CA SiteMinder®

Web Agent Installation Guide

r12.0 SP2

CA Product References

This document references the following CA products:

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

Contact CA

Contact Technical Support

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

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

Provide Feedback

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

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

Contents

Chapter 1: Preparation 11

How to Prepare for a Web Agent Installation 11
Supported Operating Systems and Web Servers 12
How to Prepare a Windows System for a Web Agent Installation 12
How to Prepare a UNIX System for a Web Agent Installation 14
AIX Requirements 16
How to Prepare a Linux System for a Web Agent Installation 16
How to Prepare a Domino System for a Web Agent Installation 17
Miscellaneous Web Server Preparations 18
General Preparations for All Web Agents 19
Gather information Needed to Complete the Agent Installation 19
Preservation of Any WebAgentTrace.conf File Changes 19
Install the Correct Agent for a Web Server 19
Policy Server Requirements 20
Agent Configuration Parameters Required by All Agents 21
Agent Configuration Parameters Required for Domino Web Agents 22
Agent Configuration Parameters Required for IIS Web Agents 23
Prepare for Password Services 23
Repair ServletExec's CLASSPATH for JSP Password Services (Windows) 24
Password Services and Forms Directories 24
Prepare for Registration Services (Optional) 25
Use Registration Services 25
Install a Servlet Engine for Registration Services (Optional) 25
Use Active Directory for Registration Services (Windows Only) 26
Modify the DMS Admin Password for Registration Services 27
Modify the ServletExecAS Startup Script to Run Registration Services with ServletExecAS (UNIX only) 28

Chapter 2: Install a Web Agent on a Windows System 31

Run a GUI Mode Installation on Windows 32
Unattended Installations on Windows 34
Prepare an Unattended Installation on Windows 34
Run an Unattended Installation on Windows 35
How to Stop an Unattended Installation in Progress on Windows 36
Reinstall the Web Agent on Windows 36
Installation History Log File 37
Register Your System as a Trusted Host on Windows 38

Installation and Configuration Log Files . . . 41
Modify the SmHost.conf File (Windows) . . . 42
Re-register a Trusted Host Using the Registration Tool (Windows) . . . 44
Register Multiple Trusted Hosts on One System (Windows) . . . 47
Registration Services Installed Files (Windows) . . . 48
Fix the ServletExec CLASSPATH for DMS . . . 50

Chapter 3: Install a Web Agent on a UNIX System 51

Install the Web Agent Documentation on UNIX Systems . . . 52
Install the Web Agent on a UNIX System . . . 53
Run a GUI Mode Installation on UNIX . . . 54
Run a Console Mode Installation on UNIX . . . 56
Unattended Installations on UNIX . . . 57
Set the Web Agent Environment Variables After Installation . . . 60
Set Web Agent Variables when using apachectl Script . . . 61
Installation History Log File . . . 61
Reinstall a Web Agent on UNIX . . . 62
Register Your System as a Trusted Host on UNIX . . . 62
Register a Trusted Host in GUI or Console Mode . . . 63
Modify the SmHost.conf File (UNIX) . . . 67
Re-register a Trusted Host Using the Registration Tool (UNIX) . . . 69
Register Multiple Trusted Hosts on One System (UNIX) . . . 74
Files Installed for Registration Services (UNIX) . . . 75

Chapter 4: Upgrade a Web Agent to r12.0 SP2 77

How to Prepare for a Web Agent Upgrade . . . 77
Review the Upgrade Procedure . . . 77
Back Up Customized Files . . . 77
Password Services and Forms Template Changes During Upgrades . . . 78
Results of Running the Configuration Wizard After an Upgrade . . . 78
Ensure LD_PRELOAD Variable Does Not Conflict with Existing Agent . . . 78
Replace Existing Read-only Files . . . 78
Upgrade a Web Agent to r12.0 SP2 on Windows Systems . . . 79
Upgrade a Web Agent to r12.0 SP2 on UNIX Systems . . . 81

Chapter 5: Configure an IIS Web Agent 83

How to Configure a SiteMinder Web Agent on IIS 7.0 . . . 83
Add Role Services to your IIS 7 Web Server . . . 84
Run the Configuration Wizard for an IIS Web Agent . . . 85
Add Handler Mappings to Additional Web Sites you want to Protect with SiteMinder . . . 87

Add the Agent ISAPI Filter to Additional Web Sites that you want to Protect with SiteMinder . . . 89
How to Configure a SiteMinder Web Agent on IIS 6.0 . . . 91
Assign Read Permissions to Samples and Error Files Directories . . . 92
Allow IIS to Execute the Agent ISAPI and CGI Extensions . . . 93
IIS 6.0 Web Agents and Third-Party Software on the Same Server . . . 94
Increase the Agent's Size Limit for Uploaded Files . . . 95
Run the Configuration Wizard for an IIS Web Agent . . . 96
Put the Agent Filter and Extension Before Other Third-Party Filters . . . 98
How to Configure a SiteMinder Web Agent to Protect Microsoft Outlook Web Access . . . 100
Confirm the SiteMinder ISAPI filter appears first in the list . . . 102
Allow IIS to Execute the Outlook Extensions . . . 103
Set the Default Web Site Directory Location and Execute Permissions . . . 104
Add the ISAPI Extension to the Exchange Web Site . . . 105
Set the Directory Security for the Exchange Web Site . . . 106
Add the ISAPI Extension to the Exchweb Web Site . . . 107
Set the Directory Security for the Exchweb Web Site . . . 108
Set the Default Web Site Directory Location and Execute Permissions . . . 108
Confirm that SiteMinder is protecting the Outlook Web Access web site . . . 109

Chapter 6: Configure a Sun Java System Web Agent 111

Run the Configuration Wizard on Windows . . . 112
Configure Sun Java System Web Agents Using GUI or Console Mode . . . 115
Manually Configure a Sun Java System Web Server . . . 119
Apply Changes to Sun Java System Web Server Files . . . 120

Chapter 7: Configure an Apache Web Agent 123

Configure an Apache Web Agent on Windows Systems . . . 124
Configuration Methods for Apache Web Agents on UNIX Systems . . . 126
Configure an Apache Web Agent Using GUI or Console Mode . . . 127
Improve Server Performance with Optional httpd.conf File Changes . . . 130
Set the LD_PRELOAD Variable for Apache Agent Operation . . . 130
Set the LD_PRELOAD Variable for an Oracle 10G Web Server on Linux . . . 131
Set the LD_PRELOAD Variable for SSL Configuration on an IBM HTTP Server 2.0.47/Linux AS 3.0 System . . . 131
Set LD_PRELOAD for Using X.509-based Auth Schemes with Domino 6.5.3/SuSe8 Linux System . . . 131
Set the LD_ASSUME_KERNEL for Apache Agent on SuSE Linux 9 for zSeries . . . 132
Enabling SHLIB Path for an Agent on Apache 2.0/HP-UX 11 . . . 133
Configure Apache for Oracle 9.0.2/9.0.3 HTTP Server . . . 133

Chapter 8: Configure a Domino Web Agent 135

Configure a Domino Web Agent on Windows Systems 135
Add the Domino Web Agent DLL (Windows) 136
Run the Configuration Wizard for a Domino Web Agent on Windows 137
(Optional) Configure the CGI Directory and CGI URL Path Settings 138
(Optional) Configure Alias Settings to Enable Forms and Other HTML Authentication Schemes 139
How to Configure a Domino Web Agent on UNIX Systems 139
Add the Domino Web Agent DLL (UNIX) 140
Configuration Methods for Domino Web Agents on UNIX Systems 141
Configure Domino Web Agents in GUI or Console Mode 142
(Optional) Configure the CGI Directory and CGI URL Path Settings 143
(Optional) Configure Alias Settings to Enable Forms and Other HTML Authentication Schemes 144

Chapter 9: Configurations Available for All Web Agents 145

How to Configure Any Web Agent in Unattended Mode 145
Prepare an Unattended Configuration 146
Run an Unattended Configuration 146
Check SmHost.conf File Permissions for Shared Secret Rollover 148
Reconfigure a Web Agent 148
How to Set Up Additional Agent Components 149

Chapter 10: Operating System Tuning 151

Tune the Shared Memory Segments 152
How to Tune the Solaris 10 Resource Controls 154

Chapter 11: Password Services 155

Password Services Implementations 155
How to Set Up Your Environment for JSP Password Services 156
How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server 157
How to Configure the ServletExec Servlet Engine for JSP Password Services on a Sun Java System Web Server in the UNIX Operating Environment 158

Chapter 12: Uninstall a Web Agent 161

Notes About Uninstalling Web Agents 161
Set JRE in PATH Variable Before Uninstalling the Web Agent 162
Uninstall a Web Agent from a Windows System 163
Uninstall Documentation from a Windows System 163

Uninstall a Web Agent from a UNIX System 164
Uninstall Documentation from UNIX Systems 165

Chapter 13: Troubleshooting 167

Agent Start-Up/Shutdown Issues (Framework Agents Only) 167
Agent Won't Start Because LLAWP is Already Running or Log Messages not Written to the Correct Log Files 168
Troubleshoot Agent Start-Up/ShutDown with LLAWP 168
Web Agent Start Up and Shut Down Issues (IBM HTTP Server) 169
Lack of Write Permissions on Host Configuration File 170
Connectivity and Trusted Host Registration Issues 171
Trusted Host Registration Fails 171
No Connection From Trusted Host to Policy Server 172
Host Registered, but the SMHost.conf file has been Deleted 172
General Installation Issues 172
One Installation Hangs During Multiple Installations on the Same System 173
Location of the Installation Failure Log 173
Attempt to Access DMS Page Returns Error 174
Web Agent Not Shown in Add/Remove Programs Control Panel 174
Error Message During Upgrade 175
Metabase Error When Configuring An IIS Web Agent 175
Miscellaneous Issues 176
Netscape Browser Won't Open PDFs 176
Adobe Acrobat Reader Won't Install on a Windows System 177
Sun Java System Web Agent Issues 177
Web Server Starts but Web Agent Not Enabled 177
smget Error Message When Web Server Starts 177
Reconfigured Web Agent Won't Operate 178
Sun Java System Web Server Fails at Runtime 178
Apache Web Agent Issues 178
Apache Server Starts But Web Agent Is Not Enabled 179
Apache Server Shows shmget Failure On Startup 179
Apache Agent is Enabled but Default Server Page or Protected Resource Not Accessible 179
Apache Web Agent Not Operating 180
Domino Web Agent Issues 180
Domino Web Agent Not Enabled but the Web Server has Started 180
Domino Agent Cannot Initialize When Local Configuration Mode is Used 180

Appendix A: Unattended Installation 181

ca-wa-installer.properties File 181
Modify General Information 182

Register a Trusted Host 182
Identify Policy Servers for Trusted Host Registration 183
Specify the Host Configuration File 183
Select a Web Server for Configuration 184
WEB_SERVER_INFO Variables 185
Configure the Web Server to Restart (Windows Only) 188
Name the Trusted Host Name and Host Configuration Object 188

Appendix B: Settings Added to the Sun Java System Server Configuration 189

Additions for Sun Java System Server 6.0 189
magnus.conf File Additions for Windows Platforms 190
Code Added to the magnus.conf File on UNIX Platforms 190
obj.conf File Additions for Windows Platforms 191
obj.conf File Additions for UNIX Platforms 193
mime.types File Additions for Windows and UNIX Platforms 194
Check Agent Start-up with LLAWP 195

Appendix C: Configuration Changes to Web Servers with Apache Web Agent 197

Library Path for the Web Server is Set for UNIX Systems 197
Set Library Path and Path for Oracle 10g Web Server Running in Apache 2.x Mode 198
Changes to the httpd.conf File 198
Entries Added to DSO Support Section 199
SmInitFile Entry Added 201
Alias Entries Added 202
AddHandler Entries Added for Traditional Agents 204
Certificate Authentication Entries Added 205
LoadFile Entries Added for Apache 2.x on HP-UX 11i 205
Agent Parameter Added for SSL Connections Using Apache 1.x Based Servers 205

Appendix D: Environment Variables Added or Modified by the Web Agent Installation 207

Added or Modified Environment Variables 207

Index 209

Chapter 1: Preparation

This section contains the following topics:

How to Prepare for a Web Agent Installation (see page 11)
Supported Operating Systems and Web Servers (see page 12)
General Preparations for All Web Agents (see page 19)
Policy Server Requirements (see page 20)
Prepare for Password Services (see page 23)
Prepare for Registration Services (Optional) (see page 25)

How to Prepare for a Web Agent Installation

To prepare for a Web Agent installation, use the following process:

1. Prepare your web server by doing the following tasks:
   a. Ensure you have an account with one of the following for your web server:
      - Administrative privileges (for Windows systems).
      - Root privileges (for UNIX systems).
   b. Confirm that the operating system has the proper service packs or patches installed.
   c. Configure any options or settings required to operate a SiteMinder Agent on your type of web server. Some possible examples of these include (but are not limited to) the following:
      - Using a non-default IIS web site (see page 12).
      - Compiling an Apache web server for use on a Linux System (see page 17).
2. Confirm the following items for all Web Agent installations:
   - Ensure the Policy Server is installed and configured (see page 20).
   - Gather the information needed to complete the Web Agent installation (see page 19).
   - Preserve the changes in your WebAgentTrace.conf file (see page 19).
   - Select the correct Agent for your web server (see page 19).
3. (Optional) Meet the prerequisites for password services (see page 23).
4. (Optional) Meet the prerequisites for registration services (see page 25).

Supported Operating Systems and Web Servers

Before you install a Web Agent, make sure you are using a supported operating system and web server configuration. For a list of SiteMinder Web Agents and supported web server platforms, go to Technical Support, and search for the SiteMinder r12.0 SP2 Platform Matrix.

Note: After you install the Web Agent, you can configure multiple Web Agent instances for each Sun Java System and Apache web server installed on your system.

How to Prepare a Windows System for a Web Agent Installation

To prepare your Windows system for a Web Agent installation, you may need to perform one or more of the following tasks, as required by your environment:

- If you are installing a Web Agent on a 64-bit Windows platform, you must install the Visual C++ 2005 Redistributable package (see page 12) first.
- Prepare a non-default IIS web site (see page 12).
- Install an Apache web server as a service for all users (see page 14).

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

Before installing an r12.0 SP2 Web Agent on a Windows 64-bit platform, you must download and install the Microsoft Visual C++ 2005 Redistributable Package (x64). Go to the Microsoft downloads page, and then search for "Microsoft Visual C++ 2005 Redistributable Package (x64)."

How to Use a Non-Default IIS Website

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

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

The actual tools and steps involved in editing the Metabase depend on the version of IIS you are using. For example, if you are using an r12.0 SP2 SiteMinder Web Agent, on IIS 6.0, you would edit the Metabase using the following process:

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

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

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

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

   root

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

   AppRoot

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

   /LM/W3SVC/*identifier_number*/Root
9. Change the value of the *identifier_number* to 1, and then click OK.

10. Close the Metabase Explorer.
11. Run the Configuration Wizard to reconfigure your IIS Web Agent.
12. Repeat Steps 3 through 10, but change the number 1 back to the original identifier from in Step 2.
13. Restart the IIS web server.

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

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

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

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

How to Prepare a UNIX System for a Web Agent Installation

To prepare your UNIX system for a Web Agent Installation, use the following process:

1. Set the DISPLAY variable.
2. Confirm that you have the required patches installed for your operating system, as shown in the following:
   - Required AIX patches (see page 16)
   - Required HP-UX patches (see page 15)
   - Required Solaris patches (see page 15)

Set the DISPLAY For Web Agent Installations on UNIX

If you are installing the Web Agent on a UNIX system from a remote terminal, such as a Telnet or Exceed terminal, be sure the DISPLAY variable is set for the local system. For example, if your machine is 111.11.1.12, set the variable as follows:

```
DISPLAY=111.11.1.12:0.0
export DISPLAY
```

Note: You can also install the Web Agent using the console mode installation, which does not require the X window display mode.

Required Solaris Patches

Before installing a Web Agent on a Solaris machine, you must install the following patches:

Solaris 9

Requires patch 111711-16.

Solaris 10

Requires patch 119963-08.

You can check on patch versions by logging in as root and executing the following command:

showrev -p | grep *patch_id*

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

Solaris Settings for Certain Apache 1.3 Type Web Servers

Certain versions of Apache 1.3 and related web servers such as IHS 1.3 may not start correctly on the Solaris operating environment due to an issue with Solaris run time initialization.

To avoid this problem, please set the following environment variable:

LD_PRELOAD=*web_agent_home*/lib/libbtunicode.so

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

Required HP-UX Patches

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

HP-UX Release	Patch
HP-UX 11i v1	■ PHCO_29029 is recommended for SiteMinder 6.0.4 and SiteMinder 6.0.5.

HP-UX Release	Patch
HP-UX 11i v1	■ PHSS_26560 ld and linker cumulative patch

AIX Requirements

SiteMinder Web Agents running on AIX systems require the following patches:

- For Apache 1.x Web Agents, install IBM HTTP Server patch PQ87084

SiteMinder Web Agents running on AIX systems also require the following:

- To run a re-architected (framework) SiteMinder Sun Java System or Apache Web Agent on an AIX system, your C/C++ runtime environment must be version 8.0.0.0.

  Note: For more information, see the following web site:
  http://www-1.ibm.com/support/docview.wss?uid=swg1IY78159

How to Prepare a Linux System for a Web Agent Installation

To prepare your Linux system for a Web Agent Installation, use the following process:

1. Confirm that you have installed the required Linux patches (see page 16).
2. Confirm that you have installed the required Linux libraries.
3. Before using an Apache web server, you must compile it (see page 17).

Required Linux Patches

The following Linux patches are required:

For Linux release 2.1

glibc-2.4.2-32.20 for Linux Application Server 2.1

For Web Agents running on 64-bit Linux systems

- Binutils 2.17
- GCC 4.1.0

Required Linux Libraries

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

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

Compile an Apache Web Server on a Linux System

For the Web Agent to operate with an Apache web server running Linux, you have to compile the server. Compiling is required because the Agent code uses pthreads (a library of POSIX-compliant thread routines), but the Apache server on the Linux platform does not, by default.

If you do not compile with the lpthread option, the Apache server starts up, but then hangs and does not handle any requests. The Apache server on Linux cannot initialize a module which uses pthreads due to issues with Linux's dynamic loader.

To compile Apache on Linux for the Web Agent

1. Enter the following:

   LIBS=-lpthread

   export LIBS

2. Configure Apache as usual by entering the folloiwng:

   configure --enable-module=so --prefix=*your_install_target_directory*

   make

   make install

How to Prepare a Domino System for a Web Agent Installation

To prepare your Domino system for a Web Agent installation, ensure you have installed whichever of the following items is appropriate for your system:

- IBM Hot fixes for Domino 6.5.2 (see page 18)

IBM Hot Fix Required for Domino 6.5.2

IBM hot fix SPR #NORK632KQA is required for a Web Agent to run on a Domino 6.5.2 server.

This hotfix applies to Windows and UNIX platforms.

Miscellaneous Web Server Preparations

The following sections discuss installation preparations for various web servers.

Add a Logs Subdirectory for Apache Web Agents

For Apache Web Agents, a logs subdirectory must exist under the Apache server's root directory so that the Web Agent can operate properly. This subdirectory must have Read and Write permissions for the user identity under which the Apache child process will be running.

If the logs subdirectory does not exist, create it with the required permissions.

Note: This configuration requirement applies to any Apache-based server that writes log files outside the Apache root directory.

Enable Write Permissions for IBM HTTP Server Logs

If you install the Web Agent on an IBM HTTP Server, this web server gets installed as root and its subdirectories do not give all users in all groups Write permissions.

For the Low Level Agent Worker Process (LLAWP) to write Web Agent initialization messages to the web server logs, the user running the web server needs permission to write to the web server's log directory. Ensure that you allow write permissions for this user.

Modify the Apache 2.0 httpd.conf File for Agents on IBM HTTP Servers

If an Apache 2.0 Web Agent is installed on an IBM HTTP Server 2.0.47 on Windows, the server does not load if the ibm_afpa_module is also loaded in the httpd.conf file.

To avoid this problem, comment out the following lines from the httpd.conf file:

```
#LoadModule ibm_afpa_module modules/mod_afpa_cache.so

#AfpaEnable
#AfpaCache on
#AfpaPort 9080
#AfpaLogFile "D:/Program Files/IBM HTTP Server 2.0/logs/afpalog" V-ECLF
```

General Preparations for All Web Agents

The following sections describe general preparations for all Web Agents.

Gather information Needed to Complete the Agent Installation

You must have the following information before installing the Web Agent:

- Name of the SiteMinder Administrator allowed to install Agents
- Name of the Host Configuration Object. This defines the trusted host configuration.
- Name of the Agent Configuration Object, which contains the Agent configuration settings. A single Agent Configuration Object can be referenced by many Agents.

Preservation of Any WebAgentTrace.conf File Changes

If you have modified the WebAgentTrace.conf file and you are installing a new Web Agent over an existing Web Agent, the WebAgentTrace.conf file is overwritten. Therefore, you should rename or back up the WebAgentTrace.conf file before the installation.

Important! Once the installer starts, the existing file is overwritten without warning. Your old settings will be lost if you do not copy or back up the original file.

After the installation, you can integrate your changes into the new file.

Install the Correct Agent for a Web Server

Install the following Web Agents with the corresponding web servers:

Web Agent	Web Server
IIS	Microsoft IIS
Domino	IBM Lotus Domino
Sun Java System	Sun Java System
Apache	Apache, HP-based Apache, IBM HTTP, Oracle HTTP Server. Most of the information for the Apache web server applies to these web servers.

For details on supported web server and operating system versions, go to Technical Support, and then search for the SiteMinder r12.0 SP2 Platform Support Matrix.

Policy Server Requirements

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

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

You must configure Policy Server with the following items:

- A SiteMinder Administrator that has the right to register trusted hosts.

