3000
```

Note: Web servers also have incoming file size limits. When planning your Web service implementations, you should ensure that you are aware of these and bear them in mind.

Chapter 6: 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 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 SiteMinder WSS Agent to a Dynamic Policy Server Cluster

You can connect a SiteMinder WSS 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:

   `agent_home\config\SmHost.conf`

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

2. Do *one* of the following tasks:

   - If this 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 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 agent is connected to dynamic Policy Server clusters.

Chapter 7: Starting and Stopping SiteMinder WSS Agents

This section contains the following topics:

Enable a SiteMinder WSS 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 following file with a text editor:

   agent_home`\bin\IIS\WebAgent.conf`

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

   Note: CA SiteMinder® 12.52 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 CA 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 SiteMinder WSS Agent is enabled.

Disable a SiteMinder WSS Agent

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

Follow these steps:

1. Open the following file with a text editor:

   `agent_home\bin\IIS\WebAgent.conf`

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

   Note: CA SiteMinder® 12.52 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 CA 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 SiteMinder WSS Agent is disabled.

Start and Stop SiteMinder WSS Agent Processing

The CA SiteMinder® Web Services Security XML SDK server is a process that must be running so the SiteMinder WSS Agent can process requests. The XML SDK Server is started automatically at system startup. This section describes how to start and stop it manually.

Note: Do not confuse the XML SDK server with the CA SiteMinder® Web Services Security SDK, which is an API that communicates with the XML SDK server.

Start the CA SiteMinder® Web Services Security XML SDK Server

The CA SiteMinder® Web Services Security XML SDK server process must be running for the SiteMinder WSS Agent to process requests.

To start the CA SiteMinder® Web Services Security XML SDK server on Windows

1. Open the Services dialog.
2. Right-click the TxMinder XML SDK Service entry and then click Start in the menu that opens.

To start the CA SiteMinder® Web Services Security XML SDK server on UNIX

1. Open a command window.
2. Navigate to *agent_home.*

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

3. Enter the following command:

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

4. Navigate to *agent_home*/bin
5. Enter the following command:

   ```
   tmxmlsdkserver -start
   ```

Stop the CA SiteMinder® Web Services Security XML SDK Server

The CA SiteMinder® Web Services Security XML SDK server process must be running for the SiteMinder WSS Agent to process requests.

To stop the CA SiteMinder® Web Services Security XML SDK server on Windows

1. Open the Services dialog.
2. Right-click TxMinder XML SDK Service entry and then click Stop in the menu that opens.

To stop the CA SiteMinder® Web Services Security XML SDK server on UNIX

1. Open a command window.
2. Navigate to *agent_home.*

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32
3. Enter the following command:

   ```
   . ./ca_wa_env.sh
   ```
4. Navigate to *agent_home*/bin
5. Enter the following command:

   ```
   tmxmlsdkserver -stop
   ```

Chapter 8: Uninstall a SiteMinder WSS Agent

This section contains the following topics:

Set JRE in PATH Variable Before Uninstalling the CA SiteMinder® Agent

On Windows and UNIX systems, when you are uninstalling a CA 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 SiteMinder WSS Agent

To uninstall a SiteMinder WSS Agent, run the CA SiteMinder® Web Services Security uninstall wizard.

Follow these steps:

1. Navigate to the WSS_*HOME*\install_config_info (Windows) or WSS_*HOME*/install_config_info (UNIX) directory and run the CA SiteMinder® Web Services Security uninstall wizard to remove core CA SiteMinder® Web Services Security components:

   - Windows: wss-uninstall.cmd
   - UNIX: wss-uninstall.sh

   WSS_HOME

   Specifies the CA SiteMinder® Web Services Security installation location.

   Important! If you are running this wizard on Windows Server 2008, run the executable file with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the CA SiteMinder® Web Services Security Release Notes.

   The uninstall wizard starts.

2. Choose whether you want to perform a complete uninstall or whether to uninstall specific features and proceed.

3. If you chose to uninstall only specific features, select the installed components that you want to uninstall and proceed.

   The uninstall wizard removes all selected CA SiteMinder® Web Services Security components.

4. Restart the server.

Chapter 9: SiteMinder WSS Agent Logging

This section contains the following topics:

Logs of Start-up Events

To assist in debugging, startup events are recorded in a log. Each message may provide clues about the problem. These logs are stored in the following locations:

- On Windows systems, these events are recorded in the Windows Application Event log.
- On UNIX systems, these events are sent to STDERR. Apache servers map STDERR to the Apache error_log file, so these events are also recorded in that log.