  A trusted host is a client computer where one or more SiteMinder Web Agents are installed. The term trusted host refers to the physical system. There must be an administrator with the privilege to register trusted hosts.

- Agent identity

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

- Host Configuration Object

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

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

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

- Agent Configuration Object

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

Agent Configuration Parameters Required by All Agents

All Agents *must* have a value set for the following parameter:

DefaultAgentName

Defines a name that the Web Agent uses when it receives a request on an IP address or interface for which there is no agent name specified in the AgentName parameter.

If you are using virtual servers, you can set up your SiteMinder environment quickly by using a DefaultAgentName instead of defining a separate Web Agent for each virtual server.

Important! If you do not specify a value for the DefaultAgentName parameter, you must list every agent identity in the AgentName parameter. Otherwise, the Policy Server will not be able to tie policies to the Web Agent.

Default: No default

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

The value of the previous parameter entry must exactly match the name of an Agent object that you defined in the Administrative UI.

Agent Configuration Parameters Required for Domino Web Agents

In addition to the parameters required by all Agents, Domino Web Agents must also have values set for the following parameters:

DominoDefaultUser

Specifies the name by which the Domino Web Agent identifies the users that SiteMinder has previously authenticated against another directory to the Domino server.

Important! This parameter must be encrypted if it is stored in a local configuration file. Use the encryptkey tool to encrypt this parameter. Do not change it by editing the local configuration file directly.

Default: **No default**

DominoSuperUser

Identifies a user who has access to all resources on the Domino server, and ensures that all users successfully logged into SiteMinder will be logged into Domino as the Domino SuperUser.

This value can be encrypted.

This parameter affects the following parameters:

- SkipDominoAuth

Default: No default

More information:

Run the Configuration Wizard for a Domino Web Agent on Windows (see page 137)

Agent Configuration Parameters Required for IIS Web Agents

In addition to the parameters required by all Agents, IIS Web Agents *may* need to have values set for the following parameters in certain circumstances:

DefaultUsername

Specifies the name of a Windows user that is used to access IIS resources as a proxy user. When users want to access resources on an IIS web server protected by SiteMinder, they may not have the necessary server access privileges. For example, if users are stored in an LDAP user directory on a UNIX system, those users may not have access to the Windows system with the IIS web server.

The Web Agent must use this NT user account, which is assigned by an NT administrator, to act as a proxy user account for users granted access by SiteMinder.

Default: **No default**

DefaultPassword

Specifies a default password for the associated Windows user that is used to access IIS resources as a proxy user.

Important! If you want to encrypt this parameter, set it centrally in the Agent Configuration Object. If this parameter is set in a local configuration file, it will not be encrypted and will be less secure.

Default: No default

When users want to access resources on an IIS web server protected by SiteMinder, they may not have the necessary server access privileges. The Web Agent must use this NT user account, which is assigned by an NT administrator, to act as a proxy user account for users granted access by SiteMinder.

Do not specify values for each of the previous parameters if you plan to do either of the following:

- Use the NTLM authentication scheme.
- Enable the Windows User Security Context feature.

More information:

How to Configure a SiteMinder Web Agent on IIS 6.0 (see page 91)

Prepare for Password Services

The following sections discuss prerequisites and guidelines for password services.

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

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

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

To repair the ServletExec classpath

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

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

2. Restart the Sun Java System web server or IIS Admin services. This forces ServletExec to write the classpath.pref.
3. For Windows 2000, do the folloiwng:
   a. Stop the IIS Admin service.
   b. Start the World Wide Web Publishing service *without* manually starting the IIS Admin service.
   c. If the error still occurs, then continue with the following steps:
   d. Open the classpath.pref file with a text editor.
   e. Collapse all entries to a single line separated by a semi-colon(;).
   f. Save the file.
   g. Restart the web server.

Password Services and Forms Directories

When you install a Web Agent for the first time, the installation program creates the following folders in the Web Agent home directory:

- jpw_default and jpw (for Password Services)
- pw_default and pw (for Password Services)
- samples_default and samples (for DMS and standard forms)

The jpw, pw, and samples directories are the working directories that include templates and forms that you customize. The "default" versions are backup directories for the original documents.

Prepare for Registration Services (Optional)

The following sections discuss prerequisites and guidelines for registration services.

Use Registration Services

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

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

To continue using your existing DMS application with r12.0 SP2 do not install Registration Services when you install the r12.0 SP2 Web Agent, as shown in the following table.

If...	Then...
■ You have DMS 2.01 ■ You install r12.0 SP2 with SiteMinder SM r12.0 SP2	you can continue running DMS 2.0
■ You have DMS 2.01 ■ You install r12.0 SP2 with SiteMinder r12.0 SP2	apply DMS 2.01 Hot Fix CR5 before you continue running DMS 2.01

Install a Servlet Engine for Registration Services (Optional)

If you want the Agent to provide Registration Services, you must install a supported servlet engine. For a list of supported servlet engines, go to Technical Support, and then search for the SiteMinder r12.0 SP2 Platform Support Matrix.

Use Active Directory for Registration Services (Windows Only)

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

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

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

Modify the DMS Admin Password for Registration Services

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

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

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

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

At the Web Agent:

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

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

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

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

At the Policy Server:

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

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

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

To modify the StartServletExec script

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

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

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

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

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

   In this CLASSPATH entry, replace:

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

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

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

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

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

   LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/export/smuser/ca/siteminder/webagent/bin; export LD_LIBRARY_PATH

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

Operating System	Path Variable

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

Chapter 2: Install a Web Agent on a Windows System

This section contains the following topics:

Run a GUI Mode Installation on Windows (see page 32)
Unattended Installations on Windows (see page 34)
Reinstall the Web Agent on Windows (see page 36)
Installation History Log File (see page 37)
Register Your System as a Trusted Host on Windows (see page 38)
Register Multiple Trusted Hosts on One System (Windows) (see page 47)
Registration Services Installed Files (Windows) (see page 48)
Fix the ServletExec CLASSPATH for DMS (see page 50)

Run a GUI Mode Installation on Windows

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

1. Exit all applications that are running and stop the web server.
2. Download the installation file from Technical Support.
3. Navigate to the win folder then run the executable file for your operating system:

   ca-wa-*version*-win*processor_type*.exe

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

   The installation program prepares the files.
4. Review the information in the Introduction dialog box, then click Next.
5. Read the License Agreement then select the radio button to accept the agreement. Click Next.

   If you do not accept the agreement, the installation terminates.
6. Read the notes in the Important Information dialog box, then click Next.
7. In the Choose Install Folder dialog box, accept the default location or use the Choose button to select a different location. Click Next.

   If you select a non-default location then want to revert to the default directory, click Restore Default Folder.
8. Select the placement of the Agent Configuration Wizard shortcut in the Choose Shortcut Folder dialog box then click Next.

   To allow all users access to the Configuration Wizard, ensure the Create Icons for All Users check box is selected. Otherwise, clear this option.
9. Review the information in the Pre-Installation Summary dialog box, then click Install.

   Note: The installation program may detect that newer versions of certain system dlls are installed on your system. It asks if you want to overwrite these newer files with older files. Select No To All if you see this message.

   The Web Agent files are copied to the specified location. Afterward, the Web Agent Configuration dialog box is displayed.
10. Choose one of the following options:
    - Yes. I would like to configure the Agent now.
    - No. I will configure the Agent later.

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

For Web Agents installed on IIS 6.0 servers, reboot your system after installation; it is not sufficient to restart the IIS service.

Important! If you are configuring an Agent on an IIS web server, do not configure the Agent immediately after installation. There are some tasks you need to do before configuring the Agent.

11. If you choose not to configure the Agent, the Install Complete dialog box displays, and prompts you to reboot the system.
12. Click Done.

    If you selected the option to configure the Agent automatically, the installation program prepares the Web Agent Configuration Wizard and begins the trusted host registration and configuration processes.

    Do the following:

    - Register the trusted host. You can do this before or after configuring an Agent, but the Agent will *not* be able to communicate properly with the Policy Server unless the trusted host is registered.
    - Configure the Web Agent.

Installation Notes:

- After installation, you can review the installation log file in *web_agent_home*\install_config_info. The file name is: CA_SiteMinder_Web_Agent_*version*_InstallLog.log

  web_agent_home

  Indicates the directory where the Web Agent is installed.

  Default (Windows installations): C:\Program Files\CA\webagent

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

- You may choose not to start the Web Agent Configuration Wizard immediately after installation—you may have to reboot your machine after installation. If so, you can start the Wizard manually when you are ready to configure an Agent.

More Information

Register Your System as a Trusted Host on UNIX (see page 62)
Configure an IIS Web Agent (see page 83)
Configure a Sun Java System Web Agent (see page 111)
Configure an Apache Web Agent (see page 123)
Configure a Domino Web Agent (see page 135)
How to Configure a SiteMinder Web Agent on IIS 6.0 (see page 91)

Unattended Installations on Windows

After you have installed the Web Agent on one system, you can automate installations on other web servers using the Agent's unattended installation feature. An unattended installation lets you install or uninstall the Web Agent without any user interaction.

An unattended installation uses a properties file that is initially configured with values from the initial GUI or console mode Web Agent installation. Therefore, you can only run an unattended installation on a system with the same platform and web server image as the system where you first installed the Web Agent. For example, if you install an Agent on a Windows system with an Sun Java System web server first, you *cannot* use the properties file to run an unattended installation on a UNIX system with an Apache web server.

Prepare an Unattended Installation on Windows

Unattended installation uses the ca-wa-installer.properties file to propagate the Web Agent installation set up to all Agents in your network. In this properties file, you define installation parameters, then copy the file and the Web Agent executable file to any web server in your network to run an unattended installation.

The ca-wa-installer.properties file is installed in the following location:
web_agent_home\install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation.

To prepare for an unattended installation

1. Run an initial installation of the Web Agent.
2. Open the ca-wa-installer.properties file and modify the parameters in the file. The parameters are as follows:
   - USER_INSTALL_DIR--Specifies the installed location of the Web Agent. Enter the full path to the installation directory.
   - USER_SHORTCUTS--Specifies where the Web Agent Configuration Wizard shortcut should be installed. Enter the path to the desired location. (Windows only)
   - USER_REQUESTED_RESTART--Indicates whether the installation program should reboot a Windows machine if required. Set to YES to allow the reboot. (Windows only)
3. Save the file.

Run an Unattended Installation on Windows

You should have completed an initial Web Agent installation and, if necessary, modified the ca-wa-installer.properties file. Now, you can use the file to run subsequent Web Agent installations.

To run an unattended Web Agent installation

1. From a system where the Web Agent is already installed, copy the following files to a local directory:
   a. ca-wa-*version*-win32.exe (Agent executable) from where it resides on your system.
   b. ca-wa-installer.properties file from *web_agent_home*\install_config_info
2. Open a command window and navigate to the directory where you copied the files.

   Important! If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.
3. Run the installation executable with the -f and - i silent options, as shown in the following example:

   agent_executable -f *properties_file* -i silent

   Assuming that you run the installation from the directory where the executable and properties file are located, the command would be:

   ca-wa-<*version*>-win32.exe -f ca-wa-installer.properties -i silent

   Note: If you are not at the directory where these files reside, you must specify the full path to each file. If there are spaces in the directory paths, enclose the entire path between quotation marks.

   When the installation is complete, you return to the command prompt.
4. Check to see if the installation completed successfully by looking in the CA_SiteMinder_Web_Agent _*version*_InstallLog.log file, located in the *web_agent_home*\install_config_info directory. This log file contains the results of the installation.
5. Register the trusted host and configure the Web Agent.

   Note: If you are configuring an Agent on an IIS 6.0 server, do not configure the Agent immediately after installation. There are some setup procedures you need to perform before configuring the Agent.

More Information

How to Configure a SiteMinder Web Agent on IIS 6.0 (see page 91)
How to Configure Any Web Agent in Unattended Mode (see page 145)

How to Stop an Unattended Installation in Progress on Windows

To manually stop an unattended installation on Windows systems, use the following process:

1. Open the Windows Task Manager.
2. Stop the following processes:
   - ca-wa-*version*-win.exe
   - wa_install.exe

Reinstall the Web Agent on Windows

You can reinstall a Web Agent to restore missing application files. For this procedure, you do not need to uninstall the existing Web Agent; simply perform a reinstall over the existing Web Agent files by repeating the installation procedure.

To reinstall the Web Agent on Windows, use the following process:

1. Make back up copies of the following:
   - Your Windows registry settings.
   - Your Web Agent configuration settings.
2. Install the Web Agent on your Windows system using the GUI installer.

More Information

Run a GUI Mode Installation on Windows (see page 32)

Installation History Log File

The installer creates a log file with following information:

- The product name
- The installed location
- The complete (full) version number

This file is created in the following location:

Windows

C:\Program Files\CA\install-info\ca-install-history.log

UNIX

/opt/ca/install-info/ca-install-history.log

More information:

Installation and Configuration Log Files (see page 41)

Register Your System as a Trusted Host on Windows

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

To establish a connection between the trusted host and the Policy Server, you need to register the host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. After this file is created successfully, the client computer becomes a trusted host.

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

Note: You only register the host once, *not* each time you install and configure a Web Agent on your system.

To register a trusted host

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

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

2. In the Host Registration dialog box:

   a. Select Yes to register a host now or No to register the host at a later time.

   b. If you are using PKCS11 cryptographic hardware in your SiteMinder environment, select the check box.

   c. Click Next.

3. If you enabled cryptographic hardware, complete the fields. If not, skip to the next step.

   a. In the PKCS11 DLL field, enter the full path to the PKCS11 DLL. Click on Choose to search for the DLL.

   b. Optionally, specify the token label in the Token Label and Token Passphrase, if applicable. Re-confirm the passphrase in the Confirm token passphrase field then click Next.

4. In the Admin Registration dialog box, complete the following fields to identify an administrator with the rights to register a trusted host, then click Next:

   - Admin User Name—enter the name of the administrator allowed to register the host with the Policy Server.

This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.

- Admin Password—enter the administrator's password.
- Confirm Admin Password—re-enter the password.
- Enabled Shared Secret Rollover—check this box to periodically change the shared secret used to encrypt communication between the trusted host and the Policy Server. Key rollover must be enabled at the Policy Server for this feature to work.

  To disable shared secret rollover or enable it at a later time, you have to re-register the trusted host, or use the Policy Management API in the C and Perl Scripting Interface to enable or disable shared secret rollover.

5. In the Trusted Host Name and Configuration Object dialog box, enter values for the two fields then click Next.

   a. In the Trusted Host Name field, enter a unique name that represents the trusted host to the Policy Server. This name *does not* have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

      Note: This name must be unique among trusted hosts and not match the name of any other Web Agent.

   b. In the Host Configuration Object field, enter the name of the Host Configuration Object specified in the Policy Server, then click Next.

      This object defines the connection between the trusted host and the Policy Server. For example, to use the default, enter DefaultHostSettings. In most cases, you will have created your own Host Configuration Object.

      Note: The entry you specify must match the Host Configuration Object entry set at the Policy Server.

6. In the Policy Server IP Address dialog box:

   a. Enter the IP address, or host name, and the authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

      You can specify a non-default port number, but if your Policy Server is configured to use a non-default port and you omit it when you register a trusted host, SiteMinder displays the following error:

      Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1)

      Note also that if you specify a non-default port, that port is used for the Policy Server's authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port. The entry in the SmHost.conf file will look like:

policyserver="*ip_address*,5555,5555,5555"

b. Click Add.

You can add more than one Policy Sever; however, for host registration, only the first server in the list will be used.

If multiple Policy Servers are specified, the Agent uses them as bootstrap servers. When the Agent starts up, the Web Agent has several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap Policy Server is no longer used by that server process. The Host Configuration Object can contain another set of servers, which may or may not include any of the bootstrap servers.

c. Click Next.

7. If you want to use FIPS encryption, choose one of the following options:

FIPS Compatibility Mode (Default)

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

FIPS Migration Mode

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

FIPS Only Mode

Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using only FIPS 140-2 algorithms.

Important! A SiteMinder r12.0 SP2 installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

If you do *not* want to use FIPS encryption, accept the default.

8. Click Next.

9. Accept the default location of the host configuration file, SmHost.conf or click Choose to select a different location. Click Next.

If you select a non-default location then want to revert to the default directory, click Restore Default Folder.

The host is registered and a host configuration file, SmHost.conf, is created in *web_agent_home*/config. You can modify this file.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

10. Click Continue.
11. Continue with the configuration by doing the following appropriate tasks:
    - Configure an IIS Web Agent
    - Configure a Sun Java System Web Agent
    - Configure an Apache Web Agent
    - Configure a Domino Web Agent

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the Web Agent, check the following log files, located in *web_agent_home*\install_config_info:

ca-wa-details.log

Provides specific details on any failures or problems that may have occurred.

CA_SiteMinder_Web_Agent_*version*_InstallLog.log

Provides complete results of the installation, including the components that installed successfully and those that failed.

More information:

Installation History Log File (see page 37)

Modify the SmHost.conf File (Windows)

Web Agents and custom Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

To modify the SmHost.conf file

1. Navigate to the *web_agent_home*\config directory.
2. Open the SmHost.conf file in a text editor.
3. Enter new values for the any of the following settings that you want to change:

   Important! Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

   hostconfigobject

   Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

   If you want to change the host configuration object an object so the Web Agent u, you need to modify this setting.

   Example: hostconfigobject="*host_configuration_object*"

   policyserver

   Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

   "*IP_address*, *port*,*port*,*port*"

   The default ports are 44441,44442,44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

   To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

   Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

Important: If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Web Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

Default: *IP_address*, 44441,44442,44443

Example (Syntax for a single entry)**:** "*IP_address*, *port*,*port*,*port*"

Example (Syntax for multiple entries, place each Policy Server on a separate line)**:**
policyserver="123.122.1.1, 44441,44442,44443"
policyserver="111.222.2.2, 44441,44442,44443"
policyserver="321.123.1.1, 44441,44442,44443"

requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.

   The changes to the SmHost.conf file are applied.

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

When you install a Web Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the *web_agent_home*\bin directory when you install a Web Agent.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To re-register a trusted host using the registration tool

1. Open a command prompt window.
2. Enter the smreghost command using the following required arguments:

   smreghost -i *policy_server_IP_address:[port]*
   -u *administrator_username* -p *Administrator_password*
   -hn *hostname_for_registration* -hc *host_configuration_ object*

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

   example:
   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings

   The following example contains the -o argument:
   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A"
   -hc DefaultHostSettings -o

The following arguments are used with the smreghost command:

-i *policy_server_IP_ address:port*

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

If you specify a port number, which can be a non-default port, that port is used for all three Policy Server servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:

"*policy_server_ip_address*,5555,5555,5555"

Example: (IPv4) 127.0.0.1,44442

Example: (IPv6) [2001:DB8::/32][:44442]

-u *administrator_username*

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

-p *Administrator_password*

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

-hn *hostname_for_registration*

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

-hc *host_config_object*

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

-sh *shared_secret*

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

-rs

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

-f *path_to_host_config_file*

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

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

-cf *FIPS mode*

Specifies one of the following FIPS modes:

- COMPAT--Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.
- MIGRATE--Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.
- ONLY--Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using *only* FIPS 140-2 algorithms.

Important! A SiteMinder r12.0 SP2 installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

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

Default: COMPAT

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

-cp *cryptographic_provider*

(Optional) Indicates the name of the cryptographic provider you are using for encryption. If you do not specify a value the default is assumed.

Default: ETPKI

-cd *crypto_provider_DLL_or_configuration_file_path*

(Required for PKCS11 encryption) Indicates the full path to the PKCS11 DLL or configuration file.

-ct *crypto_provider_token_label*

(Optional for PKCS11 encryption) Indicates the token label for the hardware token. Only use this argument if there is a token label.

-o

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

-ck *crypto_provider_token_pin*

(Required for PKCS11 encryption) Indicates the passphrase for the token.

The trusted host is re-registered.

Register Multiple Trusted Hosts on One System (Windows)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SiteMinder client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.

To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server's SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

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

  Note: If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the smreghost command-line tool: Run the smreghost tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.

  Important! If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

Registration Services Installed Files (Windows)

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

Virtual Directories

- siteminderagent\dmspages
- siteminderagent\dmsforms

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

Physical Directories

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

- *web_agent_home*\samples

  Contains files used by Registration Services that you can customize.

- *web_agent_home*\samples_default

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

The following table describes each Registration Service Directory:

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

Fix the ServletExec CLASSPATH for DMS

If you install DMS on a Windows system and get 'servlet DMS not found' errors when you access a DMS page, verify that the ServletExec classpath is correct.

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

To repair the ServletExec classpath

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

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

2. Restart the Sun Java System web server or IIS Admin services. This forces ServletExec to write the classpath.pref.
3. For Windows 2000, do the folloiwng:
   a. Stop the IIS Admin service.
   b. Start the World Wide Web Publishing service *without* manually starting the IIS Admin service.
   c. If the error still occurs, then continue with the following steps:
   d. Open the classpath.pref file with a text editor.
   e. Collapse all entries to a single line separated by a semi-colon(;).
   f. Save the file.
   g. Restart the web server.

Chapter 3: Install a Web Agent on a UNIX System

This section contains the following topics:

Install the Web Agent Documentation on UNIX Systems (see page 52)
Install the Web Agent on a UNIX System (see page 53)
Set the Web Agent Environment Variables After Installation (see page 60)
Set Web Agent Variables when using apachectl Script (see page 61)
Installation History Log File (see page 61)
Reinstall a Web Agent on UNIX (see page 62)
Register Your System as a Trusted Host on UNIX (see page 62)
Register a Trusted Host in GUI or Console Mode (see page 63)
Register Multiple Trusted Hosts on One System (UNIX) (see page 74)
Files Installed for Registration Services (UNIX) (see page 75)

Install the Web Agent Documentation on UNIX Systems

You install the Web Agent documentation independently from the Web Agent—it is not installed by default. We recommend that you install the documentation *before* installing the Web Agent so you can specify the install location.