Error Logs and Trace Logs

You can use the Web Agent logging function to monitor the performance of the Web Agent and its communication with the Policy Server. The logging feature provides accurate and comprehensive information about the operation of CA SiteMinder® processes to analyze performance and troubleshoot issues.

A log is a record of events that occur during program execution. A log consists of a series of log messages, each one describing some event that occurred during program execution. Log messages are written to log files.

Note: IIS Agents create log files only after the first user request is submitted. Apache 2.0 Web Agents create log files when the Apache server starts.

The Web Agent uses the following log files:

Error log

Contains program and operational-level errors. One example is when the Web Agent cannot communicate with Policy Server. The level of detail output in this log cannot be customized. Error logs contain the following types of messages:

Error messages

Contain program-level errors, which indicate incorrect or abnormal program behavior, or an inability to function as expected due to some external problem, such as a network failure. There are also operational-level errors. This type of error is a failure that prevents the operation from succeeding, such as opening a file or authenticating a user.

Informational messages

Contain messages for the user or administrator that some event has occurred; that is, that a server has started or stopped, or that some action has been taken.

Warning messages

Contain warnings for the user or administrator of some condition or event that is unusual or indicative of a potential problem. This does not necessarily mean there is anything wrong.

Trace log

Contains detailed warning and informational messages, which you can configure. Examples include trace messages and flow state messages. This file also includes data such as header details and cookie variables. Trace logs contain the following messages:

Trace messages

Provide detailed information about program operation for tracing and/or debugging purposes. Trace messages are ordinarily turned off during normal operation. In contrast to informational, warning, and error messages, trace messages are embedded in the source code and can not easily be localized. Moreover, trace messages may include significant data in addition to the message itself; for example, the name of the current user or realm.

You specify the location of both the error and trace log files when you configure the Web Agent. Use the error and trace logs to help solve any issues that may prevent the Web Agent from operating properly.

Note: For Agents on Windows platforms, set the EnableWebAgent parameter to yes to ensure that the Web Agent log gets created. If you leave EnableWebAgent set to no (the default) and set the logging parameters, the Agent log gets created only for Agents on UNIX platforms.

Parameter Values Shown in Log Files

Web Agents list configuration parameters and their values in the Web Agent error log file, but there are differences between the ways that Traditional and Framework agents do this.

Framework agents record the configuration parameters and their values in the log file exactly as you entered them in the Agent Configuration Object or the local configuration file. All of the parameters, including those which may contain an incorrect value, are recorded in the log file.

Traditional agents process the parameter values before recording them. If the parameter has a proper value, the parameter and its value are recorded in the log file. Parameters with incorrect values are *not* recorded in the log file.

Set Up and Enable Error Logging

Error logs require the following settings:

- Logging is enabled.
- A location for the log file is specified.

The parameters that enable error logging and determine options such as appending log data are defined in a local configuration file or an Agent Configuration Object at the Policy Server.

Agents that are installed on an IIS or Apache web servers do not support dynamic configuration of log parameters that are set locally in a local configuration file. The changes take effect when the Agent is restarts. However, these log settings can be stored and updated dynamically in an agent configuration object at the Policy Server.

Note: IIS Agents create log files only after the first user request is submitted. Apache 2.0 Web Agents create log files when the Apache server starts.

Follow these steps:

1. If you do not have a log file already, create a log file and any related directories.
2. Set the value of the LogFile parameter to yes.

   Note: Setting the value of this parameter to yes in a local configuration file of a web server overrides any of the logging settings that are defined on the Policy Server. For example, suppose that the value of this parameter is set to yes in a LocalConfig.conf file. The agent creates log files even though the value of the AllowLocalConfig parameter in the corresponding agent configuration object is set to no. You can also set the related logging parameters in the LocalConfig.conf file also to override any other settings in the agent configuration object.
3. Specify the full path to the error file, including the file name, in any of the following parameters:

   LogFileName

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

   Default: No

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

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

   LogFileName32

   Specifies the full path of a log file for a SiteMinder WSS Agent for IIS (on 64-bit Windows operating environments protecting 32-bit applications). The 32-bit applications run in Wow64 mode on the 64-bit Windows operating environment. If logging is enabled but this parameter is not set, the SiteMinder WSS Agent for IIS appends _32 to the log file name.

   Default: No

   Limits: For Windows 64-bit operating environments only. Specify the file name at the end of the path.

   Example: (Windows 64-bit operating environments using Wow64 mode) *agent_home*\log\WebAgent32.log.
4. (Optional) Set the following parameters (in the Agent Configuration Object on the Policy Server or in the local configuration file):

   LogAppend

   Adds new log information to the end of an existing log file. When this parameter is set to no, the entire log file is rewritten each time logging is invoked.

   Default: No

LogFileSize

Specifies the size limit of the log file in megabytes. When the current log file reaches this limit, a new log file is created. The new log file uses one of the following naming conventions:

- For framework agents, the new log file has a sequence number that is appended to the original name. For example, a log file named myfile.log is renamed to myfile.log.1 when the size limit is reached.
- For traditional agents, the new log files are named by appending the date and timestamp to the original name. For example, a log file named myfile.log, is renamed to myfile.log.09-18-2003-16-07-07 when the size limit is reached.

Archive or remove the old files manually.

Default: 0 (no rollover)

Example: 80

LogLocalTime

Specifies whether the logs use Greenwich Mean Time (GMT) or local time. To use GMT, change this setting to no. If this parameter does not exist, the default setting is used.

Default: Yes

If you use a local configuration file, your settings resemble the following example:

```
LogFile="yes"
LogFileName="/export/iPlanet/servers/https-myserver/logs/errors.log"
LogAppend="no"
LogFileSize="80"
LogLocalTime="yes"
```

Error logging is enabled.

Enable Transport Layer Interface (TLI) Logging

When you want to examine the connections between the agent and the Policy Server, enable transport layer interface logging.

To enable TLI logging

1. Add the following environment variable to your web server.

   `SM_TLI_LOG_FILE`

2. Specify a directory and log file name for the value of the variable, as shown in the following example:

   `directory_name/log_file_name``.log`

3. Verify that your agent is enabled.
4. Restart your web server.

   TLI logging is enabled.

Limit the Number of Log Files Saved

You can limit the number of log files that an agent keeps. For example, if you want to save disk space on the system that stores your agent logs, you can limit the number of log files using the following parameter:

LogFilesToKeep

Specifies the number of agent log files that are kept. New log files are created in the following situations:

- When the agent starts.
- When the size limit of the log file (specified by the value of the LogFileSize parameter) is reached.

Changing the value of this parameter does *not* automatically delete any existing logs files which exceed the number that you want to keep. For example, If your system has 500 log files stored, and you decide to keep only 50 of those files, the agent does *not* delete the other 450 files.

Setting the value of this parameter to zero retains all the log files.

Default: 0

Follow these steps:

1. Archive or delete any existing log files from your system.
2. Set the value of the LogAppend parameter to no.
3. Change the value of the LogFilesToKeep parameter to the number of log files that you want to keep.

How to Set Up Trace Logging

To set up trace logging, use the following process:

1. Set up and Enable Trace logging.
2. Determine what you want to record in the trace log by reviewing the following lists:
   - Trace Log Components and Subcomponents
   - Trace Message Data Fields
   - Data Field Filters
3. Duplicate the default Trace Configuration File.
4. Modify the duplicate file to include the items you want to record.
5. Restart the agent.

Configure Trace Logging

Before you can use trace logging, you must configure it by specifying a name, location, and parameters for the trace log file. These settings control the size and format of the file itself. After trace logging is configured, you determine the content of the trace log file separately. This lets you change the types of information contained in your trace log at any time, without changing the parameters of the trace log file itself.

Follow these steps:

1. Locate the WebAgentTrace.conf file on your web server. Duplicate the file.

   Note: If you are running the CA SiteMinder® Agent for IIS and protecting 32-bit applications on a 64-bit system (WoW64 mode), create two duplicates. There are separate directories for 32 and 64-bit applications on 64-bit Windows operating environments.

2. Open your Agent Configuration Object or local configuration file.
3. Set the TraceFile parameter to yes.

   Note: Setting the value of this parameter to yes in a local configuration file of a web server overrides any of the logging settings that are defined on the Policy Server. For example, suppose that the value of this parameter is set to yes in a LocalConfig.conf file. The agent creates log files even though the value of the AllowLocalConfig parameter in the corresponding agent configuration object is set to no. You can also set the related logging parameters in the LocalConfig.conf file also to override any other settings in the agent configuration object.

4. Specify the full path to the trace log files in following parameters:

   TraceFileName

   Specifies the full path to the trace log file.