Note: If you plan to install the Web Agent documentation on the same system as existing Policy Server documentation, the installation puts the Agent manuals in the same location as the Policy Server documents, for example, *policy_server_home*/ca_documents. You will not be prompted to specify a location.

To install the documentation

1. Download the documentation installation programs from Technical Support, and then navigate to the directory for your operating system.
2. Copy the appropriate installation file for your operating system to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:

   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
   - nete-wa-doc-*version*-linux.bin (linux 2.1)
3. Open a console window, and check the permissions on the binary file. You may need to add execute to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system*.bin
4. From a console window, run the documentation installation using one of the following commands:

   GUI mode:

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

   Console mode:

   ./ca-wa-doc-*version-operating_system*.bin -i console

   The documentation installation starts.
5. Read the License Agreement, pressing Enter to page through the entire document. If you agree with the terms, enter Y to continue the installation.
6. Review the Important Instructions, then click Next.
7. Specify the installation directory.

   The installation program installs the r12.0 SP2 Web Agent documentation in the directory you specified.

Install the Web Agent on a UNIX System

There are several types of Web Agent installations on a UNIX system:

Note: Installing a Web Agent on a 64-bit Suse Linux 10 system requires additional preparations.

- Installing from a graphical user interface
- Installing from a console window responding to command-line prompts
- Installing installation file, unattended by an administrator and requiring no user interaction.

Select the installation method that best suits your environment.

Note the following:

- The Web Agent installation adds and modifies a few system environment variables.
- When you install an Apache, Stronghold, or IBM HTTP Server Web Agent, the following warning is displayed when you restart the web server:

  Loaded DSO /export/smuser/ca/siteminder/webagent/bin/mod_sm.so uses plain Apache 1.3 API, this module might crash under EAPI—recompile it with -DEAPI.

  You can ignore this warning. This issue does not impact the functioning of the Web Agent.
- In console mode, when the installation program prompts with a question, the default entry is displayed in brackets **[]**. Press ENTER to accept the default.
- In these procedures, *web_agent_home* refers to the installed location of the SiteMinder Web Agent.
- After installation, you can find the installation log file in *web_agent_home*. The file name is:

  CA_SiteMinder_Web_Agent_*version*_InstallLog.log

More Information

Miscellaneous Web Server Preparations (see page 18)
Environment Variables Added or Modified by the Web Agent Installation (see page 207)

Run a GUI Mode Installation on UNIX

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

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

To run a GUI mode installation on UNIX:

1. Consider the following before you begin:
   - Running a Web Agent GUI-mode installation or running the Configuration Wizard using the Exceed application may cause text in the dialog boxes to be truncated because of unavailable fonts. This limitation has no affect on Web Agent installation and configuration.
   - If you are installing the Web Agent via telnet or other terminal emulation software, you must have an X-Windows session running in the background to run the GUI mode installation. Additionally, you need to set the DISPLAY variable to your terminal, as follows:

     DISPLAY=111.11.1.12:0.0

     export DISPLAY

     If you try to run in GUI mode through a telnet window without an X-Windows session, the installer throws an Java exception and exits.
   - You can also run a command-line installation from a console window.
2. Exit all applications that are running.
3. Ensure that the /tmp directory has at least 300MB of disk space available.
4. Download the installation file from Technical Support.
5. Navigate to the directory for your operating system.
6. Copy the appropriate binary file to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:
   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
7. Depending on your permissions, you may need to add executable permissions to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system-processor-architecture*.bin
8. Open a console window and from the local installation directory enter:

   ./ca-wa-*version-operating_system-processor-architecture*.bin

The installation program prepares the files.

9. In the Introduction dialog box, read the information then click Next.
10. Read the License Agreement then select the radio button to accept the agreement. Click Next.

    If you do not accept the agreement, the installation terminates.
11. Read the notes in the Important Information dialog box, then click Next.
12. In the Choose Install Location dialog box, accept the default location or use the Choose button to select a different location. Click Next.

    If you select a non-default location then want to revert to the default directory, click Restore Default Folder.
13. Review the information in the Pre-Installation Summary dialog box, then click Install.

    The Web Agent files are installed in the specified location.
14. In the Install Complete dialog box, click Done.
15. After installing the Agent, run the Agent Configuration Wizard to register a trusted host and configure the Web Agent.

More information:

Configurations Available for All Web Agents (see page 145)
Register Your System as a Trusted Host on UNIX (see page 62)

Installation and Configuration Log Files

To check the results of the installation or review any specific problems during the installation or configuration of the Web Agent, check the following log files, located in *web_agent_home*\install_config_info:

ca-wa-details.log

Provides specific details on any failures or problems that may have occurred.

CA_SiteMinder_Web_Agent_*version*_InstallLog.log

Provides complete results of the installation, including the components that installed successfully and those that failed.

More information:

Installation History Log File (see page 37)

Run a Console Mode Installation on UNIX

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

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

To run a console mode installation on UNIX

1. Exit all applications that are running and stop the web server.
2. Ensure that the /tmp directory has at least 300MB of disk space available.
3. Download the installation programs from Technical Support.
4. Navigate to the directory for your operating system.
5. Copy the appropriate binary file to a local directory then navigate to that directory.

   Note: The binary files use the following naming conventions:

   - ca-wa-*version-operating_system*.bin (for most versions)
   - ca-wa-*version-operating_system-processor-architecture*.bin (for versions requiring a specific processor or architecture type)
6. Open a console window, and check the permissions on the binary file. You may need to add execute permissions to the install file. For example:

   chmod +x ca-wa-*version-operating_system-processor-architecture*.bin
7. At the command prompt, start the console mode installation by entering:

   ./ca-wa-*version-operating_system-processor-architecture*.bin

   -i console

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

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

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

    Press Enter to page through the notes and continue through the installation.

12. In the Choose Install Location section, specify the location where the installation should place the Agent files. To accept the default location, press Enter.

    If you specify a path, it must contain the word "webagent." If it does not, the installation program will create this folder and append it to the path. For example, if you specify export/ca/wa, the path becomes export/ca/wa/webagent. However, if you specify export/ca/sm_webagent as the path, the installation program will accept this.

13. Review the information in the Pre-Installation Summary, then press Enter to continue. The program begins installing files.

14. When the installation is complete, you will receive a message along with instructions on locating the Configuration Wizard.

15. Press Enter to exit the installer.

16. After installing the Agent, run the Agent Configuration Wizard to register a trusted host and configure the Web Agent.

More information:

Configurations Available for All Web Agents (see page 145)

Unattended Installations on UNIX

After you have installed the Web Agent on one system, you can automate installations on other web servers using the Agent's unattended installation feature. An unattended installation lets you install or uninstall the Web Agent without any user interaction.

An unattended installation uses a properties file that is initially configured with values from the initial GUI or console mode Web Agent installation. Therefore, you can only run an unattended installation on a system with the same platform and web server image as the system where you first installed the Web Agent. For example, you cannot install an Agent on a Solaris system with an Sun Java System web server, then use the properties file to run an unattended installation on a Linux system with an Apache web server.

Prepare an Unattended Installation on UNIX

Unattended installation uses the ca-wa-installer.properties file to propagate the Web Agent installation set up to all Agents in your network. In this properties file, you define installation parameters, then copy the file and the Web Agent executable file to any web server in your network to run an unattended installation.

The ca-wa-installer.properties file is installed in the following location:

web_agent_home/install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation.

To install the ca-wa-installer.properties file

1. Run an initial installation of the Web Agent.
2. Open the ca-wa-installer.properties file and modify the parameters.

   The parameters are as follows:

Parameter	Meaning
USER_SHORTCUTS	Specifies where the Web Agent configuration shortcut should be installed. Enter the path to the desired location. (Windows only)
USER_INSTALL_DIR	Specifies the installed location of the Web Agent. Enter the full path to the installation directory.
USER_REQUESTED_RESTART	Indicates whether the installation program should reboot a Windows machine if required. Set to YES to allow the reboot. (Windows only)

3. Save the file.

Run an Unattended Installation on UNIX

You should have completed an initial Web Agent installation and, if necessary, modified the ca-wa-installer.properties file. Now, you can use the file to run subsequent Web Agent installations.

To run an unattended Web Agent installation

1. From a system where the Web Agent is already installed, copy the following files to a local directory:
   a. ca-wa-*version-operating_system*.bin (Agent executable) from where it resides on your system.
   b. Copy the ca-wa-installer.properties file from *web_agent_home*/install_config_info.
2. Open a console window and navigate to the directory where you copied the two files.
3. Run the installation executable with the -f and - i silent options, as follows:

   agent_binary -f *properties_file* -i silent

   Note: If you are not at the directory where these files reside, you must specify the full path to each file.

   Assuming that you run the installation from the directory where the executable and properties file are located, the command would be:

   ./ca-wa-*version-operating_system*.bin -f ca-wa-installer.properties -i silent

   When the installation is complete, you return to the command prompt.
4. CA_SiteMinder_Web_Agent _*version*_InstallLog.log file, located in the *web_agent_home*/install_config_info directory. This log file contains the results of the installation.
5. Register the trusted host and configure the Web Agent.

More Information

How to Configure Any Web Agent in Unattended Mode (see page 145)

Stop an Unattended Installation in Progress on UNIX

To manually stop the installation, press Ctrl + C.

Set the Web Agent Environment Variables After Installation

You can set the Web Agent environment variables after installing the Web Agent using the ca_wa_env.sh script Running the script for Web Agents installed on most UNIX platforms ensures that the Web Agent and web server can work together. The script sets environment variables required by the Web Agent.

The ca_wa_env.sh script has been enhanced to set the following environment variables:

- NETE_WA_ROOT
- PATH
- NETE_WA_PATH
- LD_LIBRARY_PATH

  Note: The Web Agent requires that LD_LIBRARY_PATH include /usr/lib before any other directory containing older versions of libm.so.
- SHLIB_PATH
- LIBPATH

To set the Web Agent environment variables after installation, source the following script after you install and configure the Web Agent:

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

You can list the script in either the user .profile file or envvars file. You must source this script if you are upgrading a Web Agent from v6.x QMR 1.

Note: You do not have to run this script for Sun Java System web servers because this file as been added to the start script.

Set Web Agent Variables when using apachectl Script

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

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

1. Locate a line resembling the following example:

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

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

   sh /*web_agent_home*/ca_wa_env.sh

   web_agent_home

   Indicates the directory where the Web Agent is installed.

   Default (Windows installations): C:\Program Files\CA\webagent

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

Installation History Log File

The installer creates a log file with following information:

- The product name
- The installed location
- The complete (full) version number

This file is created in the following location:

Windows

C:\Program Files\CA\install-info\ca-install-history.log

UNIX

/opt/ca/install-info/ca-install-history.log

More information:

Installation and Configuration Log Files (see page 41)

Reinstall a Web Agent on UNIX

You can reinstall a Web Agent to restore missing application files. For this procedure, you do not need to uninstall the existing Web Agent; simply perform a reinstall over the existing Web Agent files by repeating the installation procedure.

To reinstall the Web Agent on UNIX, use the following process:

1. Make copies of your Web Agent configuration settings to have as a back up.
2. Install the Web Agent on your UNIX system using the GUI installer.

   During the reinstallation, you must confirm the reinstall by one of the following:

   - A Reinstall dialog box (GUI mode)
   - A Confirm Upgrade/Reinstall prompt (Console mode)

Register Your System as a Trusted Host on UNIX

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

To establish a connection between the trusted host and the Policy Server, you need to register the host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. After this file is successfully created, the client computer becomes a trusted host.

Note: You only register the host once, *not* each time you install and configure a Web Agent on your system.

You can register the trusted host immediately after installing the Web Agent or at a later time; however, you must perform the registration at some point.

You can run the Registration Tool independently from GUI or Console mode.

More Information

How to Configure Any Web Agent in Unattended Mode (see page 145)

Register a Trusted Host in GUI or Console Mode

These instructions are for GUI and Console Mode registration. The steps for the two modes are the same, with the following exceptions for Console mode:

- You may be instructed to select an option by entering a corresponding number for that option.
- You press Enter after each step to proceed through the process. The prompts should guide you through the process.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

To register a host

1. If necessary, start the Configuration Wizard as follows:
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI Mode: ./ca-wa-config.bin

      Console Mode: ./ca-wa-config.bin -i console

   The Configuration Wizard starts.
2. In the Host Registration dialog box:
   a. Select Yes to register a host now or No to register the host at a later time.
   b. If you are using PKCS11 cryptographic hardware in your SiteMinder environment, select the check box.
   c. Click Next.
3. If you enabled cryptographic hardware, complete the fields. If not, skip to the next step.
   a. In the PKCS11 DLL field, enter the full path to the PKCS11 DLL. Click on Choose to search for the DLL.
   b. Optionally, specify the token label in the Token Label and Token Passphrase, if applicable. Re-confirm the passphrase in the Confirm token passphrase field then click Next.
4. Complete the following fields in the Admin Registration dialog box, then click Next:
   - Admin User Name—enter the name of the administrator allowed to register the host with the Policy Server.

     This administrator should already be defined at the Policy Server and have the permission Register Trusted Hosts set. The default administrator is SiteMinder.

- Admin Password—enter the administrator's password.
- Confirm Admin Password—re-enter the password.
- Enabled Shared Secret Rollover—check this box to periodically change the shared secret used to encrypt communication between the trusted host and the Policy Server. Key rollover must be enabled at the Policy Server for this feature to work.

  Important: If you enable shared secret rollover, the user who owns the web server process must have permissions to write to the SmHost.conf file. If this file cannot be modified by this user, then the shared secret rollover cannot be updated.

  For example, for Sun Java System and Apache web servers, the person specified by the User directive needs write permission to the SmHost.conf file. If the SmHost.conf file is owned by User1 and no other user has write permissions, the shared secret rollover is not written to the SmHost.conf file if User2 owns the server process.

5. In the Trusted Host Name and Configuration Object dialog box, enter values for the two fields then click Next.

   a. In the Trusted Host Name field, enter a unique name that represents the trusted host to the Policy Server. This name *does not* have to be the same as the physical client system that you are registering; it can be any unique name, for example, mytrustedhost.

      Note: This name must be unique among trusted hosts and not match the name of any 4.x Web Agent. It can be the same name as a 5.0 Web Agent, but this is not recommended.

   b. In the Host Configuration Object field, enter the name of the Host Configuration Object specified in the Policy Server, then click Next.

      This object defines the connection between the trusted host and the Policy Server. To use the default, enter DefaultHostSettings. In most cases, you will use your own Host Configuration Object.

      Note: The entry you specify must match the Host Configuration Object entry set at the Policy Server.

6. In the Policy Server IP Address dialog box:

   a. Enter the IP address, or host name, and the authentication port of the Policy Server where you are registering the host. The default port is 44442. If you do not provide a port, the default is used.

      You can specify a non-default port number, but if you are using a nondefault port and you omit it, SiteMinder displays the following error:

      Registration Failed (bad ipAddress[:port] or unable to connect to Authentication server (-1))

Note also that if you specify a non-default port, that port is used for the Policy Server's authentication, authorization, and accounting ports; however, the unified server responds to any Agent request on any port. The entry in the SmHost.conf file will resemble:

policyserver="*ip_address*,5555,5555,5555"

b. Click Add.

You can add more than one Policy Sever; however, for host registration, only the first server in the list will be used. If you add multiple entries, separate them by a comma.

If multiple Policy Servers are specified, the Agent uses them as bootstrap servers. When the Agent starts up, the Web Agent has several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap Policy Server is no longer used by that server process. The Host Configuration Object can contain another set of servers, which may or may not include any of the bootstrap servers.

c. Click Next.

7. If you want to use FIPS encryption, choose one of the following options:

FIPS Compatibility Mode (Default)

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

FIPS Migration Mode

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

FIPS Only Mode

Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using only FIPS 140-2 algorithms.

Important! A SiteMinder r12.0 SP2 installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

If you are not using FIPS encryption, use the default value.

8. Click Next.

9. Accept the default location of the host configuration file, SmHost.conf or click Choose to select a different location. Click Next.

   If you select a non-default location then want to revert to the default directory, click Restore Default Folder.

   The host is registered and a host configuration file, SmHost.conf, is created in *web_agent_home*/config. You can modify this file.

10. Configure your Web Agent.

Modify the SmHost.conf File (UNIX)

Web Agents and custom Agents act as trusted hosts by using the information in the SmHost.conf file to locate and make initial connections to a Policy Server. Once the Agent connects to the Policy Server, the initial connections are closed. Any further communication between the Agent and the Policy Server is based on settings in the Host Configuration Object that is located on the Policy Server.

You can modify portions of the SmHost.conf file to change the initial Agent-to-Policy Server connection.

To modify the SmHost.conf file

1. Navigate to the *web_agent_home*/config directory.
2. Open the SmHost.conf file in a text editor.
3. Enter new values for the any of the following settings that you want to change:

   Important! Change only the settings of the parameters listed here. Do not modify the settings of any other parameters in the SmHost.conf file.

   hostconfigobject

   Specifies the host configuration object that defines connectivity between the Agent that is acting as trusted host and the Policy Server. This name must match a name defined in the Administrative UI.

   If you want to change the host configuration object an object so the Web Agent u, you need to modify this setting.

   Example: hostconfigobject="*host_configuration_object*"

   policyserver

   Specifies the Policy Server to which the trusted host will try to connect. The proper syntax is as follows:

   "*IP_address*, *port*,*port*,*port*"

   The default ports are 44441,44442,44443, but you can specify non-default ports using the same number or different numbers for all three ports. The unified server responds to any Agent request on any port.

   To specify additional bootstrap servers for the Agent, add multiple Policy Server entries to the file. Multiple entries provide the Agent with several Policy Servers to which it can connect to retrieve its Host Configuration Object. After the Host Configuration Object is retrieved, the bootstrap servers are no longer needed for that server process.

   Multiple entries can be added during host registration or by modifying this parameter. If a Policy Server is removed from your SiteMinder environment or is no longer in service, delete the entry.

Important: If an Agent is configured on a multi-process web server, specifying multiple Policy Server entries is recommended to ensure that any child process can establish a connection to the secondary Policy Server if the primary Policy Server fails. Each time a new child process is started, it will not be able to initialize the Web Agent if only one Policy Server is listed in the file and that Policy Server is unreachable.

Default: *IP_address*, 44441,44442,44443

Example (Syntax for a single entry)**:** "*IP_address*, *port*,*port*,*port*"

Example (Syntax for multiple entries, place each Policy Server on a separate line)**:**
policyserver="123.122.1.1, 44441,44442,44443"
policyserver="111.222.2.2, 44441,44442,44443"
policyserver="321.123.1.1, 44441,44442,44443"

requesttimeout

Specifies an interval of seconds during which the Agent that is acting as a trusted host waits before deciding that a Policy Server is unavailable. You can increase the time-out value if the Policy Server is busy due to heavy traffic or a slow network connection.

Default: 60

Example: requesttimeout="60"

4. Save and close the SmHost.Conf file.

   The changes to the SmHost.conf file are applied.

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

When you install a Web Agent on a server for the first time, you are prompted to register that server as a trusted host. After the trusted host is registered, you do not have to re-register with subsequent Agent installations. There are some situations where you may need to re-register a trusted host independently of installing an Agent, such as the following:

- To rename the trusted host if there has been a change to your SiteMinder environment.
- To register a trusted host if the trusted host has been deleted in the Administrative UI.
- To register a trusted host if the trusted host policy objects have been deleted from the policy store or the policy store has been lost.
- To change the shared secret that secures the connection between the trusted host and the Policy Server.
- To recreate the SmHost.conf configuration file if it is lost.
- To overwrite an existing trusted host without deleting it first.

The registration tool, smreghost, re-registers a trusted host. This tool is installed in the *web_agent_home*/bin directory when you install a Web Agent.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To re-register a trusted host using the registration tool

1. Open a command prompt window.
2. Ensure that the library path environment variable contains the path to the Web Agent's bin directory.
3. Enter the following two commands:

   library_path_variable=${*library_path_variable*}:*web_agent_home*/bin

   export *library_path_variable*

   For example, for Solaris systems enter the following two commands:

   LD_LIBRARY_PATH=${LD_LIBRARY_PATH}:/usr/ca/webagent/bin

   export LD_LIBRARY_PATH

   The following list shows the different variables for each operating system:

   Solaris

   LD_LIBRARY_PATH

HP-UX

SHLIB_PATH

LINUX

LD_LIBRARY_PATH

AIX

LIBPATH

4. Enter the smreghost command using the following required arguments, as shown in the following example:

   smreghost -i *policy_server_IP_address:[port]*

   -u *administrator_username* -p *Administrator_password*

   -hn *hostname_for_registration* -hc *host_configuration_ object*

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

   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A" -hc DefaultHostSettings

   Example with the -o argument:

   smreghost -i 123.123.1.1 -u SiteMinder -p mypw -hn "host computer A" -hc DefaultHostSettings -o

   The following arguments are used with the smreghost command:

   -i *policy_server_IP_ address:port*

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

   If you specify a port number, which can be a non-default port, that port is used for all three Policy Server servers (authentication, authorization, accounting), however, the unified server responds to any Agent request on any port. For example, if you specify port 55555, the policy server entry in the SmHost.conf file will show the following:

   "*policy_server_ip_address*,5555,5555,5555"

   Example: (IPv4) 127.0.0.1,44442

   Example: (IPv6) [2001:DB8::/32][:44442]

   -u *administrator_username*

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

-p *Administrator_password*

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

-hn *hostname_for_registration*

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

-hc *host_config_object*

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

-sh *shared_secret*

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

-rs

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

-f *path_to_host_config_file*

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

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

-cf *FIPS mode*

Specifies one of the following FIPS modes:

- COMPAT--Specifies non-FIPS mode, which lets the Policy Server and the Agents read and write information using the existing SiteMinder encryption algorithms. If your organization does not require the use of FIPS-compliant algorithms, the Policy Server and the Agents can operate in non-FIPS mode without further configuration.
- MIGRATE--Specifies FIPS-migration mode, which is used when you are upgrading an earlier version of SiteMinder to full-FIPS mode. The Policy Server and the Agents continue to use the existing SiteMinder encryption algorithms as you migrate your environment to use only FIPS 140-2 approved algorithms.
- ONLY--Specifies full-FIPS mode, which requires that the Policy Server and Web Agents read and write information using *only* FIPS 140-2 algorithms.