   Default: No default

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

   TraceFileName32

   Specifies the full path to the trace file for the CA SiteMinder® Agent for IIS is running on a 64-bit Windows operating environment and protecting 32-bit applications. Set this parameter if you have a CA SiteMinder® Agent for IIS installed on a 64-bit Windows operating environment and protecting a 32-bit Windows application. The 32-bit applications run in Wow64 mode on the 64-bit Windows operating environment. If trace logging is enabled but this parameter is not set, the SiteMinder WSS Agent for IIS appends _32 to the file name.

   Default: No default.

   Limits: For Windows 64-bit operating environments only. Specify the trace file name at the end of the path.

   Example: (Windows 64-bit operating environments using Wow64 mode)
   agent_home\log\WebAgentTrace32.log.

5. Specify the full path to the duplicate copies of WebAgentTrace.conf file (you created in Step 1) in the following parameters:

   TraceConfigFile

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

   Default: No default

   Example: *agent_home*\config\WebAgentTrace.conf

   TraceConfigFile32

   Specifies the location of the WebAgentTrace.conf configuration file that determines which components and events to monitor. Set this parameter if you have a SiteMinder WSS Agent for IIS installed on a 64-bit Windows operating environment and protecting a 32-bit Windows application. The 32-bit applications run in Wow64 mode on the 64-bit Windows operating environment. If logging is enabled but this parameter is not set, the SiteMinder WSS Agent appends _32 to the file name.

   Default: No default.

   Limits: For Windows 64-bit operating environments only. Specify the configuration file name at the end of the path.

   Example: (Windows 64-bit operating environments using Wow64 mode) *agent_home*\config\WebAgentTrace32.conf.

   Note: This file is not used until the web server is restarted.

6. Define the format of the information in your trace log file by setting the following parameters in your Agent Configuration Object or local configuration file:

   TraceAppend

   Adds new logging information to the end of an existing log file instead of rewriting the entire file each time logging is invoked.

   Default: No

   TraceFormat

   Specifies how the trace file displays the messages. Choose *one* of the following options:

   - default—uses square brackets [] to enclose the fields.
   - fixed—uses fields with a fixed width.
   - delim—uses a character of your choice to delimit the fields.
   - xml—uses XML-like tags. A DTD or style sheet is *not* provided with the Web Agent.

   Default: default (square brackets)

TraceDelimiter

Specifies a custom character that separates the fields in the trace file.

Default: No default

Example: |

TraceFileSize

Specifies (in megabytes) the maximum size of a trace file. The Web Agent creates a new file when this limit is reached.

Default: 0 (a new log file is not created)

Example: 20 (MB)

LogLocalTime

Specifies whether the logs use Greenwich Mean Time (GMT) or local time. To use GMT, change this setting to no. If this parameter does not exist, the default setting is used.

Default: Yes

7. Edit the WebAgentTrace.conf file to include a "components:" entry with value "XMLAgent.". For example:

```
# For WSS Agent
components: XMLAgent
data: Date, Time, Pid, Tid, TransactionID, Function, Message.
```

Framework agents do not support dynamic configuration of log parameters set locally in the Agent configuration file. Consequently, when you modify a parameter, the change does not take effect until you restart the web server. However, these log settings can be stored and updated dynamically if you configure them in an Agent configuration object on the Policy Server.

Note: IIS Agents create log files only after the first user request is submitted. Apache 2.0 Web Agents create log files when the Apache server starts.

8. Restart the web server so the SiteMinder WSS Agent uses the new trace configuration file.

Trace Log Components and Subcomponents

The CA SiteMinder® Agent can monitor specific CA SiteMinder® components. When you monitor a component, all of the events for that component are recorded in the trace log. Each component has one or more subcomponents that the agent can also monitor. If you do not want the agent to record all of the events for a component, you can specify only those subcomponents you want to monitor instead.

For example, if you want to record only the single sign-on messages for an agent on a web server, you would specify the WebAgent component and the SSO subcomponent.

The following components and subcomponents are available:

AgentFramework

Records all Agent framework messages. (Applies only to framework agents.) The following subcomponents are available:

- Administration
- Filter
- HighLevelAgent
- LowLevelAgent
- LowLevelAgentWP

AffiliateAgent

Records web Agent messages related to the 4.x Affiliate Agent, which is part of Federation Security Services, a separately-purchased product. (Applies only to framework agents.) The following subcomponent is available:

- RequestProcessing

SAMLAgent

Web Agent messages related to the SAML Affiliate Agent. (Applies only to framework agents.) The following subcomponent is available:

- RequestProcessing

WebAgent

Records all Web Agent log messages. Applies to all Agents *except* IIS 6.0 or Apache 2.0 Agents. The following subcomponents are available:

- AgentCore
- Cache
- authentication
- Responses
- Management
- SSO
- Filter

Agent_Functions

Records all Agent API messages. The following subcomponents are available:

- Init
- UnInit
- IsProtected
- Login
- ChangePassword
- Validate
- Logout
- Authorize
- Audit
- FreeAttributes
- UpdateAttributes
- GetSessionVariables
- SetSessionVariables
- DeleteSessionVariables
- Tunnel
- GetConfig
- DoManagement

Agent_Con_Manager

Records messages related to internal processing of the Agent API. The following subcomponents are available:

- RequestHandler
- Cluster
- Server
- WaitQueue
- Management
- Statistics

For an explanation of each subcomponent, see the WebAgentTrace.conf file.

Trace Message Data Fields

You can define what each trace message for a specific component contains by specifying which data fields to include in the message.

Data fields use the following syntax:

```
data:data_field1,data_field2,data_field3
```

Some data fields are shown in the following example:

```
data:message,date,time,user,agentname,IPAddr
```

There may not be data for fields in each message, so blank fields my occur. For example, if you select RealmOID as a data field, some trace messages will display the realm's OID while others will not.

The following data fields are available:

Message

Includes the actual trace message

SrcFile

Includes the source file and line number of the trace message

Pid

Includes the process ID

Tid

Includes the thread ID

Date

Includes the date

Time

Includes the time

PreciseTime

Includes the time, including milliseconds

Function

Includes the function in the code containing the trace message

User

Includes the name of the user

Domain

Includes the CA SiteMinder® domain

Realm

Includes the CA SiteMinder® realm

AgentName

Includes the Agent name being used

TransactionID

Includes the transaction ID

DomainOID

Includes the CA SiteMinder® domain OID

IPAddr

Includes the client IP address

RequestIPAddr

Includes the trace file displays the IP of the server where Agent is present

IPPort

Includes the client IP port

CertSerial

Includes the certificate serial number

SubjectDN

Includes the subject DN of the certificate

IssuerDN

Includes the Issuer DN of the certificate

SessionSpec

Includes the CA SiteMinder® session spec

SessionID

Includes the CA SiteMinder® session ID

UserDN

Includes the User DN

Resource

Includes the requested resource

Action

Includes the requested action

RealmOID

Includes the realm OID

ResponseTime

Includes the average response time in milliseconds of the Policy Servers associated with a CA Web Agent or SDK Agent and API application

Note: To output the ResponseTime to a trace log, include the component Agent_Con_Manager along with the data field ResponseTime in the WebAgentTrace.conf file or other file specified in the Policy Server Configuration Object (ACO) and restart the Policy Server. The Agent_Con_Manager component, or Agent API Connection Manager, calculates the ResponseTime each time a response is received from a Policy Server and keeps a running average. To locate the ResponseTime in the trace log, search for [PrintStats].

Trace Message Data Field Filters

To focus on a specific problem, you can narrow the output of the trace log by specifying a filter based on the value of a data field. For example, if you are having problems with an index.html page, you can filter on resources with an html suffix by specifying Resource:==/html in the trace configuration file. Each filter should be on a separate line in the file.

Filters use the following syntax:

data_field:*filter*

The following types of filters are available:

- == (exact match)
- != (does not equal)

The filters use boolean logic as shown in the following examples:

Action:!=get (all actions except get)

Resource:==/html (all resources ending in /html)

Determine the Content of the Trace Log

The WebAgentTrace.conf file determines the content of the trace log. You can control which components and data items appear in your trace log by modifying the settings of the WebAgentTrace.conf file on your web server. The following factors apply when editing the file:

- Entries are case-sensitive.

  When you specify a component, data field, or filter, the values must match exactly the options in the WebAgentTrace.conf file instructions.

- Uncomment the configuration settings lines.
- If you modify the WebAgentTrace.conf file before installing a new agent over an existing agent, the file is overwritten. Rename or back up the file first. After the installation, you can integrate your changes into the new file.

Follow these steps:

1. Open the WebAgentTrace.conf file.

   Note: We recommend duplicating the original file and changing the copy. Modifying the copy preserves the default settings.

2. Add components and subcomponents using the following steps:

   a. Find the section that matches your type of agent. For example, if you have an Apache 2.0 Agent that is installed on your server, look for a line resembling the following example:

   ```
   # For Apache 2.0, Apache 2.2, IIS 7.0 and SunOne Web Agents
   ```

   Note: For more information, see the *CA SiteMinder® Web Agent Installation Guide*.