Important! A SiteMinder r12.0 SP2 installation that is running in Full FIPS mode cannot interoperate with, or be backward compatible to, earlier versions of SiteMinder, including all agents, custom software using older versions of the Agent API, and custom software using PM APIs or any other API that the Policy Server exposes. You must re-link all such software with the r12.0 SP2 versions of the respective SDKs to achieve the required support for Full FIPS mode.

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

Default: COMPAT

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

-cp *cryptographic_provider*

(Optional) Indicates the name of the cryptographic provider you are using for encryption. If you do not specify a value the default is assumed.

Default: ETPKI

-cd *crypto_provider_DLL_or_configuration_file_path*

(Required for PKCS11 encryption) Indicates the full path to the PKCS11 DLL or configuration file.

-ct *crypto_provider_token_label*

(Optional for PKCS11 encryption) Indicates the token label for the hardware token. Only use this argument if there is a token label.

-ck *crypto_provider_token_pin*

(Required for PKCS11 encryption) Indicates the passphrase for the token.

-o

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

The trusted host is re-registered.

Register Multiple Trusted Hosts on One System (UNIX)

You typically register only one trusted host for each machine where web servers and Agents are installed. However, you can register multiple trusted hosts on one computer to create distinct connections for each SiteMinder client. Using multiple trusted hosts ensures a unique shared secret and a secure connection for each client requiring communication with the Policy Server.

For most installations this is not a recommended configuration. However, it is an option for sites who require distinct, secure channels for each client or group of client applications protected by SiteMinder Agents. For example, an application service provider may have many client computers with different applications installed. You may want a secure connection for each application, which you can achieve by registering multiple trusted hosts. The Policy Server then issues unique shared secrets for each client connection.

To register multiple trusted hosts, use one of the following methods:

- Registering with the Configuration Wizard: To register additional servers as trusted hosts, go through the registration process again; however, when prompted to specify a location for the SmHost.conf file, enter a unique path. Do not register a new host and use an existing web server's SmHost.conf file or that file will be overwritten. You can use the name SmHost.conf or give the file a new name.

  Note: If you have registered a trusted host with a Policy Server and you run the Configuration Wizard to configure subsequent Agents without using a unique path for the SmHost.conf file, you will see a warning message in the Host Registration dialog box. The message reads:

  "Warning: You have already registered this Agent with a Policy Server."

- Registering with the smreghost command-line tool: Run the smreghost tool after you have completed the first Agent installation on a given computer. You can run this tool for each trusted host that you want to register.

Files Installed for Registration Services (UNIX)

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

Virtual Directories

- siteminderagent/dmspages
- siteminderagent/dmsforms

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

Physical Directories

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

- *web_agent_home*/samples

  Contains files used by Registration Services that you can customize.

- *web_agent_home*/samples_default

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

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

The following table describes each directory.

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

Chapter 4: Upgrade a Web Agent to r12.0 SP2

This section contains the following topics:

How to Prepare for a Web Agent Upgrade (see page 77)
Upgrade a Web Agent to r12.0 SP2 on Windows Systems (see page 79)
Upgrade a Web Agent to r12.0 SP2 on UNIX Systems (see page 81)

How to Prepare for a Web Agent Upgrade

You can prepare for upgrading a Web Agent using the following process:

1. Review the upgrade process in the *SiteMinder Upgrade Guide*.
2. Back up any customized files on your web server.
3. Review the Password Services and Form Template changes that occur during the upgrade.
4. Review the changes to the various Web Agent configuration files that occur when you run the Web Agent Configuration wizard *after* an upgrade.
5. Set the LD_PRELOAD variable to avoid conflicts with existing Web Agents.
6. Replace existing read-only files during the upgrade (if prompted).

Review the Upgrade Procedure

Before upgrading a Web Agent, you should review the upgrade process in the *SiteMinder Upgrade* Guide. This guide contains important overview information as well as critical tasks that you should complete *before* upgrading a Web Agent.

Note: If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation.

Back Up Customized Files

Customized files may be overwritten by the upgrade. Back up configured files, such as Agent and Host configuration files *before* upgrading.

Password Services and Forms Template Changes During Upgrades

For Password Services and forms templates, the jpw_default, pw_default, and samples_default directories are upgraded. However the non-default versions of these directories (jpw, pw, and samples), which may contain customized files, will not be modified in any way.

Results of Running the Configuration Wizard After an Upgrade

When you run the Web Agent Configuration Wizard after upgrading the Web Agent, the following occurs:

- SiteMinder saves a copy of the current Web Agent configuration file (WebAgent.conf).
- SiteMinder moves the IgnoreExt and BadURLCharacters lines into the new WebAgent.conf file as commented lines, so that you can easily add your custom elements.

Note: SiteMinder does not save a copy of the Trusted Host configuration file (SmHost.conf).

Ensure LD_PRELOAD Variable Does Not Conflict with Existing Agent

If you are upgrading or reinstalling a Web Agent on a Linux system, from the shell, set the LD_PRELOAD variable so that it points to a different location from any existing Web Agent installation directory. For example, if an existing LD_PRELOAD entry is set to:

LD_PRELOAD=*web_agent_home*/bin/libbtunicode.so

Before you reinstall or upgrade, set the variable to:

export LD_PRELOAD=

This entry sets the variable to a blank value.

Replace Existing Read-only Files

When you upgrade a Web Agent, you may see messages asking whether you want to replace read-only files. Select Yes to all.

Upgrade a Web Agent to r12.0 SP2 on Windows Systems

The executable on the SiteMinder media upgrades your existing SiteMinder Web Agents to r12.0 SP2, provided the web server version has not changed since the last installation of the Web Agent.

If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation. However, you can upgrade if you have applied a hotfix.

Important! Remove any 5.x Web Agent Option Packs before upgrading to r12.0 SP2. 6.x Web Agent Option Packs do not need to be removed before upgrading to r12.0 SP2. For more information about removing and reinstalling Web Agent Option Packs, see the SiteMinder Web Agent Option Pack Guide.

Consider the following:

- If the installation program detects any locked Agent files, it prompts you to restart your system instead of reconfiguring it. Select whether to restart the system immediately or later.
- If you are installing an Agent on an Sun Java System web server, you may see an error message stating that the httpd.exe service is unable to locate the smconapi.dll. If this message appears, reboot your system before launching the Web Agent Configuration Wizard.

To upgrade Web Agents on Windows

1. Exit all applications that are running and stop the web server.
2. Download the installation program from Technical Support.
3. Navigate to the win32 folder and double-click the ca-wa-*version_number*-win32.exe file.

   The Installation Wizard starts.
4. In the Introduction dialog box, read the information then click Next.
5. Read the License Agreement. Click the radio button to accept the terms of the license agreement, and then click Next.
6. Read the notes in the Important Information dialog box, then click Next.
7. Select the placement of the Agent Configuration Wizard shortcut in the Choose Shortcut Folder dialog box then click Next.

   To allow all users access to the Configuration Wizard via the shortcut, select the Create Icons for All Users check box. Otherwise, clear the check box.

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

8. In the Confirm Upgrade dialog box, select one of the following options, and then click Next:
   - Continue with the upgrade—upgrades the Web Agent to r12.0 SP2.
   - Abort the upgrade—exits the upgrade procedure without upgrading the Web Agent.
9. In the Pre-installation Summary dialog box, confirm that the installation settings are correct, then click Install.

   The new Web Agent files are copied to the specified location.

   Note: The installation program may detect that newer versions of certain system .dlls are installed on your system. If you are prompted to overwrite these newer files with older files, click No To All.
10. In the Install Complete dialog box, choose whether to restart your system immediately or later. Then click Done.
11. Re-configure your upgraded web agent with the Web Agent Configuration Wizard.

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

Upgrade a Web Agent to r12.0 SP2 on UNIX Systems

The executable on the SiteMinder media upgrades your existing SiteMinder Web Agents to r12.0 SP2, provided the web server version has not changed since the last installation of the Web Agent.

If you have upgraded the web server itself since you last installed the Web Agent, the Agent upgrade may not work. The upgrade is ensured only if the web server version has remained the same since the last Web Agent installation. However, you can upgrade if you have applied a hotfix.

Important! Remove any 5.x Web Agent Option Packs before upgrading to r12.0 SP2. 6.x Web Agent Option Packs do not need to be removed before upgrading to r12.0 SP2. For more information about removing and reinstalling Web Agent Option Packs, see the SiteMinder Web Agent Option Pack Guide.

To upgrade a Web Agent on UNIX systems

Note: If you are upgrading an existing r12 Web Agent to r12 SP1, you must login as the root user. If you are installing a new r12 SP1 Web Agent, root privileges are not required.

1. Exit all applications that are running and stop the web server.
2. Download the installation program from Technical Support.
3. Navigate to the appropriate directory for your operating system.
4. Copy the appropriate binary file to a local directory then navigate to that directory. The file names use the following convention:

   ca-wa-*version-operating_system*.bin
5. Depending on your permissions, you may need to add executable permissions to the installation file by running the chmod command, for example:

   chmod +x ca-wa-*version-operating_system*.bin
6. Open a console window and from the location of the installation program enter:

   ./ca-wa-*version-operating_system*.bin
7. In the Introduction dialog box, read the information then click Next.
8. Read the License Agreement, and then click the radio button to accept the agreement. Click Next.
9. Read the notes in the Important Information dialog box, and then click Next.

   The Confirm Upgrade dialog box is displayed.
10. In the Confirm Upgrade dialog box, select one of the following, and then click Next:

- Continue with the upgrade—upgrades the Web Agent to r12.0 SP2.
- Abort the installation—exits the upgrade procedure without upgrading the Web Agent.

11. In the Pre-installation Summary dialog box, confirm that the installation settings are correct, then click Install.

    The new Web Agent files are copied to the specified location.

12. In the Install Complete dialog box, click Done.

    The Web Agent upgrade is complete. If the system with the 5.x Web Agent being upgraded has *not* previously been registered as a trusted host, you need to register at the system at some point.

Chapter 5: Configure an IIS Web Agent

This section contains the following topics:

How to Configure a SiteMinder Web Agent on IIS 7.0 (see page 83)
How to Configure a SiteMinder Web Agent on IIS 6.0 (see page 91)
How to Configure a SiteMinder Web Agent to Protect Microsoft Outlook Web Access (see page 100)

How to Configure a SiteMinder Web Agent on IIS 7.0

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

1. Verify the following prerequisites:
   - The SiteMinder Web Agent is installed.
   - The computer running the SiteMinder Web Agent was restarted after the installation (*without* running the SiteMinder Web Agent Configuration wizard).
   - The web server (IIS) role is added your web server.
2. Add role services to your IIS 7.0 web server.
3. Run the Web Agent Configuration wizard.
4. Add the handler mappings to any additional web sites that you want to protect with SiteMinder.

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

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

More Information

Agent Configuration Parameters Required for IIS Web Agents (see page 23)

Add Role Services to your IIS 7 Web Server

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

To add role services to your IIS 7 web server

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

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

   The Server Manager opens.

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

   The Add Roles Wizard starts.

3. Use the wizard to add the following role services to your IIS 7 web server:

   - ASP.NET
   - CGI
   - ISAPI Extensions
   - ISAPI Filters

   The role services are added to your IIS web server.

Run the Configuration Wizard for an IIS Web Agent

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

To configure an IIS Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

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

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

2. If you have registered the trusted host, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

3. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

4. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, enter IISDefaultSettings to use the default.

5. If you want to configure Registration Services for DMS2, select Yes. If not, select No.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Registration Services:

a. Select a servlet engine to be configured for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

   The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

   The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

   The Web Agent files are installed.

7. Click Done when the installation is complete.

8. Enable the Web Agent:

   a. Open the WebAgent.conf file located in *web_agent_home*\bin\IIS

      Example: C:\Program Files\CA\webagent\bin\IIS

   b. Set the value of the EnableWebAgent parameter to yes.

   c. Save the file and restart the web server.

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

More Information

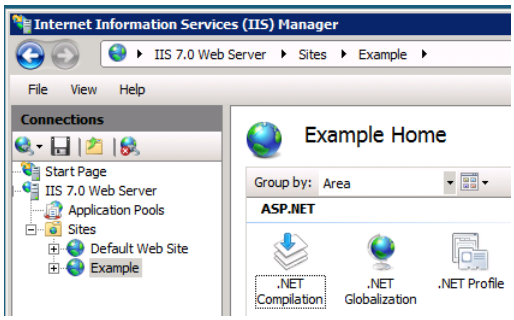
Install a Web Agent on a Windows System (see page 31)

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

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

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

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



To add a handler mapping to additional web sites

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

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

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

   The Sites folder appears.

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

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

   A list of the installed handler mappings appears.

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

   The Add Wildcard Script Map dialog appears.

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

   The Open dialog appears.

7. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgent.DLL

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

8. Click Open.

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

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

10. Click OK.

    A confirmation dialog appears.

11. Click Yes.

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

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

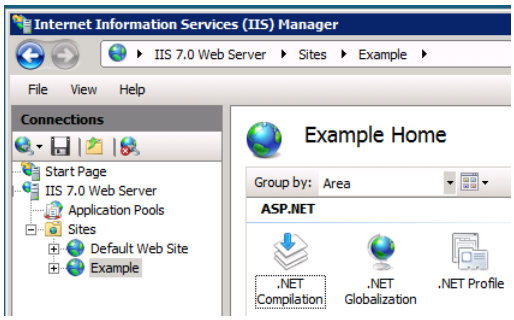
    The handler mappings are added.

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

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

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

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



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

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

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

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

   The Sites folder appears.

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

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

   The ISAPI Filters screen appears.

5. Under the actions pane, click Add.

   The Add ISAPI Filter dialog appears.

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

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

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgent.DLL

9. Click Open.

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

10. Click OK.

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

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

How to Configure a SiteMinder Web Agent on IIS 6.0

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

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

More Information

Agent Configuration Parameters Required for IIS Web Agents (see page 23)

Assign Read Permissions to Samples and Error Files Directories

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

To Assign Read Permissions to the Samples and Error Files Directories

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

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

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

Allow IIS to Execute the Agent ISAPI and CGI Extensions

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

To add the extensions and permissions

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

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

      The New Web Service Extension dialog box opens.
   b. In the Extension name field, enter ISAPI6WebAgentDLL, and then click Add.

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

      web_agent_home

      Indicates the directory where the Web Agent is installed.

      Default (Windows installations): C:\Program Files\CA\webagent

      Default (UNIX installations): /opt/ca/webagent
   d. Click Open

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

      You return to the New Web Service Extension dialog box.
   f. Select the Set extension status to allowed check box.
   g. Click OK.

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

- *web_agent_home*/pw_default/smpwservicescgi.exe (suggested extension name: PW Default CGI)

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

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

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

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

Increase the Agent's Size Limit for Uploaded Files

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

To upload files that are larger than this limit

1. Open the registry editor.

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

2. Navigate to the following location:

   HKEY_LOCAL_MACHINE\SOFTWARE\ca\SiteMinder Web Agent\Microsoft IIS

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

   MaxRequestAllowed

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

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

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

5. Close the registry editor.

   The size limit is changed.

Run the Configuration Wizard for an IIS Web Agent

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

To configure an IIS Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

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

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

2. If you have registered the trusted host, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

3. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

4. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, enter IISDefaultSettings to use the default.

5. If you want to configure Registration Services for DMS2, select Yes. If not, select No.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Registration Services:

a. Select a servlet engine to be configured for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

   The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

   The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

   The Web Agent files are installed.

7. Click Done when the installation is complete.

8. Enable the Web Agent:

   a. Open the WebAgent.conf file located in *web_agent_home*\bin\IIS

      Example: C:\Program Files\CA\webagent\bin\IIS

   b. Set the value of the EnableWebAgent parameter to yes.

   c. Save the file and restart the web server.

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

More Information

Install a Web Agent on a Windows System (see page 31)

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

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

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

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

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

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

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

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

a. Open the IIS Manager, and then expand the web server.

b. Right-click the Default Web Site folder, and select Properties.

c. Click the Home Directory tab, and then click Configuration.

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

web_agent_home\bin\ISAPI6WebAgent.dll

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

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

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

Note: See the SiteMinder r12.0 SP2 Product Support Matrix at http://ca.com/support to determine which versions of this component are supported.

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

      Note: The Microsoft Exchage Server and Web Access Client components can be installed on the same system, or on separate systems. Only one Web Agent is required if both are installed on the same system. If the components are installed on different systems, then two Web Agents are used. When different systems are used, the Exchange Server acts as a back-end system, while the Web Access Client acts as a front-end system.
   c. A SiteMinder Policy Server with the following:
      - A Microsoft Active Directory used for a policy-store and user-directory.
      - A SQL Server database instance used for a session server.
      - Persistent sessions enabled for the realms (r6.x) or applications (r12.0 SP2) associated with the Microsoft Outlook Web Access resources you want to protect.
2. Perform the following steps on the IIS web server that hosts your Microsoft Exchange Server:
   a. Confirm the SiteMinder ISAPI filter appears first in the list.
   b. Allow IIS to Execute the Outlook Extensions.
   c. Set the Default Web Site Home directory location and Execute Permission settings.
   d. Add the ISAPI extension to Exchange Web Site.
   e. Set Directory Security for Exchange Web Site.
   f. Set the ISAPI Extension for Exchweb Virtual Site.
   g. Set the Directory Security for Exchweb Virtual Site.
   h. Set the Owa Web Site Home directory location and Execute Permission settings.

3. Repeat Steps 2a through 2g on the IIS web server that hosts your Microsoft Outlook Web Access Client.
4. Confirm that SiteMinder is protecting the Outlook Web Access web site.

Confirm the SiteMinder ISAPI filter appears first in the list

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

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

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

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

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

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

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

a. Open the IIS Manager, and then expand the web server.

b. Right-click the Default Web Site folder, and select Properties.

c. Click the Home Directory tab, and then click Configuration.

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

web_agent_home\bin\ISAPI6WebAgent.dll

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

- **Default** (UNIX installations): /opt/ca/webagent

Allow IIS to Execute the Outlook Extensions

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

To allow IIS to execute the Outlook extensions

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

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

Set the Default Web Site Directory Location and Execute Permissions

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

To set the default web site directory location and execute permissions

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

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

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

Add the ISAPI Extension to the Exchange Web Site

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

To add the ISAPI extension to the Exchange web site

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

   A list of web sites appears.

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

   The Exchange Properties dialog appears.

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

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

4. Click Configuration.

   The Application Configuration dialog appears.

5. Click Insert.

   The Add/Edit Extension Mapping dialog appears.

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

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

7. Click Open.

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

8. Clear the Verify that file exists check box.

9. Click OK.

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

10. Click OK.

    The Application Configuration dialog closes.

11. Click OK.

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

Set the Directory Security for the Exchange Web Site

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

To set the directory security for the Exchange web site

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

   A list of web sites appears.

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

   The Exchange Properties dialog appears.

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

   The Authentication Methods dialog closes.

8. Click OK.

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

Add the ISAPI Extension to the Exchweb Web Site

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

To add the ISAPI extension to the Exchweb web site

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

   A list of web sites appears.

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

   The Exchweb Properties dialog appears.

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

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

4. Click Configuration.

   The Application Configuration dialog appears.

5. Click Insert.

   The Add/Edit Extension Mapping dialog appears.

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

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

7. Click Open.

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

8. Clear the Verify that file exists check box.

9. Click OK.

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

10. Click OK.

    The Application Configuration dialog closes.

11. Click OK.

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

Set the Directory Security for the Exchweb Web Site

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

To set the directory security for the Exchweb web site

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

   A list of web sites appears.

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

   The Exchweb Properties dialog appears.

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

   The Authentication Methods dialog closes.

8. Click OK.

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

Set the Default Web Site Directory Location and Execute Permissions

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

To set the owa web site directory location and execute permissions

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

   The owa Web Site Properties dialog appears.

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

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

Confirm that SiteMinder is protecting the Outlook Web Access web site

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

Confirm that SiteMinder is protecting the Outlook Web Access web site

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

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

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

   The Inbox appears.

Chapter 6: Configure a Sun Java System Web Agent

This section contains the following topics:

Run the Configuration Wizard on Windows (see page 112)
Configure Sun Java System Web Agents Using GUI or Console Mode (see page 115)
Manually Configure a Sun Java System Web Server (see page 119)
Apply Changes to Sun Java System Web Server Files (see page 120)

Run the Configuration Wizard on Windows

To configure the Web Agent on an Sun Java System web server

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you have placed the Wizard shortcut in a non-default location, the procedure will be different.

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

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

2. If you have already done host registration, skip to the next step. If not, select No in the Host Registration dialog box to skip registration, then click Next.

   To register a trusted host, go to the installation chapter for your platform.

3. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

4. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter iPlanetDefaultSettings.

5. If applicable, select one of the advanced SSL authentication schemes listed in the SSL Authentication dialog box. If the Agent is not providing advanced authentication, select No advanced authentication. Click Next.

   The selections are:

   - HTTP Basic over SSL—identifies a user based on a user name and password. The credential delivery is always done over an encrypted Secure Sockets Layer (SSL) connection.

- X509 Client Certificate—identifies a user based on X.509 V3 client certificates. Digital certificates act as a signature for a user. Certificate authentication uses SSL communication.
- X509 Client Cert and HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified **and** he or she must provide a valid user name and password.
- X509 Client Cert or HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified, or he or she must provide a valid user name and password.
- X509 Client Cert or Form—The X.509 Client Certificate or HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **or** the user must provide the credentials requested by an HTML form.
- X509 Client Cert and Form—The X.509 Client Certificate and HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **and** the user must provide the credentials requested by an HTML form.

Note: For additional information about advanced authentication schemes, see the *Policy Server Configuration* Guide.

6. If you want to configure Self Registration for DMS2, select Yes. If not, select No.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Self Registration:

   a. Select a servlet engine to be set up for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

   b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

      The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

      The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

The Web Agent files are installed and the Configuration Complete dialog box displays.

8. Click Done to exit the Configuration Wizard.
9. Enable the Web Agent:
   a. Open the WebAgent.conf file, located in:

      Sun_Java_System_server_home\servers\https-*hostname*\config

   b. Set the EnableWebAgent parameter to Yes.
   c. Save the file.
10. Apply changes to Sun Java System Web Server files. This is required for the Agent's configuration to take effect.

More Information

Apply Changes to Sun Java System Web Server Files (see page 120)

Configure Sun Java System Web Agents Using GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Sun Java System Web Server, you enter a 3, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To configure the Web Agent on a Sun Java System Web Server

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI mode: **.**/ca-wa-config.bin

      Console mode: ./ca-wa-config.bin -i console
2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.
3. In the Select Web Server(s) dialog box, select the option for the iPlanet or Sun ONE Web Server and click Next.
4. Specify the root path where the Sun Java System web server is installed and click Next. For example, /opt/iPlanet/servers.

   You can click Choose to locate the root directory.
5. Select the web server instances that you want to configure with Web Agents.

If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

a. Select one of the following:

   Overwrite—to overwrite the server instance configuration.

   Preserve—to preserve the web server's configuration.

   Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter iPlanetDefaultSettings.

7. If applicable, select one of the advanced SSL authentication schemes listed in the SSL Authentication dialog box. If the Agent is not providing advanced authentication, select No advanced authentication. Click Next following your choice.

   The selections are:

   - HTTP Basic over SSL—identifies a user based on a user name and password. The credential delivery is always done over an encrypted Secure Sockets Layer (SSL) connection.
   - X509 Client Certificate—identifies a user based on X.509 V3 client certificates. Digital certificates act as a signature for a user. Certificate authentication uses SSL communication.
   - X509 Client Cert and HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified **and** he or she must provide a valid user name and password.
   - X509 Client Cert or HTTP Basic—combines X.509 Client Certificate and Basic authentication. The user's X.509 client certificate must be verified, or he or she must provide a valid user name and password.
   - X509 Client Cert or Form—The X.509 Client Certificate or HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **or** the user must provide the credentials requested by an HTML form.

- X509 Client Cert and Form—The X.509 Client Certificate and HTML Forms authentication scheme combines the use of X.509 Client Certificates and the use of customized HTML forms to collect authentication information. Using this scheme, the user's X.509 client certificate must be verified **and** the user must provide the credentials requested by an HTML form.

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

8. If you want to configure Self Registration for DMS2, select Yes. If not, select No.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Self Registration:

   a. Select a servlet engine to be configured for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

   b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

      The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

      The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

   The Web Agent files are installed and the Configuration Complete message is displayed.

10. Click Done when the installation is complete.

11. Enable the Web Agent:

    a. Open the WebAgent.conf file, located in

       Sun_Java_System_server/servers/https-*hostname*/config

    b. Set the value of the EnableWebAgent parameter to Yes.

    c. Save the file.

    d. Restart the web server.

12. Apply changes to the Sun Java System Web Server files. This is required for the Agent's configuration to take effect.

More Information

Apply Changes to Sun Java System Web Server Files (see page 120)

Manually Configure a Sun Java System Web Server

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

- Servers installed in a non-default directory
- Servers you want to configure as a reverse proxy (we recommend configuring the reverse proxy using your Sun Java System interface before adding the SiteMinder settings to the obj.conf file).
- Virtual servers on the same computer

To manually configure a Sun Java System Web Server

1. Locate the directory of the server instance you want to configure.
2. Open the obj.conf file with a text editor.
3. Locate the following line:

   ```
   <Object name="default">
   ```

4. Insert a new line below the previous one, and then add the following text:

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

5. Locate the following line:

   ```
   AuthTrans fn="match-browser" browser="*MSIE*" ssl-unclean-shutdown="true"
   ```

6. Insert a new line below the previous one, and then add the following text:

   ```
   NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi" dir="web_agent_home/pw" name="cgi"
   NameTrans fn="pfx2dir" from="/siteminderagent/pw" dir="web_agent_home/pw"
   NameTrans fn="pfx2dir" from="/siteminderagent/jpw" dir="web_agent_home/jpw"
   NameTrans fn="pfx2dir" from="/siteminderagent/redirectjsp"
   dir="web_agent_home/affwebservices/redirectjsp"
   NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" dir="web_agent_home/samples"
   NameTrans fn="pfx2dir" from="/siteminderagent" dir="web_agent_home/samples"
   ```

   web_agent_home

   Indicates the directory where the Web Agent is installed.

   Default (Windows installations): C:\Program Files\CA\webagent

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

7. Locate the following line:

   ```
   NameTrans fn="ntrans-j2ee" name="j2ee"
   ```

8. Insert a new line below the previous one, and then add the following text:

   ```
   PathCheck fn="SmRequireAuth"
   ```

9. Remove the following line:

   NameTrans fn="pfx2dir" from="/mc-icons" dir="C:/Program Files/Sun/WebServer7/lib/icons" name="es-internal"

10. Locate the following line:

    ObjectType fn="force-type" type="text/plain"

11. Insert a new line below the previous one, and then add the following text:

    Service method="(GET|POST)" fn="SmAdvancedAuth"

12. Save the obj.conf file.

    The Sun Java System web server is manually configured.

Apply Changes to Sun Java System Web Server Files

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

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

To apply changes to the Sun Java System configuration files

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

   You will see a warning message about loading the modified configuration files.

4. Click Load Configuration Files.
5. Exit the console.
6. Restart the web server.
7. Optimize the Sun Java System Web Agent by tuning the shared memory segments.

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

More Information

Settings Added to the Sun Java System Server Configuration (see page 189)
Tune the Shared Memory Segments (see page 152)

Chapter 7: Configure an Apache Web Agent

This section contains the following topics:

Configure an Apache Web Agent on Windows Systems (see page 124)
Configuration Methods for Apache Web Agents on UNIX Systems (see page 126)
Improve Server Performance with Optional httpd.conf File Changes (see page 130)
Set the LD_PRELOAD Variable for Apache Agent Operation (see page 130)
Set the LD_ASSUME_KERNEL for Apache Agent on SuSE Linux 9 for zSeries (see page 132)
Enabling SHLIB Path for an Agent on Apache 2.0/HP-UX 11 (see page 133)
Configure Apache for Oracle 9.0.2/9.0.3 HTTP Server (see page 133)

Configure an Apache Web Agent on Windows Systems

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

To configure the Apache Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you've placed the Wizard shortcut in a non-default location, the procedure will be different.

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

2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.

3. In the Select Web Server(s) dialog box, select the radio button for the Apache Web Server and click Next.

4. In the Apache Web Server Path dialog box, specify the Apache web server root.

   If you installed the Agent on an Apache-based server, such as an IBM HTTP Server, or Oracle server, the Web Agent may not recognize the path. In this case, the Configuration Wizard displays the Apache Web Server Failure dialog box with the following options:

   - I would like to re-enter the Apache Server Root.

     Select this option for an Apache web server and re-enter the root path.

   - I would like to enter a specific configuration path.

     Select this option if you are using an Apache-based web server (such as, IBM HTTP, HP Apache-based, or Oracle). You are prompted to enter the full configuration path to the web server root.

   - I don't have an Apache web server.

     Choose this option to skip Apache configuration and continue with the Agent configuration.

   Click Next.

5. Following the server root path, specify the version of Apache you are using. Select from these two options:

   - Apache version 1.0
   - Apache version 2.0

6. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.

7. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter ApacheDefaultSettings.

8. If you want to configure Self Registration for DMS2, select Yes. If not, select No and go to Step 9.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Self Registration:

   a. Select a servlet engine to be configured for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

   b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

      The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

      The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

   The Web Agent files are installed.

10. Click Done when the installation is complete.

11. Enable the Web Agent:

    a. Open the WebAgent.conf file, located as follows:

Apache_home\conf

where *Apache_home* is the installed location of the Apache web server.

b. Set the EnableWebAgent parameter to Yes.

c. Save and close the file.

12. Restart the web server.

When you run the Configuration Wizard for the Apache Web Agent, it makes changes to the Web Server's httpd.conf file and to the library path.

For httpd.conf changes to take effect, you need to restart the web server.

More Information

Configuration Changes to Web Servers with Apache Web Agent (see page 197)
Configure an Apache Web Agent (see page 123)

Configuration Methods for Apache Web Agents on UNIX Systems

The following configuration methods are available for Web Agents on UNIX systems:

- GUI mode
- Console mode
- Unattended mode

Notes:

- For the IBM HTTP web server, HP Apache-based web server, and Oracle HTTP web server, the Apache Web Agent is the Agent you should have installed. All the information for the Apache web server applies to those web servers also.
- Before you configure the Agent, you may want to register the system as a trusted host; however, you can do this at a later time.

More Information

Configure an Apache Web Agent Using GUI or Console Mode (see page 127)
How to Configure Any Web Agent in Unattended Mode (see page 145)

Configure an Apache Web Agent Using GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Apache Web Server, you enter a 1, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To configure the Apache Web Agent

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI mode: **.**/ca-wa-config.bin

      Console mode: ./ca-wa-config.bin -i console
2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.
3. In the Select Web server(s) dialog box, select the option for the Apache Web Sever and click Next.
4. In the Apache Web Server Path dialog box, specify the Apache Web Server root, for example, /opt/apache2. Click Next.

   If you installed the Agent on an Apache-based server, such as an IBM HTTP Server, or Oracle server, the Web Agent may not recognize the path. In this case, the Configuration Wizard displays the Apache Web Server Failure dialog box with the following options:

   - I would like to re-enter the Apache Server Root.

     Select this option for an Apache web server and re-enter the root path.
   - I would like to enter a specific configuration path.

Select this option if you are using an Apache-based web server (such as IBM HTTP, HP Apache-based, or Oracle). You are prompted to enter the full configuration path to the web server root.

- I don't have an Apache web server.

  Choose this option to skip Apache configuration and continue with the Agent configuration.

Click Next.

5. Following the server root path, specify the version of Apache you are using. Select from these two options:
   - Apache version 1.0
   - Apache version 2.0
6. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.

   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

      Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

   b. Click Next.
7. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter ApacheDefaultSettings.
8. If you want to configure Self Registration for DMS2, select Yes. If not, select No.

   A servlet engine is required to run Self Registration. If the Web Agent Configuration Wizard does not detect a servlet engine, the Select Servlet Engine for Registration dialog box is not displayed.

   If you selected Yes to configure Self Registration:

   a. Select a servlet engine to be configured for the web server. If you do not see your engine displayed, select Other Advanced server. Click Next.

   b. In the Self Registration Services Admin Account dialog box, identify the the DMS Administrator by provide values for the Admin User Name, Admin Password and Admin Confirm Password fields and click Next.

The user name and password that you enter here must match the DMS Admin values you set at the Policy Server.

The DMS Administrator account secures DMS requests that are performed outside of the scope of a DMS administrator, such as self-registration. The user name and encrypted password for the account are stored in the dms.properties file on the Web Agent.

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

   The Web Agent files are installed.

10. Click Done when the installation is complete.
11. Enable the Web Agent:
    a. Open the WebAgent.conf file, located as follows:

       Apache_home/conf

    b. Set the EnableWebAgent parameter to yes.
    c. Save and close the file.
12. Restart the web server.

    When you run the Configuration Wizard for the Apache Web Agent, it makes changes to the Web Server's httpd.conf file and to the library path.

    For httpd.conf changes to take effect, you need to restart the web server.

13. For Apache on UNIX systems, optimize the Apache Web Agent by tuning the shared memory segments.

More Information

Configuration Changes to Web Servers with Apache Web Agent (see page 197)
Configure an Apache Web Agent (see page 123)
Tune the Shared Memory Segments (see page 152)

Improve Server Performance with Optional httpd.conf File Changes

You can improve server performance by modifying the default configuration settings in the httpd.conf file; however, these changes are *not* required:

To improve server performance with optional httpd.conf file changes

1. For Apache and Sun Java System servers, assign a higher priority level to your Apache20WebAgent.dll file than any other auth or access modules installed in your server's configuration.
2. For low-traffic websites, define the following directives:
   - Set MaxRequestsPerChild>1000 *or* Set MaxRequestsPerChild=0
   - MinSpareServers >5
   - MaxSpareServers>10
   - StartServers=MinSpareServers>5
3. For high-traffic websites, define the following directives:
   - Set MaxRequestsPerChild>3000 *or* Set MaxRequestsPerChild=0
   - MinSpareServers >10
   - MaxSpareServers>15
   - StartServers=MinSpareServers>10

Note: CA Services can provide assistance with performance-tuning for your particular environment.

Set the LD_PRELOAD Variable for Apache Agent Operation

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

More Information

Set the LD_PRELOAD Variable for an Oracle 10G Web Server on Linux (see page 131)
Set the LD_PRELOAD Variable for SSL Configuration on an IBM HTTP Server 2.0.47/Linux AS 3.0 System (see page 131)

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

After you install the Web Agent r12.0 SP2 on an Oracle 10G web server running on a Linux platform, you must set the LD_PRELOAD environment variable in the apachectl script.

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

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

   LD_PRELOAD=*web_agent_home*/bin/libbtunicode.so

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

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

Set the LD_PRELOAD Variable for SSL Configuration on an IBM HTTP Server 2.0.47/Linux AS 3.0 System

When configuring SSL on an IBM HTTP Server 2.0.47.1 running SUSE8, ikeyman, the graphical user interface for the IBM key management utility, crashes when it is used to create a key database.

To resolve this issue, set the following environment variable:

export LD_PRELOAD=/usr/lib/libstdc++-libc6.2-2.so.3

After setting this variable, the key database file, key.kdb, is created successfully.

Set LD_PRELOAD for Using X.509-based Auth Schemes with Domino 6.5.3/SuSe8 Linux System

When accessing resource protected with any X.590-based Authentication Schemes on Domino 6.5.3/SuSe8 Linux, the Domino Server Crashes and generates an NSD.

To resolve this issue, set the following environment variable before starting the Domino Web Server:

export LD_PRELOAD=/usr/lib/libstdc++-libc6.2-2.so.3

Set the LD_ASSUME_KERNEL for Apache Agent on SuSE Linux 9 for zSeries

After you install the Web Agent on an Apache web server running on SuSE Linux 9 for zSeries, set the LD_ASSUME_KERNEL environment variable as follows:

```
LD_ASSUME_KERNEL=2.4.21
export LD_ASSUME_KERNEL
```

Important! You must set this variable to 2.4.21 because it represents the kernel release upon which the Web Agent libraries are built.

Without this setting, the following problems occur:

- The Apache web server will not start properly.
- Host registration dumps core.

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

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

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

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

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

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

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

Configure Apache for Oracle 9.0.2/9.0.3 HTTP Server

Oracle HTTP Server (OHS) is based on the Apache Web Server and is protected using the Apache Web Agent.

Prerequisites:

- Before you configure the Apache Agent for OHS, you should have already installed the Oracle Server 9.0.2/9.0.3 on a system running Solaris 9 or HP-UX 11i.
- For HP-UX 11i systems, install patch a C++ runtime A.03.30 or later before installing the Oracle server.

To configure the Apache Web Agent for Oracle HTTP Server, you must:

1. Optionally, Install a Server Certificate (Required for SSL Only). For SSL-enabled Oracle HTTP Servers, you must install a server certificate using the Oracle Wallet Manager application. For more information, see the documentation supplied with your Oracle HTTP Server.
2. Configure the Apache Web Agent for the Oracle Server
3. Restart the Web Server as follows:
   a. Stop the Web server from *OHS_home*/dcm/bin by executing the command:

      dcmctl stop

   b. Restart the Web Server by executing the command:

      dcmctl start –ct ohs –v

Note: When you configure an Apache Web Agent on an Oracle HTTP Server, the Configuration Wizard makes changes to the server's httpd.conf file.

Chapter 8: Configure a Domino Web Agent

This section contains the following topics:

Configure a Domino Web Agent on Windows Systems (see page 135)
How to Configure a Domino Web Agent on UNIX Systems (see page 139)

Configure a Domino Web Agent on Windows Systems

To configure a Domino Web Agent on Windows systems, perform the following tasks:

- Add the Domino Web Agent DLL
- Run the Web Agent Configuration Wizard
- (Optional) Configure the CGI directory and CGI URL Path Settings
- (Optional) Configure alias settings to enable HTML Forms authentication schemes

Add the Domino Web Agent DLL (Windows)

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

To add the Domino Web Agent DLL

1. Open Lotus Notes.
2. Select File, Database, Open.
3. In the Server field, select the Domino Server where you installed the Web Agent.
4. In the Database scroll box, select the server's address book.

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

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

   The Domino server's administration console opens.
8. Select the Internet Protocols tab.
9. In the DSAPI section of the window, find the DSAPI filter file names field and enter the full path to the Domino Web Agent DLL, for example:

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

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

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

Run the Configuration Wizard for a Domino Web Agent on Windows

Before you configure the Agent, you may want to register the system where the Agent is installed as a trusted host; however, you can do this at a later time.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To configure a Domino Web Agent

1. If necessary, start the Web Agent Configuration Wizard.

   The default method is to select Start, Programs, SiteMinder, Web Agent Configuration Wizard. If you've placed the Wizard shortcut in a non-default location, the procedure will be different.

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

2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   For information on registering the trusted host, see the installation chapter for your platform.

3. In the Select the Web server(s) dialog box, select the radio button for the Domino Web Sever and click Next.

4. In the Domino Web Server Path dialog box, specify the location of the notes.ini file, such as C:\Lotus\Domino\notesdata, then click Next.

   Note: The installation automatically writes the path to the WebAgent.conf in the notes.ini file.

5. Select the Web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional Web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the Web servers that you have previously configured.

   a. Select one of the following:

      - Overwrite--replaces the existing configuration of server instance with the new one.
      - Preserve--keeps the existing web server's configuration without changing it.

Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this Web server instance, then click Next.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter DominoDefaultSettings.

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

   The Web Agent files are installed.

8. Click Done when the installation is complete.

9. Enable the Web Agent:

   a. Open the WebAgent.conf file, located in where you installed the Domino Web server root directory.

   b. Set the EnableWebAgent parameter to YES.

   c. Save the file.

More Information

Agent Configuration Parameters Required for Domino Web Agents (see page 22)
Register Your System as a Trusted Host on UNIX (see page 62)

(Optional) Configure the CGI Directory and CGI URL Path Settings

To configure appropriate cgi-bin (ScriptAlias) settings for the Domino Web Agent, navigate to Internet Protocols tab for your server configuration in the Domino Administrator and configure the following settings:

- CGI directory: domino\html\cgi-bin
- CGI URL path: /cgi-bin

(Optional) Configure Alias Settings to Enable Forms and Other HTML Authentication Schemes

To configure the Domino Web Agent to support HTML Forms authentication schemes perform the following tasks:

1. Create a subdirectory named "siteminderagent" in the Domino document root (\domino\html\) directory.
2. Copy all the subdirectories of *agent_home*\samples to the siteminderagent directory you created in Step 1.

   agent_home

   Specifies the SiteMinder Web Agent installation path.
3. To support X.509 Client Certificate and HTML Forms authentication schemes, additionally create a directory named "certoptional" in the siteminderagent directory you created in Step 1 and also copy all the subdirectories of *agent_home*\samples into it.

How to Configure a Domino Web Agent on UNIX Systems

To configure a Domino Web Agent on Windows systems, perform the following tasks:

- Add the Domino Web Agent DLL
- Run the Web Agent Configuration Wizard
- (Optional) Configure the CGI directory and CGI URL Path Settings
- (Optional) Configure Alias settings to enable HTML Forms authentication schemes

Add the Domino Web Agent DLL (UNIX)

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

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

To add the Domino Web Agent DLL

1. Open Lotus Notes.
2. Select File, Database, Open.
3. In the Server field, select the Domino Server where you installed the Web Agent.
4. In the Database scroll box, select the server's address book.

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

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

   The Domino server's administration console opens.
8. Select the Internet Protocols tab.
9. In the DSAPI section of the window, find the DSAPI filter file names field and enter the full path to the Domino Web Agent file, for example:

   web_agent_home>/bin/dominowebagent.so

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

Configuration Methods for Domino Web Agents on UNIX Systems

The following configuration methods are available for Web Agents on UNIX systems:

- GUI mode
- Console mode
- Unattended mode

More Information

How to Configure Any Web Agent in Unattended Mode (see page 145)
Register Your System as a Trusted Host on UNIX (see page 62)

Configure Domino Web Agents in GUI or Console Mode

These instructions are for GUI and Console Mode configuration. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number. For example, to select the Apache Web Server, you enter a 1, which corresponds to this server.
- Press ENTER after each step to proceed through the process instead of "clicking Next," as stated in the following procedure.
- All passwords that you enter are displayed in clear text. To workaround this issue, run the installation in GUI or unattended mode.

The prompts for each mode will help guide you through the process.

1. If necessary, start the Configuration Wizard.
   a. Open a console window.
   b. Navigate to *web_agent_home*/install_config_info
   c. Enter one of the following commands:

      GUI mode: **.**/ca-wa-config.bin

      Console mode: ./ca-wa-config.bin -i console

   Note: If you chose to configure the Web Agent immediately after the installation, SiteMinder automatically starts the Configuration Wizard.
2. If you have already done host registration, skip to the next step. Otherwise, select the option to skip host registration, then click Next.

   To register the trusted host, go to the installation chapter for your platform.
3. In the Select the Web server(s) dialog box, select the radio button for the Domino Web Sever and click Next.
4. In the Domino Web Server Path dialog box, specify the location of the notes.ini file, such as /local/notesdata, then click Next.

   Note: The installation automatically writes the path to the WebAgent.conf in the notes.ini file.
5. Select the web server instances that you want to configure with Web Agents.