   b. Locate the following line in that section:

   ```
   #components:
   ```

   c. Uncomment the line. Then add the component names that you want after the colon. Separate multiple components commas as shown in the following example:

   ```
   components:  AgentFramework, HTTPAgent
   ```

   d. (Optional) Follow the component name with the name of a subcomponent you want. Separate the subcomponent name with a slash as shown in the following example:

   ```
   components:  AgentFramework/Administration
   ```

3. Add data fields and filters using the following steps:

   a. Locate the following line in the appropriate section:

      ```
      #data:
      ```

   b. Uncomment the line. Then add the data fields that you want after the colon. Separate multiple data fields with commas as shown in the following example:

      ```
      data: Date, Time, Pid, Tid, TransactionID, Function, Message, IPAddr
      ```

   c. (Optional) Add filters to your data fields by following the data field with a colon, the Boolean operator and the value you want. The values you specify for the filters must match exactly. The following example shows a filter which logs activities for a specific IP address:

      ```
      data: Date, Time, Pid, Tid, TransactionID, Function, Message,
      IPAddr:==127.0.0.1
      ```

      Note: Each filter must be on a separate line in the file.

4. Save your changes and close the file.

5. Restart the web server to apply your changes.

   The content of the trace log has been determined.

Limit the Number of Trace Log Files Saved

You can limit the number of trace logs that a CA SiteMinder® agent keeps. For example, if you want to save disk space on the system that stores your agent logs, you can limit the number of trace logs using the following parameter:

TraceFilesToKeep

Specifies the number of CA SiteMinder® agent trace log files that are kept. New trace logs are created in the following situations:

- When the agent starts.
- When the size limit of the trace log (specified by the value of the TraceFileSize parameter) is reached.

Changing the value of this parameter does *not* automatically delete any existing trace logs which exceed the number that you want to keep. For example, If your system has 500 trace logs stored, and you decide to keep only 50 of those files, the agent does *not* delete the other 450 trace logs.

Setting the value of this parameter to zero retains all the trace logs.

Default: 0

Follow these steps:

1. Archive or delete any existing trace logs from your system.
2. Set the value of the TraceAppend parameter to no.
3. Change the value of the TraceFilesToKeep parameter to the number of trace logs that you want to keep.

Collect Detailed Agent Connection Data with an Agent Connection Manager Trace Log

To collect detailed information about the connections between a SiteMinder WSS Agent and Policy Server, you create a Trace Log file that contains information gathered by the Agent Collection Manager.

Follow these steps:

1. Open your Agent Configuration object or local configuration file.
2. Set the value of the TraceFile parameter to yes.

   Note: Setting the value of this parameter to yes in a local configuration file of a web server overrides any of the logging settings defined on the Policy Server. For example, when the value of this parameter is set to yes in a LocalConfig.conf file log files are generated even if the value of the AllowLocalConfig parameter in the corresponding Agent Configuration object on the Policy Server is set to no. Additionally, set the related trace logging parameters (that define the file name, size, and so on) in the LocalConfig.conf file to override any Policy Server trace log settings.

3. Specify the full path to the trace log file for your Agent Connection Data in the TraceFileName parameter. This is the file that contains the trace log output.
4. Set the value of the TraceConfigFile parameter to the full path of the following file:

   ```
   agent_home/config/AgentConMgr.conf
   ```

   agent_home

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

   Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

   Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

   Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

5. Define the format the trace log file for your Agent Connection Data by setting the following parameters:

   TraceAppend

   Adds new logging information to the end of an existing log file instead of rewriting the entire file each time logging is invoked.

   Default: No

   TraceDelimiter

   Specifies a custom character that separates the fields in the trace file.

   Default: No default

   Example: |

   TraceFileSize

   Specifies (in megabytes) the maximum size of a trace file. The Web Agent creates a new file when this limit is reached.

   Default: 0 (a new log file is not created)

   Example: 20 (MB)

   TraceFormat

   Specifies how the trace file displays the messages. Choose *one* of the following options:

   - default—uses square brackets [] to enclose the fields.
   - fixed—uses fields with a fixed width.
   - delim—uses a character of your choice to delimit the fields.
   - xml—uses XML-like tags. A DTD or style sheet is *not* provided with the Web Agent.

   Default: default (square brackets)

   LogLocalTime

   Specifies whether the logs use Greenwich Mean Time (GMT) or local time. To use GMT, change this setting to no. If this parameter does not exist, the default setting is used.