   If you have already configured a server with a Web Agent and you are running the Configuration Wizard to configure additional web servers instances, the Wizard displays the Select One or More Instances to Overwrite dialog box. This dialog box lists the web servers that you have previously configured.
   a. Select one of the following:

      Overwrite—to overwrite the server instance configuration.

      Preserve—to preserve the web servers configuration.

Important! If you uncheck a previously configured server, the Web Agent will be removed from this server.

b. Click Next.

6. In the Agent Configuration Object field, enter the name of the Agent Configuration Object for this web server instance.

   This name must match an Agent Configuration Object already defined at the Policy Server. For example, to use the default enter DominoDefaultSettings.

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

   The Web Agent files are installed.

8. Click Done when the installation is complete.

9. Enable the Web Agent:

   a. Open the WebAgent.conf file, located in the Domino web server root directory.

   b. Set the EnableWebAgent parameter to Yes.

   c. Save the file.

10. If your Domino web server runs on AIX, you must enable run time linking after configuring your agent (you only need to do this once) with the following steps:

    a. Run the following commands:

    ```
    cd domino_server_path/lotus/notes/latest/ibmpow
    /usr/bin/rtl_enable ./http -brtl
    mv ./http ./http.orig
    mv ./http.new ./http
    ```

    b. Start the Domino web server.

(Optional) Configure the CGI Directory and CGI URL Path Settings

To configure appropriate cgi-bin (ScriptAlias) settings for the Domino Web Agent, navigate to Internet Protocols tab for your server configuration in the Domino Administrator and configure the following settings:

- CGI directory: domino/html/cgi-bin
- CGI URL path: /cgi-bin

(Optional) Configure Alias Settings to Enable Forms and Other HTML Authentication Schemes

To configure the Domino Web Agent to support HTML Forms authentication schemes perform the following tasks:

1. Create a subdirectory named "siteminderagent" in the Domino document root (/domino/html) directory.
2. Copy all the subdirectories of *agent_home/*samples to the siteminderagent directory you created in Step 1.

   agent_home

   Specifies the SiteMinder Web Agent installation path.
3. To support X.509 Client Certificate and HTML Forms authentication schemes, additionally create a directory named "certoptional" in the siteminderagent directory you created in Step 1 and also copy all the subdirectories of *agent_home/*samples into it.

Chapter 9: Configurations Available for All Web Agents

This section contains the following topics:

How to Configure Any Web Agent in Unattended Mode (see page 145)
Check SmHost.conf File Permissions for Shared Secret Rollover (see page 148)
Reconfigure a Web Agent (see page 148)
How to Set Up Additional Agent Components (see page 149)

How to Configure Any Web Agent in Unattended Mode

After you have installed the Web Agent on one system, you can automate the Web Agent configuration on other web servers using the Agent's unattended configuration feature. An unattended configuration lets you configure the Web Agent without any user interaction.

To configure any Web Agent in unattended mode, use the following process:

1. Prepare an unattended configuration.
2. Run an unattended configuration.

Prepare an Unattended Configuration

Unattended configuration uses the ca-wa-installer.properties file to propagate the Web Agent configuration set up across all Agents in your network. For configuration, you define configuration parameters in the properties file, then copy the file to any web server in your network to run an unattended configuration.

When you perform an initial Web Agent installation and configuration, the ca-wa-installer.properties file is installed in the following location:

web_agent_home/install_config_info

The default parameters and paths in the file reflect the information you entered during the initial Web Agent installation and configuration.

To make the ca-wa-installer.properties file available on your system

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

More Information

Install a Web Agent on a UNIX System (see page 51)
Install a Web Agent on a Windows System (see page 31)

Run an Unattended Configuration

Before you run an unattended configuration, you should have completed the following tasks:

- an initial (attended) Web Agent installation
- an initial (attended) Web Agent configuration
- modification of the ca-wa-installer.properties file

  You use this file to run subsequent unattended Web Agent configurations
- an installation (attended or unattended) on the system where you want to run the unattended configuration. This installation makes the configuration executable available.

To run an unattended Web Agent configuration

1. From a system where the Web Agent is already installed, copy the ca-wa-installer.properties file from *web_agent_home*/install_config_info to a local directory on the system where you want to run an unattended configuration.
2. Open a console window and navigate to *web_agent_home*/install_config_info.

   Important! If you are running a SiteMinder utility or executable on Windows Server 2008, be sure to open the command–line window with Administrator permissions, even if you are logged into the system as an Administrator. For more information, see the release notes for your SiteMinder component.

   Note: You must run the unattended configuration from the install_config_info directory because the configuration executable file must remain in this directory.
3. Run the following command:

   agent_config_executable -f *properties_file* -i silent

   For example, if you copied the properties file to the install_config_info directory, the command would be:

   Windows:

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

   UNIX:

   ca-wa-config.bin -f ca-wa-installer.properties -i silent

   If you do not copy the properties file to the install_config_info directory, specify the full path to this file in the command. If there are spaces in the directory path, enclose the entire path between quotation marks.

   When the configuration is complete, you return to the command prompt.
4. Check to see if the configuration completed successfully by looking in the CA_SiteMinder_Web_Agent_*version*_InstallLog.log file, located in the *web_agent_home*/install_config_info directory. This log file contains the results of the configuration.

Check SmHost.conf File Permissions for Shared Secret Rollover

If you enable shared secret rollover, the user who owns the web server process must have permissions to write to the SmHost.conf file. If this file cannot be modified by this user, then the shared secret rollover cannot be updated.

For example, for Sun Java System and Apache web servers, the person specified by the User directive needs write permission to the SmHost.conf file. If the SmHost.conf file is owned by User1 and no other user has write permissions, the shared secret rollover cannot be updated if User2 owns the server process.

Reconfigure a Web Agent

Reconfigure a Web Agent for the following reasons:

- You have upgraded the Web Agent and now you need to update the configuration
- You need to change the configuration settings previously defined for a Web Agent
- You need to remove the configuration settings from the Web Agent without uninstalling the entire Web Agent (you would need to configure the Web Agent again at a later time)
- You want to configure the Web Agent for a different Web Server installed on the same system as the configured server.

To reconfigure a Web Agent in any mode, re-run the Configuration Wizard. There are no additional steps or prompts for reconfiguring an Agent.

More Information

Configure an IIS Web Agent (see page 83)
Configure a Sun Java System Web Agent (see page 111)
Configure an Apache Web Agent (see page 123)
Configure a Domino Web Agent (see page 135)

How to Set Up Additional Agent Components

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

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

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

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

- Configuring an Agent as a forms credential collector

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

- Configuring an Agent as an SSL credential collector

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

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

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

Chapter 10: Operating System Tuning

This section contains the following topics:

Tune the Shared Memory Segments (see page 152)
How to Tune the Solaris 10 Resource Controls (see page 154)

Tune the Shared Memory Segments

If you install an Apache or Sun Java System Web Agent on Solaris or HP-UX systems, you must tune the operating system's shared memory settings for the Web Agent to function correctly. By increasing the operating system's shared memory segments, you improve the performance of the Web Agent. The variables that control shared memory segments are defined in the operating system's specification file.

For AIX operating systems, you must run the following command before starting an Apache server:

```
export EXTSHM=ON
```

Note: You may need to tune the shared memory segments if you are using Linux. For more information about the shared memory segments and how to tune them, see the documentation for your particular operating system.

To increase shared memory segments

1. Follow the appropriate procedure for your operating system:
   - Solaris**:** Open the /etc/system file, using the editor of your choice.
   - HP-UX: Start the System Administration Manager (SAM) utility
2. Modify the shared memory variables using *one* of the following methods:
   - Solaris: Add the variables shown in the following list and configure them using the recommended settings shown in the examples. Use the following syntax:

     ```
     set shmsys:shminfo_shmmax=33554432
     ```

   - HP-UX: Using the SAM utility, select Kernel Configuration, Configurable Parameters. SAM displays a set of variables. Highlight and modify each one in the following list using the recommended settings shown in the examples.

   shmsys:shminfo_shmmax

   Specifies the maximum shared memory segment size. Controls the maximum size of the Agent resource and session cache.

   Note: To estimate the amount of memory segments required, allocate 4KB/entry in each cache, or view cache usage statistics in the OneView Monitor. See the *Web Agent Configuration* Guide for more information about using the OneView Monitor.

   Example: 33554432 (32 mb) for busy sites that need large cache capacity.

   shmsys:shminfo_shmmin

   (Not required for Solaris) Minimum shared memory segment size. Controls the minimum size of the Agent resource and session cache.

shmsys:shminfo_shmmni

Specifies the maximum number of shared memory segments that can exist simultaneously, system-wide.

Example: (except Apache 1.x/Solaris 9) N/A

Example: (Apache 1.x/Solaris 9) 200

shmsys:shminfo_shmseg

(Not required for Solaris 9) Specifies the maximum number of shared memory segments per process.

Example: 24

semsys:seminfo_semmni

Specifies the number of semaphore identifiers. Use 11 for every instance of the Agent that you run on the system.

Example: (except Apache 1.x/Solaris 9) 100

Example: (Apache 1.x/Solaris 9) 200

semsys:seminfo_semmns

Specifies the number of semaphores in the system. Use 10 for every instance of the Agent that you run on the system.

Example: (except Apache 1.x/Solaris 9) 100

Example: (Apache 1.x/Solaris 9) 400

semsys:seminfo_semmnu

Specifies the number of processes using the undo facility. For optimal performance, semmnu should be greater than the number of Apache child processes or Sun Java System processes running on the system at any one time. For Apache servers, this value should exceed the maxclients setting by 200 or more. For Sun Java System servers, this value should exceed the maxprocs setting by 200 or more.

Example: (except Apache 1.x/Solaris 9) 200

Example: (Apache 1.x/Solaris 9) 400

3. Save your changes then exit the file or the utility.
4. Reboot the system.
5. Verify your changes by entering the command:
   ```
   $ sysdef -i
   ```

How to Tune the Solaris 10 Resource Controls

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

Note: See your Solaris documentation for more information.

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

1. Determine the project associated with the user account under which the Web Agent runs.
2. Increase the settings for any of the following resource controls of that project:

   project.max-shm-ids

   Specifies the maximum shared memory IDs for a project.

   project.max-sem-ids

   Specifies the maximum number of semaphore IDs for a project.

   project.max-msg-ids

   Specifies the maximum number of message queue IDs for a project.

   project.max-shm-memory

   Specifies the total amount of shared memory allowed for a project.

   process.max-sem-nsems

   Specifies the maximum number of semaphores allowed per semaphore set.

   process.max-sem-ops

   Specifies the maximum number of semaphore operations allowed per semop.

   process.max-msg-messages

   Specifies the maximum number of messages on a message queue.

   process.max-msg-qbytes

   Specifies the maximum number of bytes of messages on a message queue.

Chapter 11: Password Services

This section contains the following topics:

Password Services Implementations (see page 155)
How to Set Up Your Environment for JSP Password Services (see page 156)
How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server (see page 157)
How to Configure the ServletExec Servlet Engine for JSP Password Services on a Sun Java System Web Server in the UNIX Operating Environment (see page 158)

Password Services Implementations

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

The following mechanisms are available for implementing password management:

Password Services CGI

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

FCC-based Password Services

Implements Password Services using SiteMinder forms.

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

Password Services servlet

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

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

How to Set Up Your Environment for JSP Password Services

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

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

   web_agent_home\jpw\jpw.jar
   web_agent_home\Java\servlet.jar
   web_agent_home\Java\jsafe.jar

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

   /siteminderagent/pwservlet/PSWDChangeServlet=PSWDChangeServlet

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

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

More Information

How to Configure the ServletExec Servlet Engine for JSP Password Services on a Sun Java System Web Server in the UNIX Operating Environment (see page 158)
How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server (see page 157)

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

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

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

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

   web_agent_home\jpw\jpw.jar

   web_agent_home\java\jsafe.jar

   web_agent_home

   Indicates the directory where the Web Agent is installed.

   Default (Windows installations): C:\Program Files\CA\webagent

   Default (UNIX installations): /opt/ca/webagent
3. Make the following modifications to the top-level web.xml file of your web application.
   a. Add the following servlet:.
      - Servlet Name: PSWDChangeServlet
      - Servlet Class: PSWDChangeServlet

   b. Create the following servlet mapping:
      - URL pattern: /siteminderagent/pwservlet/PSWDChangeServlet
      - Servlet Name: PSWDChangeServlet
4. Repeat Step 3 for each web.xml file of your web application.

How to Configure the ServletExec Servlet Engine for JSP Password Services on a Sun Java System Web Server in the UNIX Operating Environment

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

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

      web_agent_home

      Indicates the directory where the Web Agent is installed.

      Default (Windows installations): C:\Program Files\CA\webagent

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

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

      /siteminderagent/pwservlet/PSWDChangeServlet and Servlet Name: PSWDChangeServlet

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

      web_agent_home/jpw/jpw.jar

      web_agent_home/java/jsafe.jar

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

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

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

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

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

   a. Add the following servlets:

      - Servlet Name: PSWDChangeServlet
      - Servlet Class: PSWDChangeServlet

   b. Add the following Servlet Alias:

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

5. Make the following changes to the magnus.conf file of the Sun Java System server instance on which your Web Agent runs:

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

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

6. Add the following entry to the obj.conf file the Sun Java System server instance on which your Web Agent runs:

   NameTrans fn="assign-name" from="/siteminderagent/pwservlet/PSWDChangeServlet" name="*instance_name*"

   Insert the entry into the following block:

   <Object name="default">

   AuthTrans fn="SiteMinderAgent"

   NameTrans fn="assign-name" from="/servlet/*" name="*instance_name*"

   NameTrans fn="assign-name" from="/siteminderagent/pwservlet/PSWDChangeServlet"

   name="*instance_name*"

   </Object>

7. Restart the Sun Java System web server, and then start the ServletExec Servlet engine.

Chapter 12: Uninstall a Web Agent

This section contains the following topics:

Notes About Uninstalling Web Agents (see page 161)
Set JRE in PATH Variable Before Uninstalling the Web Agent (see page 162)
Uninstall a Web Agent from a Windows System (see page 163)
Uninstall a Web Agent from a UNIX System (see page 164)

Notes About Uninstalling Web Agents

Be aware of the following:

- All Web Agents for all installed web servers will be uninstalled.
- The Password Services and Forms directories, (pw_default, jpw_default, samples_default) will be removed. However, the non-default copies of these directories (pw, jpw, samples) are not removed because these directories may contain customized files.
- Make sure that the JRE is installed on the Web Agent system, as it is needed for uninstallation. For a supported version, see the SiteMinder r12.0 SP2 Platform Matrix at Technical Support.

Set JRE in PATH Variable Before Uninstalling the Web Agent

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

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

To set the JRE in the PATH variable:

On Windows

a. Go to the Control Panel.

b. Double-click System.

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

   For example, C:\j2sdk1.5.0_01\jre\bin

On Solaris

Run these two commands:

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

   where *JRE* is the location of your JRE.

   For example, /usr/bin/j2sdk1.5.0_01/jre

b. export PATH

Uninstall a Web Agent from a Windows System

Before you uninstall, you may want to make copies of your registry settings and Web Agent configuration settings to have as a back up.

To uninstall a Web Agent from a Windows system

1. Stop the web server.
2. Click Start, Control Panel, Add/Remove Programs.

   The Add/Remove Programs dialog appears.
3. Scroll through the program list and select CA SiteMinder Web Agent *version*.
4. Click Change/Remove.

   The uninstallation wizard appears.
5. Review the information in the Uninstall SiteMinder Web Agent dialog box, then click Uninstall.
6. When the uninstallation is finished, the dialog box displays, choose whether to reboot your system now or later then click Done.
7. Restart your web server.

   The Web Agent is uninstalled.

Uninstall Documentation from a Windows System

Running the documentation uninstallation program removes the manuals for all products from the ca_documents directory.

To uninstall the documentation

1. Stop the web server.
2. Open the Control Panel.
3. Select Add/Remove Programs.
4. Scroll through the program list and select CA SiteMinder Documentation *version* for Web Agent.
5. Click Change/Remove.
6. Review the information in the dialog box to confirm the uninstallation.
7. Click Uninstall.

   The documents are removed.
8. Click Done to exit the installer.

Uninstall a Web Agent from a UNIX System

These instructions are for GUI and Console Mode uninstallation.

Note: Removing a Web Agent from a 64-bit Suse Linux 10 system requires additional preparations.

The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number.
- Press Enter after each step to proceed through the process instead of "clicking Next," as stated in the following procedure. The prompts for each mode will help guide you through the process.

Note: Before you uninstall, you may want to make copies of your Web Agent configuration settings to have as a back up.

1. Stop the web server.
2. Log into the UNIX system.
3. Specify the JRE in the PATH environment variable to uninstall the Web Agent. If you receive an error message that the Java virtual machine could not be found, add the JRE to the PATH variable as follows:

   PATH=/*jre_home*/bin:${PATH}

   export PATH

   jre_home is the location of the JRE
4. Navigate to the directory where the Web Agent is installed: *web_agent_home*/install_config_info/ca-wa-uninstall
5. If necessary, ensure you have execute permissions on the uninstallation program by entering chmod +x uninstall.
6. From a console window, enter one of the following commands:
   - GUI mode: ./uninstall
   - Console mode: ./uninstall -i console

   The uninstallation program starts.
7. Read the information in the dialog box to confirm the removal of the Web Agent, then click Uninstall. The Web Agent is removed from the system.
8. Click Done to exit the uninstallation program.
9. Optionally, if you are uninstalling an Apache Web Agent, remove the lines from the httpd.conf file that the Configuration Wizard added.
10. Change to your home directory (the current directory has been deleted).

11. Restart the web server(s).

Note: For Sun Java System web servers, the obj.conf, magnus.conf, and mime.types files are restored to its original settings prior to the Web Agent installation.

Uninstall Documentation from UNIX Systems

These instructions are for GUI and Console Mode uninstallation. The steps for the two modes are the same, with these exceptions for Console Mode:

- You may be instructed to select an option by entering a corresponding number.
- Press Enter after each step to proceed through the process instead of "clicking Next," as stated in the following procedure. The prompts for each mode help guide you through the process.

To uninstall documentation from UNIX systems

1. Navigate to the following directory:

   documentation_home/install_config_info/ca-wa-doc-uninstall

2. Enter one of the following commands:
   - GUI mode: ./uninstall
   - Console mode: ./uninstall -i console

   The uninstallation program begins and displays a dialog box to confirm the uinstallation.

3. Click Uninstall.

   The documentation is removed.

4. Click Done to exit the installer.

To reinstall the documentation, run the appropriate documentation program for the product.

Chapter 13: Troubleshooting

This section contains the following topics:

Agent Start-Up/Shutdown Issues (Framework Agents Only) (see page 167)
Connectivity and Trusted Host Registration Issues (see page 171)
General Installation Issues (see page 172)
Miscellaneous Issues (see page 176)
Sun Java System Web Agent Issues (see page 177)
Apache Web Agent Issues (see page 178)
Domino Web Agent Issues (see page 180)

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

If the Web Agent does not start after installation or you cannot shut it down, check the following error logs:

- On Windows, check the Event Viewer's Application Log.
- On UNIX, messages are processed by the server's standard error handling. For the Apache 2.0, errors are written to the web server error log.
- On Windows or UNIX, run the Low Level Agent Worker Process (LLAWP) to isolate the problem.

Agent Won't Start Because LLAWP is Already Running or Log Messages not Written to the Correct Log Files

Valid on UNIX

Symptom:

I'm having one or more of the following problems:

- My Web Agent won't start because the LLAWP process is already running.
- My Web Agent starts, however the log messages are being written to the log files of a second agent instance.

Solution:

This problem may occur when multiple disks on the same computer use the same mount point. The Web Agent uses the inode of a directory to allocate system resources, and if the inodes are the same, resource collisions and errors result. To fix this problem, use the following process:

1. Create a new subdirectory on your web server (this creates a unique inode).
2. Change the path shown in the ServerPath parameter of the Web Agent so it points to the new subdirectory.

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

Troubleshoot Agent Start-Up/ShutDown with LLAWP

If the Agent is not starting or shutting down properly, you can run the Low Level Agent Worker Process (LLAWP) from the command line.

The LLAWP handles inter-process Agent management. For IIS 6.0, LLAWP starts up after the Web Agent receives the first request. For Apache 2.0, the LLAWP process automatically starts when the Apache web server starts.

By running LLAWP from the command line, you eliminate the web server from the diagnostic process, which isolates Web Agent issues. Error messages are written to the Event log for Windows or to the console on UNIX systems.

Shut Down LLAWP

If the LLAWP process does not shut down properly when shutting down the web server, shut down the LLAWP from the command line. This shuts down the running worker process associated with a WebAgent.conf file.

To shut down the LLAWP, use the command with this syntax:

LLAWP *path_to_WebAgent.conf -web_server_type* -shutdown

For example:

LLAWP /usr/apache/conf/WebAgent.conf -APACHE20 -shutdown

Note: Configuration file names and version strings that contain spaces should be surrounded by quotes, such as "value with spaces."

The LLAWP process will take a few seconds to shut down.

Use the command line to shut the LLAWP down instead of the kill -9 command, so that the process cleans up shared system resources used by the Web Agent.

Web Agent Start Up and Shut Down Issues (IBM HTTP Server)

If the Web Agent does not start after installation or you cannot shut it down, check the following error logs:

- On Windows, check the Event Viewer's Application Log.
- On UNIX, messages are processed by the server's standard error handling.

Stop LLAWP When Stopping IBM HTTP Server 2.0.47

The IBM HTTP Server 2.0.47 on Windows 2000 and 2003 crashes if the ibm_afpa_module and the Web Agent are enabled. If the ibm_afpa_module is loaded and a module registering an init function does not exit that function quickly, the apache.exe child process crashes with an access violation in LIBAPR.dll.

To solve this issue for versions of IBM HTTP Server v2.0.x, if there is an <IfModule mod_afpa_cache.c> line in the httpd.conf file associated with LoadModule ibm_afpa_module, comment out the following lines:

```
#LoadModule ibm_afpa_module modules/mod_afpa_cache.so
#<IfModule mod_afpa_cache.c>
# AfpaEnable
# AfpaCache on
# AfpaPort 8082
# AfpaLogFile "C:/Program Files/IBM HTTP Server 2.0/logs/afpalog"
  V-ECLF #</IfModule>
#<IfModule !mod_afpa_cache.c>
# Listen @@Port@@
#</IfModule>
```

By disabling the AFPA module, the IBM HTTP Server 2.0.47 starts properly.

Note: More information about the IBM HTTP Server limitation may be found by reading the document titled "Hang or crash of Microsoft Windows when Running AFPA and When Antivirus Software is Active" on the IBM Support site.

Lack of Write Permissions on Host Configuration File

Symptom:

My web agent log shows the following error:

Siteminder Web Agent not having write permissions on host configuration file.

Solution:

Verify that the account under which the web server operates has write permissions for the SmHost.conf file. For example, on IIS web servers, verify that the NETWORK SERVICE account has write permissions for the SmHost.conf file.

Connectivity and Trusted Host Registration Issues

This section contains troubleshooting information related to trusted host registration.

Trusted Host Registration Fails

Symptom:

I cannot register a trusted host.

Solution:

Check the following:

- Make sure that the Policy Server is installed and configured on the target server, that the IP address for the server is correct, and that the Policy Server is running.
- Check the SiteMinder administrator name and password and make sure these are correct.
- Make sure that the Host Configuration Object and Agent Configuration Object specified during the Agent installation and configuration are defined at the Policy Server.
- You may be using a name for the trusted host that is already in use by an existing trusted host. Re-register using a unique name for the trusted host.

No Connection From Trusted Host to Policy Server

Symptom:

Trusted host cannot make a connection to the Policy Server.

Solution:

Do the following:

- Ensure that the EnableWebAgent parameter in the WebAgent.conf file is set to yes.
- Check for the SmHost.conf file in *web_agent_home*/config. The presence of this file indicates a successful registration of the trusted host.

  web_agent_home

  Indicates the directory where the Web Agent is installed.

  Default (Windows installations): C:\Program Files\CA\webagent

  Default (UNIX installations): /opt/ca/webagent
- Ensure that the host where the Agent is installed and has been registered as a trusted host.
- Make sure the Agent Configuration Object has a DefaultAgentName specified. Also, ensure that the minimum required parameters are configured for your particular web server.
- Ensure that the Policy Server is running.

Host Registered, but the SMHost.conf file has been Deleted

Symptom:

A Trusted Host is registered but the SmHost.conf file has been deleted.

Solution:

In the Administrative UI, remove the Trusted Host Object corresponding to the host name for which the file was deleted. Re-register the host using the smreghost tool.

General Installation Issues

This section contains troubleshooting information related to installations.

More Information

Fix the ServletExec CLASSPATH for DMS (see page 50)

One Installation Hangs During Multiple Installations on the Same System

Symptom:

You are running multiple installations on the same system at the same time and an installation hangs.

Solution:

Try the following tasks in the order listed:

1. Reboot the system and try the installation again.
2. Rename the ZeroG registry file, then retry the installation. The registry file is in the following locations:
   - Windows: C:\Program Files\ZeroG Registry\com.zerog.registry.xml
   - UNIX: $HOME/.com.zerog.registry.xml or /var/.com.zerog.registry.xml

   The registry file is locked while an installation is taking place, so if multiple installations are running at the same time, they cannot write to this file, causing the installation to hang.

Location of the Installation Failure Log

Symptom:

I want to see what failed during the installation.

Solution:

See the ca-wa-details.log file, located in *web_agent_home*/install_config_info.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

Attempt to Access DMS Page Returns Error

Valid on Windows

Symptom:

On Windows systems, you receive a servlet DMS not found error when you access a DMS page.

Solution:

Check the ServletExec CLASSPATH and modify it if necessary.

More information:

Fix the ServletExec CLASSPATH for DMS (see page 50)

Web Agent Not Shown in Add/Remove Programs Control Panel

Symptom:

I cannot uninstall the Web Agent from the Add/Remove Programs list control panel because the SiteMinder Web Agent is not listed.

Solution:

Remove the Agent as follows:

1. Open the registry editor.
2. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\SiteMinder\WebAgent
3. Highlight the entire UninstallString entry and copy it.
4. Open a DOS window and paste the UninstallString into the window at a DOS prompt.
5. Press ENTER.

   The Agent is uninstalled.

Error Message During Upgrade

Valid on Windows, UNIX

Symptom:

You receive the following error during an upgrade:

ComponentMoveData Error -115

Solution:

Do the following:

1. Click OK to exit the error message.
2. Start the Policy Server Management Console.
3. From the console, stop the Policy Server.
4. Close the Management Console.
5. Run the upgrade or again and this error message should no longer appear.

Metabase Error When Configuring An IIS Web Agent

Symptom:

When I try to configure a Web Agent on an IIS server, I receive a Metabase error with a message similar to the following:

Unable to add entry to metabase : siteminderagent ==

Solution:

Use the following process:

1. Run the configuration wizard again and remove the IIS web server (by clearing its check box).

   An error similar to the following appears:

   Unable to remove entry from the metabase : siteminderagent ==

2. Set the IIS web server to use a non-default web site by editing the Metabase.

More information:

How to Use a Non-Default IIS Website (see page 12)

Miscellaneous Issues

This section contains troubleshooting information related to miscellaneous issues.

Netscape Browser Won't Open PDFs

Valid on UNIX

Symptom:

I cannot open PDF Files from the Online Manuals Index HTML page on a UNIX system using a Netscape browser.

Solution:

If a .pdf file does not open after you click a link on the doc_index.htm page, set Acrobat Reader as a helper application in Netscape Navigator. When you set this option, Netscape automatically launches Acrobat Reader each time you request to view a .pdf file.

To set Acrobat Reader as a helper application

1. In Navigator, go to Edit, Preferences.
2. In the Netscape Preferences dialog, select Navigator, Applications.
3. Under Applications, Specify helper applications for different file types, select Portable Document Format and click Edit.
4. In the Netscape Applications dialog, select Applications and set it to the following:

   Acrobat_Reader_home/bin/acroread %s

   For example, if you installed Acrobat Reader in the default location, set this value to:

   /usr/local/Acrobat4/bin/acroread %s.
5. Click OK to close these dialogs.

   After you set this option, Navigator launches Acrobat Reader and opens the .pdf file in the /tmp directory.

Adobe Acrobat Reader Won't Install on a Windows System

Valid on Windows

Symptom:

I cannot install Adobe Acrobat Reader on a Windows system.

Solution:

If the Acrobat Reader installation program hangs while the Policy Server is running, stop the server using the Policy Server Management Console, then the installation program should start.

Sun Java System Web Agent Issues

This section contains troubleshooting information related to Sun Java System Web Agents.

Web Server Starts but Web Agent Not Enabled

Symptom:

The Web Agent is not enabled even though the web server has started.

Solution:

Open the WebAgent.conf file, and then set the EnableWebAgent parameter to yes.

smget Error Message When Web Server Starts

Valid on Sun Java System web servers

Symptom:

When starting the Web Server, you see the message:

shmget failed. You may be trying to make a cache that is too large.

Solution:

Make the recommended adjustments to the shared memory segments.

More information:

Tune the Shared Memory Segments (see page 152)
How to Tune the Solaris 10 Resource Controls (see page 154)

Reconfigured Web Agent Won't Operate

Valid on Sun Java System web servers

Symptom:

Web Agent configuration changes are not in the obj.conf file. The Web Agent cannot operate.

Solution:

The Sun Java System Administration console was used to make server modifications before the changes made by the Agent configuration to the obj.conf were applied. Re-configure the Web Agent.

Sun Java System Web Server Fails at Runtime

Symptom:

Sun Java System web server is failing at run time.

Solution:

Increase the StackSize setting in the Sun Java System server's magnus.conf file to a value of 256 KB. The magnus.conf file is located in:

Sun_Java_System_home/*web_server_instance*/config

More Information

Tune the Shared Memory Segments (see page 152)

Apache Web Agent Issues

This section lists troubleshooting information for the Apache Web Agent.

More Information

Tune the Shared Memory Segments (see page 152)

Apache Server Starts But Web Agent Is Not Enabled

Symptom:

The Apache Agent is not enabled even though the web server has started.

Solution:

Do the following tasks:

- Open the WebAgent.conf file, and then set EnableWebAgent to yes.
- Compile the Apache web server to include the mod_so Apache module .
- Modify the httpd.conf file so it to loads the mod_sm SiteMinder Agent Module.
- Modify the httpd.conf file to initialize the Agent, using the SmInitFile entry.
- For Apache Agents on HP-UX systems, modify the httpd.conf file to add the mod-hpaCCso.c SiteMinder Agent Module.

Apache Server Shows shmget Failure On Startup

Symptom:

When starting the web server, you see: shmget failed.

You may be trying to make a cache that is too large or be doing apachectl restart.

Solution:

Make the recommended adjustments to the shared memory segments.

Apache Agent is Enabled but Default Server Page or Protected Resource Not Accessible

Symptom:

The default web server page or the protected resource is not accessible after enabling Web Agent.

Solution:

Make the recommended adjustments to the shared memory segments.

Apache Web Agent Not Operating

Symptom:

The Apache Web Agent is not operating.

Solution:

Tune the Apache operating system shared memory.

Domino Web Agent Issues

This section contains troubleshooting information related to Domino Web Agents.

Domino Web Agent Not Enabled but the Web Server has Started

Valid on Domino

Symptom:

The Domino Web Agent is not enabled even though the web server has started.

Solution:

Do the following:

- In the WebAgent.conf file, set the EnableWebAgent parameter to yes.
- Ensure that the DOMINOWebAgent.dll file has been added to the filter DLLs. The Web Agent DLL must be the first DLL in the list.

More Information

Add the Domino Web Agent DLL (Windows) (see page 136)

Domino Agent Cannot Initialize When Local Configuration Mode is Used

Valid on Domino

Symptom:

Domino Agent cannot initialize in local configuration mode.

Solution:

Check that the full path to the WebAgent.conf file is added to the notes.ini file.

Appendix A: Unattended Installation

This section contains the following topics:

ca-wa-installer.properties File (see page 181)
Modify General Information (see page 182)
Register a Trusted Host (see page 182)
Identify Policy Servers for Trusted Host Registration (see page 183)
Specify the Host Configuration File (see page 183)
Select a Web Server for Configuration (see page 184)
Configure the Web Server to Restart (Windows Only) (see page 188)
Name the Trusted Host Name and Host Configuration Object (see page 188)

ca-wa-installer.properties File

The ca-wa-installer.properties file is generated during a Web Agent installation and configuration. It contains all of the parameters, paths, and passwords entered during the installation and configuration.

During an unattended installation and configuration, this properties file provides the settings that would be entered by an end-user in a GUI or Console mode installation. Be default, the ca-wa-installer.properties file contains the settings from the initial installation. You can use the default properties file to run installations with the same settings or use the file as a template that you modify to suite your environment.

An unattended installation uses a properties file that is initially configured with values from the initial GUI or console mode Web Agent installation. Therefore, you can only run an unattended installation on a system with the same platform and web server image as the system where you first installed the Web Agent. For example, you cannot install an Agent on a Solaris system with an Sun Java System web server, then use the properties file to run an unattended installation on a Linux system with an Apache web server.

Modify General Information

In the General Information section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
USER_INSTALL_DIR	The location where the unattended installation will place the Web Agent. For example: C:\\Program Files\\ca\\webagent
USER_SHORTCUTS	The location where the installation places a shortcut to the Configuration Wizard. For example: C:\\Documents and Settings\\jdoe\\Start Menu\\Programs

Register a Trusted Host

In the Trusted Host Registration section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
HOST_REGISTRATION_YES	Indicates whether the installation will go through the trusted host registration process. For example, HOST_REGISTRATION_YES=1
ADMIN_REG_NAME	Name of the administrator with the rights to register a trusted host. For example, ADMIN_REG_NAME=siteminder
ADMIN_REG_PASSWORD	Password for the administrator with the rights to register a trusted host. This value is encrypted by the installation program. For example, ADMIN_REG_PASSWORD=ENC:nGDaSDy1H7qZqcdbkJKPEQ To change the password, you can either re-configure the Agent or modify this parameter by entering a new password in clear text.
SHARED_SECRET_ROLLOVER_YES	Enables shared secret rollover, which periodically changes the secret that encrypts communication between the trusted host and the Policy Server.

Parameter	Description and Sample Value
	The default is 0. Set this parameter to 1 to enable shared secret rollover. For example, SHARED_SECRET_ROLLOVER_YES=1

Identify Policy Servers for Trusted Host Registration

In the section to list Policy Servers for trusted host registration, you can modify the setting in the following table:

Parameter	Description and Sample Value
IP_ADDRESS_STRING	Specifies the IP address of the Policy Server where you are registering the trusted host. To have multiple bootstrap servers for failover. you can specify multiple addresses, separated by a comma. For example, IP_ADDRESS_STRING=111.11.1.11, 122.123.2.34

Specify the Host Configuration File

In the Host Configuration File Location section you can modify the settings in the following table:

Parameter	Description and Sample Value
SM_HOST_FILENAME	Names the Host Configuration File, SmHost.conf. For example, SM_HOST_FILENAME=SmHost.conf
SM_HOST_DIR	Identifies the directory where the SmHost.conf file is installed. The default For example, SM_HOST_DIR=C:\\Program Files\\ca\\webagent\\config

Select a Web Server for Configuration

In the Trusted Host Registration section of the properties file, you can modify the settings in the following table:

Parameter	Description and Sample Value
APACHE_SELECTED APACHE_WEBSERVER_ROOT	Indicates which Apache web server you are configuring and that server's root directory. For example, for UNIX Systems: APACHE_SELECTED=0 APACHE_WEBSERVER_ROOT=/export/agent5qa/apache
IPLANET_SELECTED IPLANET_WEBSERVER_ROOT	For UNIX Systems. Indicates which Sun Java System web server you are configuring and that server's root directory. For example, for UNIX Systems: IPLANET_SELECTED=1 IPLANET_WEBSERVER_ROOT=/export/agent5qa/sunonewebserver
DOMINO_SELECTED DOMINO_WEBSERVER_ROOT	For UNIX Systems. Indicates which Apache web server you are configuring and that server's root directory. For example, for UNIX Systems: DOMINO_SELECTED=0 DOMINO_WEBSERVER_ROOT=
WEB_SERVER_INFO	The WEB_SERVER_INFO setting contains information about the web servers configured with a SiteMinder Web Agent. You can either edit this setting in the file or re-run the Web Agent configuration to regenerate this string with the appropriate values. The WEB_SERVER_INFO entry consists of a set of web servers, separated by a semicolon. Each web server consists of comma-separated values. **Important!** The WEB_SERVER_INFO setting can be modified from one web server to another, even for the same machine, but modify the setting at your own risk. Making a mistake when changing a value could cause the Agent installer to fail or the Agent to be configured with inappropriate data. The WEB_SERVER_INFO setting is as follows: WEB_SERVER_INFO=;*server_instance*,*web_server_config_dir*,*web_server_listing*,*service_name*,*web_server_type*,*web_server_version*,*web_server_path*,empty_string,*empty_string*,*selected_web_server*,*existing_server_config*,*preserve_web_server*,*document_selection*,*OneView_Monitor_config*,*confirm_web_server_config*,*advanced_auth_scheme*,*agent_config_obj*,*self_registration*,*DMS_admin_username*,*DMS_admin_password*

More Information

WEB_SERVER_INFO Variables (see page 185)

WEB_SERVER_INFO Variables

The WEB_SERVER_INFO variables and their values are as follows:

server_instance

Indicates the web server instance.

Example: https-server1

web_server_config_dir

Indicates the path to the web server's config directory.

Example: /usr/iplanet/servers/https-server1/config

web_server_listing

Reflects how the web server is shown in the list of available web servers to configure during configuration.

Example: https-server1 (Sun Java System 6.0)

service_name

Indicates the web server service name.

Example: https-server1

web_server_type

Indicates the type of web server. Choose from the following types:

- apache
- domino
- IIS
- iplanet
- sunone

For the Sun Java System web server, use iplanet or sunone.

Example: sunone

web_server_version

Indicates the web server version

Example: 6.0

web_server_path

Indicates the path to the web_server_instance root

Example: /usr/iplanet/servers/https-server1

web_agent_operating_system

Indicates the type of operating system used by the Web Agent.

Limits: Windows, Unix

Example: Windows

empty_string

Indicates an empty string saved for future use.

Example: +EMPTYSTR+

selected_web_server

Indicates whether the selected web server should be configured with an Agent.

Limits: 1 (yes) or 0 (no)

existing_server_config

Previous web server configuration states whether there is an existing Agent configuration

Limits: 1 (yes) or 0 (no)

preserve_web_server

Indicates whether the specified web server's configuration with a Web Agent should be overwritten with a new configuration or preserved.

Limits: 1 (preserve) or 0 (overwrite)

document_selection

Used only for the Policy Server only. The Web Agent ignores this entry. Accept the default.

Limits: 1 (yes) or 0 (no)

OneView_Monitor_config

Used only for the Policy Server only. The Web Agent ignores this entry. Accept the default.

Limits: 1 (yes) or 0 (no)

confirm_web_server_config

Confirms whether the selected web server should be configured with an Agent.

Limits: 1 (yes) or 0 (no)

advanced_auth_scheme

Specifies which advanced authentication scheme, if any, is being used. Choose one of the following options:

- HTTP Basic over SSL
- X509 Client Certificate
- X509 Client Certificate and HTTP Basic
- X509 Client Certificate or HTTP Basic
- X509 Client Certificate or Form
- X509 Client Certificate and Form
- No advanced authentication

agent_config_object

Indicates which Agent Configuration Object to use.

Example: iplanetdefaultsettings

self_registration

Enables self Registration.

Limits: 1 (yes) or 0 (no)

DMS_admin_name

DMS Administrator's name.

Example: Admin1

DMS_admin_password

DMS Administrator's password.

Example: ENC:6f1I5TLVEpuSBHpf4GrASg

You can change any of these values *except* the DMS Admin password. The password can be reused by copying the value from one properties file to another. The only way to change the DMS Admin password is to repeat the Agent configuration. The encryption and decryption will always encrypt and decrypt in the same manner.

The following is an example of the file:

WEB_SERVER_INFO=;https-server1,/usr/iplanet/servers/https-server1/config,https-server1 (iPlanet 6.0),https-server1,iplanet,6.0,/usr/iplanet/servers/https-host,Unix,+EMPTYSTR+,1,0,1,0,0,1,HTTP Basic over SSL,agent1,0,undefined,ENC:6f1I5TLVEpuSBHpf4GrASg==,;https-host2,/usr/iplanet/servers/https-host2/config,https-host2 (Netscape ES 6.0),https-host2,iplanet,6.0,/usr/iplanet/servers/https-iplanetdefaultsettings,+EMPTYSTR+,+EMPTYSTR+,1,0,0,0,1,No advanced authentication,host2,0,undefined,ENC:6f1I5TLVEpuSBHpf4GrASg==

Configure the Web Server to Restart (Windows Only)

In the section to list Policy Servers for trusted host registration, you can modify the setting in the following table:

Parameter	Description and Sample Value
USER_REQUESTED_RESTART	Allows the installation program to reboot the Windows machine, if required after the configuration process. Set to Yes to allow a reboot. Otherwise, set to No.

Name the Trusted Host Name and Host Configuration Object

In the section for naming the Trusted Host and Host Configuration Object, you can modify the settings in the following table:

Parameter	Description and Sample Value
TRUSTED_HOST_NAME	Names the trusted host. This name must be unique. For example: TRUSTED_HOST_NAME=mytrustedhost
CONFIG_OBJ	Identifies the Host Configuration Object, which defines communication between the trusted host and Policy Server. For example: CONFIG_OBJ=MyHostSettings

Appendix B: Settings Added to the Sun Java System Server Configuration

This section contains the following topics:

Additions for Sun Java System Server 6.0 (see page 189)
magnus.conf File Additions for Windows Platforms (see page 190)
Code Added to the magnus.conf File on UNIX Platforms (see page 190)
obj.conf File Additions for Windows Platforms (see page 191)
obj.conf File Additions for UNIX Platforms (see page 193)
mime.types File Additions for Windows and UNIX Platforms (see page 194)
Check Agent Start-up with LLAWP (see page 195)

Additions for Sun Java System Server 6.0

When you install the Web Agent on an Sun Java System web server 6.0, configuration settings are automatically added to the following files:

- magnus.conf
- obj.conf file
- mime.types

These files load automatically when the web server starts. The additional settings initialize the Web Agent. When the Web Agent installation program adds information to the web server's configuration, it divides this information differently for different versions of the Sun Java System web server.

For Windows platforms, these files are in the *Sun_Java_System_install_location*\servers\https-*hostname*\config\ directory.

For UNIX platforms, these files are in the /usr/*Sun_Java_System_install_location*/servers/https-*hostname*/config/ directory.

Note: The *Sun_Java_System_install_location* is the directory where you installed the Sun Java System server on your computer, and *hostname* is the name of the server.

magnus.conf File Additions for Windows Platforms

The following lines are added to the magnus.conf file on Windows platforms:

```
Init fn="load-modules" shlib="C:/Program Files/ca/webagent/bin/SunOneWebAgent.dll"
funcs="SmInitAgent,SmInitChild,SiteMinderAgent,SmRequireAuth,SmAdvancedAuth"
Init fn=SmInitAgent config="C:/iPlanet/Servers/https-server1/config/WebAgent.conf" errortext="Error initializing Web Agent..."
Init fn="SmInitChild" LateInit="yes"
```

Note: Some entries in your file may differ slightly from the example shown.