   Default: Yes

6. Restart your web server so the new settings take effect.

   Detailed information about the SiteMinder WSS Agent connections will be collected.

   Note: For CA SiteMinder® 12.52, the BusyHandleCount and FreeHandleCount attributes are not used.

Configure XML Message Processing Logging

In addition to Web Agent logging functionality, the SiteMinder WSS Agent provides an additional level of log information relating specifically to its processing of XML messages. SiteMinder WSS Agent logging is implemented using Apache's *log4j* standard (see http://logging.apache.org).

Note: SiteMinder WSS Agent logging does not start until an XML message that needs to be processed is received.

By default, SiteMinder WSS Agent logging is enabled and written to the soasm_agent.log file in:

- Windows—*agent_home*\bin\
- UNIX—*agent_home*/bin/

  agent_home

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

  Default (Windows 32-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent

  Default (Windows 64-bit SiteMinder WSS Agent installations: C:\Program Files\CA\Web Services Security\webagent\win64

  Default (Windows 32-bit SiteMinder WSS Agent installations operating on 64-bit systems: [set the PRF value for your book]\CA\Web Services Security\webagent\win32

You can change logging parameters for your SiteMinder WSS Agent by editing the log.config file, which can be found in:

- Windows—*agent_home*\config\
- UNIX— *agent_home*/config/

Disable SiteMinder WSS Agent XML Message Processing Logging

To disable SiteMinder WSS Agent XML message processing logging, remove or comment out (using a "#" prefix) the following lines from the log.config file located in the Agent config subdirectory:

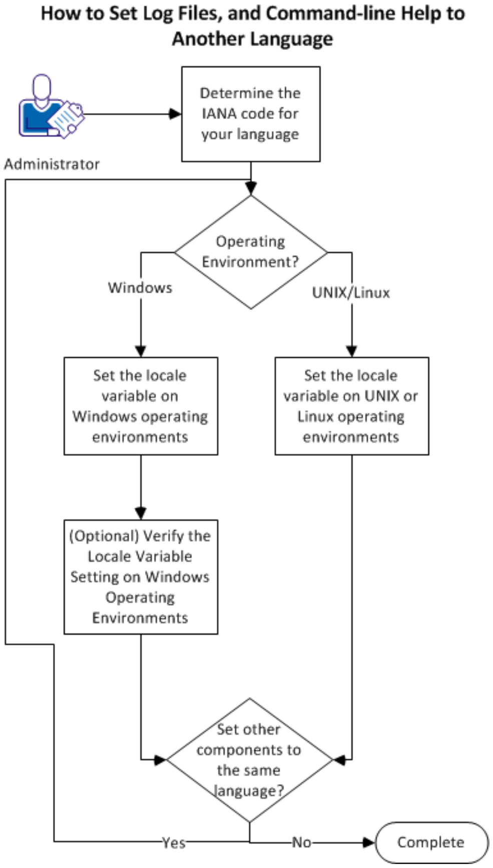
```
log4j.appender.A2=org.apache.log4j.DailyRollingFileAppender
log4j.appender.A2.File=${NETE_TXM_ROOT}/bin/soasm_agent.log
```

How to Set Log Files, and Command-line Help to Another Language

The following components support log files, and command-line help in other languages:

- The Policy Server
- The Web Agent
- The Report Server
- The CA SiteMinder Agent for SharePoint
- The CA SiteMinder® SPS
- SiteMinder WSS Agents
- Any custom software that is created with the CA SiteMinder® SDK.

The following graphic describes the work flow for setting log files, and command-line help to another language:


How to Set Log Files, and Command-line Help to Another Language
Administrator
Determine the IANA code for your language
Operating Environment?
Windows
UNIX/Linux
Set the locale variable on Windows operating environments
Set the locale variable on UNIX or Linux operating environments
(Optional) Verify the Locale Variable Setting on Windows Operating Environments
Set other components to the same language?
Yes
No
Complete

Follow these steps:

1. Determine the IANA code for your language (see page 93).
2. Create the environment variable for your operating environment using one of the following procedures:
   - Set the locale variable on Windows operating environments (see page 95).
   - Set the locale variable on UNIX or Linux operating environments (see page 97).
3. (Optional) Verify the locale variable setting on windows operating environments (see page 96).
4. (Optional) Repeat Steps 1 through 3 to set any other components in your environment to the same language.

Determine the IANA Code for Your Language

Each language has a unique code. The Internet Assigned Numbers Authority (IANA) assigns these language codes. Adding a language code to a locale variable changes the language that the software displays. Determine the proper code for the language that you want before creating the locale variable.

The following table lists the IANA codes that correspond to the languages supported by the software:

Language	**IANA Code**
Brazilian Portuguese	pt_BR
French	fr
German	de
Italian	it
Japanese	ja
Korean	ko
Simplified Chinese	zh-Hans
Spanish	es

Note: A list of IANA language codes is available from this third-party website.

Environment Variables

The environment variables are settings by which users can customize a computer to suit their needs. Examples of environment variables include the following items:

- A default directory for searching or storing downloaded files.
- A username.
- A list of locations to search for executable files (path).

Windows operating environments allow global environment variables, which apply to all users of a computer. The environment variables on UNIX or Linux operating environments must be set for each user or program.

To set the locale variable, pick the procedure for your operating environment from the following list:

- Set the locale variable on Windows operating environments (see page 95).
- Set the locale variable on UNIX or Linux operating environments (see page 97).

Set the Locale Variable on Windows Operating Environments

The following locale variable specifies the language settings for the software:

```
SM_ADMIN_LOCALE
```

Create this variable and set it to the language that you want. Set this variable on *each* component for which you want to use another language. For example, suppose you want to have a Policy Server and an agent that is set to French. Set this variable on both of those components to French.

Note: The installation or configuration programs do *not* set this variable.

Follow these steps:

1. Click Start, Control Panel, System, Advanced system settings.

   The system properties dialog appears.

2. Click the Advanced tab.
3. Click Environment Variables.
4. Locate the System variables section, and then click New.

   The New System Variable dialog opens with the cursor in the Variable name: field.

5. Type the following text:

   ```
   SM_ADMIN_LOCALE
   ```

6. Click the Variable name: field, and then type the IANA language code (see page 93) that you want.
7. Click OK.

   The New System Variable dialog closes and the SM_ADMIN_LOCALE variable appears in the list.

8. Click OK *twice*.

   The locale variable is set.

9. (Optional) Repeat Steps 1 through 8 to set other components to the same language.

Verify the Locale Variable Value on Windows Operating Environments

You can very the value to which the locale variable is set at any time. You can do this procedure after setting the variable to confirm that it is set correctly.

Note: Instructions for verifying the variable value on UNIX and Linux are in the setting procedure (see page 97).

Follow these steps:

1. Open a command-line window with the following steps:

   a. Click Start, Run.

   b. Type the following command:

      ```
      cmd
      ```

   c. Click OK.

      A command-line window opens.

2. Enter the following command:

   ```
   echo %SM_ADMIN_LOCALE%
   ```

   The locale appears on the next line. For example, when the language is set to German, the following code appears:

   ```
   de
   ```

   The value of the locale variable is verified.

Set the Locale Variable on UNIX or Linux Operating Environments

The following locale variable specifies the language settings for the software:

```
SM_ADMIN_LOCALE
```

Create this variable and set it to the language that you want. Set this variable on *each* component for which you want to use another language. For example, suppose you want to have a Policy Server and an agent that is set to French. Set this variable on both of those components to French.

Note: The installation or configuration programs do *not* set this variable.

Follow these steps:

1. Log in to the computer that is running the component that you want.
2. Open a console (command-line) window.
3. Enter the following command:

   ```
   export SM_ADMIN_LOCALE=IANA_language_code
   ```

   The command in the following example sets the language to French:

   ```
   export SM_ADMIN_LOCALE=fr
   ```

   The locale variable is set.
4. (Optional) Verify that the locale variable is set properly by entering the following command:

   ```
   echo $SM_ADMIN_LOCALE
   ```

   The locale appears on the next line. For example, when the language is set to German, the following code appears:

   ```
   de
   ```
5. (Optional) Repeat Steps 1 through 4 to set other components to the same language.

Chapter 10: 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.

Incorrect Error Code Returned Returned on XML-DCC Authentication Failure

Valid on Oracle Directory Enterprise Edition (formerly Oracle iPlanet Directory Server Enterprise Edition)

Symptom:

Authentication against the XML Document Credential Collector authentication scheme fails, but the web server returns a 500 Internal Server Error instead of a 403 Forbidden error.

Solution:

Perform the following steps:

1. Open the obj.conf file on your web server.
2. Locate the following line:

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

3. Add UseOutputStreamSize="0"to the end of the previous line, as shown in the following example:

   ```
   AuthTrans fn="SiteMinderAgent" UseOutputStreamSize="0"
   ```

4. Save the file, and then restart the web server.

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 the Information for the Agent Installation Program for the Windows Operating Environment (see page 31)