The additional lines instruct the web server to load the SiteMinder Web Agent with the following NSAPI functions:

- SmInitAgent
- SiteMinderAgent
- SmRequireAuth
- SmAdvancedAuth

Code Added to the magnus.conf File on UNIX Platforms

The following lines are added to the magnus.conf file for UNIX platforms:

```
Init fn="load-modules" shlib="/usr/ca/siteminder/agents/bin/libSunOneWebAgent.so"
funcs="SmInitAgent,SmInitChild,SiteMinderAgent,SmRequireAuth,SmAdvancedAuth"
Init fn=SmInitAgent config="/usr/iPlanet/servers/https-yourserver/config/WebAgent.conf" errortext+"Error initializing Web Agent..."
Init fn="SmInitChild" LateInit=”yes”
```

These lines instruct the web server to load the SiteMinder Web Agent with the following NSAPI functions:

- SmInitAgent
- SmInitChild
- SiteMinderAgent
- SmRequireAuth
- SmAdvancedAuth

obj.conf File Additions for Windows Platforms

When a Web Agent is configured to support an advanced authentication scheme, the Web Agent adds settings to the Sun Java System's obj.conf file. SiteMinder does not remove these settings later if the Agent is reconfigured to support a different advanced authentication scheme. You must manually edit the obj.conf file to remove the settings that are no longer relevant.

Most of the additional lines in the file are added by the Web Agent installation program. Other lines (shown in bold) are added by the servlet engine that you configure for the JSP version of the SiteMinder Password Services.

The lines added by the servlet engine must come before the NameTrans fn functions added by the SiteMinder Web Agent.

In the following example of a modified obj.conf file, smhome represents the installed location of SiteMinder on your system:

Note: Some entries in your file may differ slightly from the example shown.

```
AuthTrans fn="SiteMinderAgent"
NameTrans fn="assign-name" from="*.jsp*" name="myservletengine"
NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"
NameTrans fn="assign-name" from="/siteminderagent/pwservlet/*" name="servletengine"
NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi" dir="/smhome/siteminder/webagent/pw" name="cgi"
NameTrans fn="pfx2dir" from="/siteminderagent/pw" dir="/smhome/siteminder/webagent/pw"
NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" dir="/smhome/siteminder/webagent/samples"
NameTrans fn="pfx2dir" from="/siteminderagent/jpw" dir="/smhome/siteminder/webagent/jpw"
NameTrans fn="pfx2dir" from="/siteminderagent" dir="/smhome/siteminder/webagent/samples"

PathCheck fn="SmRequireAuth"
PathCheck fn="get-client-cert" dorequest="1"
PathCheck fn="get-client-cert" require="0" dorequest="1"

Service method="(GET|POST)" fn="SmAdvancedAuth"
```

The following items describe the content of the lines that are added to the obj.conf file:

- The line that reads AuthTrans fn="SiteMinderAgent" is added to the default object (<Object name="default">). It sets up the SiteMinder Web Agent as the Authorization method, or AuthTrans function, for the Web server.
- The line that reads NameTrans fn="assign-name" from= "/siteminderagent/pwservlet/*" name="myservletengine" is a filter added by the Web Agent that maps the JSP Password Services servlet to the instance of the servlet engine so that engine can process it.
- Most of the lines that begin NameTrans fn="pfx2dir" add virtual directories and mappings for the Agent to support SiteMinder's Password Services (CGI and JSP versions).

- The line that begins NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" is added if you chose to configure a certificate based authentication scheme.
- The line that reads PathCheck fn="SmRequireAuth" is added to any existing PathCheck lines in the default object. It verifies that the user is authorized to perform the requested action on the requested resource.
- The line that reads PathCheck fn="get-client-cert" dorequest="1" is added if, during configuration, you indicated that the Web Agent would support advanced authentication schemes. It supports the use of certificate, certificate plus basic, and certificate and forms authentication schemes.
- The line that reads PathCheck fn="get-client-cert" require="0" dorequest="1" is added if, during configuration you indicated during installation that the Web Agent would support advanced authentication schemes. It supports the use of certificate or basic or the certificate or forms authentication schemes.

  Note: Both PathCheck lines for advanced authentication should be commented out for "Basic Auth over SSL."
- The lines that begin Service method are added to instruct the Web server what to do with the MIME types.
- The lines that read NameTrans fn="assign-name" from="*.jsp*" name="myservletengine" and NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"create mappings for the Agent to support SiteMinder's Password Services.

obj.conf File Additions for UNIX Platforms

When a Web Agent is configured to support an advanced authentication scheme, the Web Agent adds settings to the Sun Java System's obj.conf file. SiteMinder does not remove these settings later if the Agent is reconfigured to support a different advanced authentication scheme. You must manually edit the obj.conf file to remove the settings that are no longer relevant.

Most of the additional lines in the file are added by the Web Agent installation program. Other lines (shown in bold) are added by the servlet engine that you configure for the JSP version of the SiteMinder Password Services.

The lines added by the servlet engine must come before the NameTrans fn functions added by the SiteMinder Web Agent.

In the following example of a modified obj.conf file, smhome represents the installed location of SiteMinder on your system:

Note: Some entries in your file may differ slightly from the example shown.

```
AuthTrans fn="SiteMinderAgent"

NameTrans fn="assign-name" from="*.jsp*" name="myservletengine"
NameTrans fn="assign-name" from="/servlet/*" name="myservletengine"
NameTrans fn="assign-name" from="/siteminderagent/pwservlet/*" name="servletengine"
NameTrans fn="pfx2dir" from="/siteminderagent/pwcgi" dir="/smhome/siteminder/webagent/pw" name="cgi"
NameTrans fn="pfx2dir" from="/siteminderagent/pw" dir="/smhome/siteminder/webagent/pw"
NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" dir="/smhome/siteminder/webagent/samples"
NameTrans fn="pfx2dir" from="/siteminderagent/jpw" dir="/smhome/siteminder/webagent/jpw"
NameTrans fn="pfx2dir" from="/siteminderagent" dir="/smhome/siteminder/webagent/samples"

PathCheck fn="SmRequireAuth"
#SMSSL The line below should be uncommented for "cert" and "cert plus basic" schemes
PathCheck fn="get-client-cert" dorequest="1"
#SMSSL The line below should be uncommented for "cert or basic" or "cert or form" schemes
PathCheck fn="get-client-cert" require="0" dorequest="1"
#SMSSL Both of the above PathCheck lines should be commented out for "Basic Auth over SSL"

Service method="(GET|POST)" fn="SmAdvancedAuth"
```

The following items describe the content of the lines that are added to the obj.conf file:

- The line that reads AuthTrans fn="SiteMinderAgent" is added to the default object (<Object name="default">). It sets up the SiteMinder Web Agent as the Authorization method, or AuthTrans function, for the Web server.
- The line that reads NameTrans fn="assign-name" from= "/siteminderagent/pwservlet/*" name="myservletengine" is a filter added by the Web Agent that maps the JSP Password Services servlet to the instance of the servlet engine so that engine can process it.

- Most of the lines that begin NameTrans fn="pfx2dir" add virtual directories and mappings for the Agent to support SiteMinder's Password Services (CGI and JSP versions).
- The line that begins NameTrans fn="pfx2dir" from="/siteminderagent/certoptional" is added if you chose to configure a certificate based authentication scheme.
- The line that reads PathCheck fn="SmRequireAuth" is added to any existing PathCheck lines in the default object. It verifies that the user is authorized to perform the requested action on the requested resource.
- The line that reads PathCheck fn="get-client-cert" dorequest="1" is added if, during configuration, you indicated that the Web Agent would support advanced authentication schemes. It supports the use of certificate, certificate plus basic, and certificate and forms authentication schemes.
- The line that reads PathCheck fn="get-client-cert" require="0" dorequest="1" is added if, during configuration you indicated during installation that the Web Agent would support advanced authentication schemes. It supports the use of certificate or basic or the certificate or forms authentication schemes.

  Note: Both PathCheck lines for advanced authentication should be commented out for "Basic Auth over SSL."
- The lines that begin Service method are added to instruct the Web server what to do with the MIME types.

mime.types File Additions for Windows and UNIX Platforms

The following lines are added to the mime.types file by the setup program:

```
type=magnus-internal/sfcc exts=sfcc
type=magnus-internal/fcc exts=fcc
type=magnus-internal/scc exts=scc
type=magnus-internal/ccc exts=ccc
```

These lines set up the mime types to support advanced SiteMinder features.

Check Agent Start-up with LLAWP

You can see if the Web Agent is starting up properly by starting the LLAWP process.

To start the LLAWP process

1. Ensure you have configured the Web Agent with the Configuration Wizard.
2. Open a console window and enter the following command:

   LLAWP *path_to_WebAgent.conf* **-***web_server_type*

   web_server_type can be ISAPI60 or APACHE20

   path_to_WebAgent.conf can be a full path or a relative path from the location where you are running LLAWP. For example:

   - Windows:

     LLAWP "C:\Program Files\ca\Siteminder Web Agent\Bin\IIS\WebAgent.conf" -ISAPI60

   - UNIX:

     LLAWP /usr/apache/conf/WebAgent.conf -APACHE20

   Note: If you start the LLAWP from the command line, you must also shut it down from the command line.

Appendix C: Configuration Changes to Web Servers with Apache Web Agent

This appendix lists changes made automatically by running the Web Agent Configuration Wizard to configure an Apache Web Agent. These changes apply to all web servers that support the Apache Web Agent, including Apache 1.x, Apache 2.0, IBM HTTP Server, and the HP Apache web server.

This section contains the following topics:

Library Path for the Web Server is Set for UNIX Systems (see page 197)
Set Library Path and Path for Oracle 10g Web Server Running in Apache 2.x Mode (see page 198)
Changes to the httpd.conf File (see page 198)
Agent Parameter Added for SSL Connections Using Apache 1.x Based Servers (see page 205)

Library Path for the Web Server is Set for UNIX Systems

The library path for the Apache web server is required because it enables the Apache server to load libraries correctly on a UNIX system. For example:

export LD_LIBRARY_PATH *web_agent_home*/bin

The library path variable depends on the operating system—it should always point to *web_agent_home*/bin.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

The following table lists the variables.

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

Set Library Path and Path for Oracle 10g Web Server Running in Apache 2.x Mode

For an Oracle 10g web server running in Apache 2.x mode, both the LD_LIBRARY_PATH and PATH variables need to be set in the apachectl script. The LD_LIBRARY_PATH is automatically added to the apachectl script. The location of the apachectl script varies according to your version of OHS:

Apache 1.3.x based OHS

OHS_home/Apache/Apache/conf/

Note: Apache 1.3x is *not* supported with Oracle 10g on Windows Server 2003.

Apache 2.x based OHS

OHS_home/ohs/conf/

Note: Apache 2.x is supported with Oracle 10g on Windows Server 2003 for r12.0 SP2 Web Agents.

To set the PATH variable, add the following entry to the apachectl script:

PATH=*Path_of_webagent_install*/bin:${PATH} ; export PATH

Changes to the httpd.conf File

The Configuration Wizard modifies the httpd.conf configuration file to enable the web server to operate with the Apache Web Agent.

The examples in this procedure are for UNIX platforms; however the same changes are made to Windows platforms using the appropriate Windows syntax.

web_agent_home

Indicates the directory where the Web Agent is installed.

Default (Windows installations): C:\Program Files\CA\webagent

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

For most Apache-based web servers, this file is located in the conf directory:

Apache_home/conf

Note: For more information about the location of this file, see the documentation provided by the vendor of your web server.

Entries Added to DSO Support Section

The following line(s) are added to the Dynamic Shared Object (DSO) Support configuration section, which precedes the Main server configuration section of the file.

LoadModule Entries Added

The SiteMinder Agent requires one of the following modules in order to load:

Apache 1.x (except servers running on HP-UX 11i)

LoadModule sm_module *web_agent_home*/bin/mod_sm.so

Apache 1.x running on HP-UX 11i

LoadModule hpaCCso_module *web_agent_home*/bin/mod_hpaCCso.sl

HPaCCLoadModule sm_module *web_agent_home*/bin/mod_sm.sl

Note: HP-UX uses the extension .sl to refer to a shared library. If the operating system for the Web Agent is HP-UX, the .sl extension is used.

Apache 1.x running on Windows

LoadModule sm_module *web_agent_home*/bin/Apache20WebAgent.dll

Apache 2.0 (excluding servers running on HP-UX 11i)

LoadModule sm_module *web_agent_home*/bin/libmod_sm20.so

Apache 2.0 running on HP-UX 11i

LoadModule sm_module *web_agent_home*/bin/libmod_sm20.sl

Apache 2.0 running on Windows

LoadModule sm_module *web_agent_home*/bin/mod_sm20.dll

Apache 2.2(excluding servers running on HP-UX 11i)

LoadModule sm_module *web_agent_home*/bin/libmod_sm22.so

Apache 2.2 running on Windows

LoadModule sm_module web_agent_home/bin/mod_sm22.dll

Oracle HTTP Server (excluding servers running on HP-UX 11i)

Add the following line:

LoadModule sm_module *web_agent_home*/bin/mod_sm.so

Oracle HTTP Server running on HP-UX 11i

LoadModule hpaCCso_module *web_agent_home*/bin/mod_hpaCCso.sl

HPaCCLoadModule sm_module *web_agent_home*/bin/mod_sm.sl

(Optional) UNIX systems

To enable certificate-based authentication, the following line is added to the DSO configuration section:

LoadModule sm_certenv *web_agent_home*>/bin/mod_smcertenv.so

mod_smcertenv enables certificate-based authentication to work with Apache web servers without requests being redirected to the SSL credential collector.

Note: This module is only for Apache 1.3.27 web servers. It is not supported for proprietary versions of the Apache 1.3.x web server, such as IBM HTTP Server, or Oracle HTTP Server.

The entry to load mod_smcertenv must come after the entry to load mod_sm.

mod_sm.c Entry Added to ClearModuleList

If the directive ClearModuleList exists in the DSO configuration section, the mod_sm.c entry is placed at the end of the AddModule section of the file, as shown in bold:

ClearModuleList

AddModule mod_env.c

.

.

.

AddModule mod_servletexec.c

#Siteminder

AddModule mod_sm.c

SmInitFile Entry Added

In the Main server section of the file, the SmInitFile entry is added:

SmInitFile *Apache_home*/conf/WebAgent.conf

This entry is placed after the LoadModule entry. A full path is used, not a relative path. For example:

SmInitFile "/export/Apache2/conf/WebAgent.conf"

Alias Entries Added

In the Aliases section of the file, entries are added to enable SiteMinder features.

Note the following:

- The Alias /siteminderagent/ "*web_agent_home*/samples/" entry must come **after** all other aliases in the Aliases section.
- For SiteMinder to use Basic over SSL or X.509 certificate-based authentication schemes with an Apache Web Agent, SSL must be enabled by compiling the Apache server to include the mod_ssl module. To obtain this module, see www.modssl.org.
- Each alias entry appears on its own line.

Password Services

```
Alias /siteminderagent/pwcgi/ "<web_agent_home/pw/>"
 <Directory "/export/webagent/pw/">
  Options Indexes MultiViews ExecCGI
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>

Alias /siteminderagent/pw/ "<web_agent_home>/pw/"
 <Directory "/export/webagent/pw/">
  Options Indexes MultiViews ExecCGI
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>
```

Basic over SSL authentication

```
AliasMatch /siteminderagent/nocert/[0-9]+/(.*)
 "<web_agent_home>/$1"
 <Directory "<web_agent_home>/$1">
  Options Indexes MultiViews
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>
```

X509 Client Cert or X509 Client Cert and Basic authentication

```
AliasMatch /siteminderagent/cert/[0-9]+/(.*)
"<web_agent_home>/$1"
 <Directory "<web_agent_home>/$1">
  Options Indexes
  AllowOverride None
  Order allow,deny
```

```
  Allow from all
 </Directory>
```

X509 Client Cert or Basic authentication

```
AliasMatch /siteminderagent/certoptional/[0-9]+/(.*) "<web_agent_home>/$1"
 <Directory "<web_agent_home>/$1"
  Options Indexes
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>
```

X509 Certificate or Form or X509 Client Cert and Form authentication

```
Alias /siteminderagent/certoptional/"<web_agent_home>/
 samples/"
 <Directory "<web_agent_home>/samples/"
  Options Indexes
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>
```

Forms authentication or Agent is cookie provider for single sign-on

```
Alias /siteminderagent/ "<web_agent_home>/samples/"
 <Directory "/export/webagent/samples/">
  Options Indexes MultiViews
  AllowOverride None
  Order allow,deny
  Allow from all
 </Directory>
```

Note: This is the alias that should be placed at the end of the section.

AddHandler Entries Added for Traditional Agents

For traditional Web Agents (versions before 5.x QMR 6, such as Agents installed on Apache 1.x web servers), the following entries are added to the AddHandler section of the file for SiteMinder features.

Note: These entries do not apply to Framework Web Agents (versions including v5.x QMR 6 and all subsequent versions, such as Agents installed on Apache 2.0 web servers). These functions are now part of the Web Agent Framework.

SiteMinder Feature	AddHandler Entry
Password Services	AddHandler cgi-script .exe
Forms authentication	AddHandler smformsauth-handler .fcc
Certificate and Forms authentication	
Certificate or forms authentication	AddHandler smsslformsauth-handler .sfcc
SSL authentication, including:	AddHandler smadvancedauth-handler .scc
Basic over SSL	
Certificate	
Certificate or basic	
Certificate and basic	
Cookie provider for single sign-on	AddHandler smcookieprovider-handler .ccc

The modified section would appear as follows:

```
AddHandler cgi-script .exe
AddHandler smformsauth-handler .fcc
AddHandler smsslformsauth-handler .sfcc
AddHandler smadvancedauth-handler .scc
AddHandler smcookieprovider-handler .ccc
```

Certificate Authentication Entries Added

- If you are using X509 Client Cert, X509 Client Cert and Basic, or X509 Client Cert or Basic authentication, the following SSL Engine Options entry in the Virtual Hosts section is uncommented for the appropriate virtual host (if multiple hosts are defined):

  SSLOptions +ExportCertData +StdEnvVars

  Note: If there is an existing SSL option in the Virtual Hosts section, then that existing entry is commented out and the new SSL entry is added.

- If you are using X509 Client Cert or Forms authentication, the following SSL Engine Options entry in the Virtual Hosts section is uncomment for the appropriate virtual host (if multiple hosts are defined):

  SSLOptions +StdEnvVars +CompatEnvVars

- In the Virtual Hosts section of the file, the SSL Client Authentication type is set it to optional:

  SSLVerifyClient optional

LoadFile Entries Added for Apache 2.x on HP-UX 11i

The following entries are added and uncommented in the httpd.conf file for Apache 2.x on HP-UX 11i:

```
#For C++ modules that require standard libraries
LoadFile /usr/lib/hpux32/libunwind.so
LoadFile /usr/lib/hpux32/libCsup.so
LoadFile /usr/lib/hpux32/libstd_v2.so
```

Agent Parameter Added for SSL Connections Using Apache 1.x Based Servers

If you are using SSL connections (HTTPS) to a Web server, the httpsports parameter is added to the WebAgent.conf file or the Agent Configuration Object configured at the Policy Server. This parameter specifies one or more (comma-separated) HTTPS port numbers the web server is listening on. For example, set httpsports to 80.

Note: If a server is behind an HTTPS accelerator, which converts HTTPS to HTTP, all requests are treated as SSL connections by your browser.

Appendix D: Environment Variables Added or Modified by the Web Agent Installation

This section contains the following topics:

Added or Modified Environment Variables (see page 207)

Added or Modified Environment Variables

The following environment variables are added or modified by the Web Agent installation:

- NETE_WA_ROOT = $INSTALL_PATH$
- NETE_WA_PATH = $INSTALL_PATH$$/$bin

Index

(

(Optional) Configure Alias Settings to Enable Forms and Other HTML Authentication Schemes • 139, 144
(Optional) Configure the CGI Directory and CGI URL Path Settings • 138, 143

A

Add a Logs Subdirectory for Apache Web Agents • 18
Add Handler Mappings to Additional Web Sites you want to Protect with SiteMinder • 87
Add Role Services to your IIS 7 Web Server • 84
Add the Agent ISAPI Filter to Additional Web Sites that you want to Protect with SiteMinder • 89
Add the Domino Web Agent DLL (UNIX) • 140
Add the Domino Web Agent DLL (Windows) • 136
Add the ISAPI Extension to the Exchange Web Site • 105
Add the ISAPI Extension to the Exchweb Web Site • 107
Added or Modified Environment Variables • 207
AddHandler Entries Added for Traditional Agents • 204
Additions for Sun Java System Server 6.0 • 189
Adobe Acrobat Reader Won't Install on a Windows System • 177
Agent Configuration Object
  definition • 20
  Domino requirements • 20
  IIS requirements • 20
  installation requirement • 20
Agent Configuration Parameters Required by All Agents • 21
Agent Configuration Parameters Required for Domino Web Agents • 22
Agent Configuration Parameters Required for IIS Web Agents • 23
Agent Parameter Added for SSL Connections Using Apache 1.x Based Servers • 205
Agent Start-Up/Shutdown Issues (Framework Agents Only) • 167
Agent Won't Start Because LLAWP is Already Running or Log Messages not Written to the Correct Log Files • 168
AIX Requirements • 16
Alias Entries Added • 202
Allow IIS to Execute the Agent ISAPI and CGI Extensions • 93
Allow IIS to Execute the Outlook Extensions • 103
Apache Agent is Enabled but Default Server Page or Protected Resource Not Accessible • 179
Apache Server Shows shmget Failure On Startup • 179
Apache Server Starts But Web Agent Is Not Enabled • 179
Apache Web Agent
  Configuration Wizard, accessing • 85, 112, 124
  configuring • 124, 127
  configuring, console mode • 127
  configuring, GUI mode • 127
  for IBM HTTP Web server • 126
  for Stronghold server • 126
  increasing shared memory • 152
  installing • 53
  LD_PRELOAD, setting • 131
  modifying httpd.conf • 198
  reinstalling • 62
  supported platforms • 12
  tuning shared memory • 152
  uninstalling, UNIX • 164
Apache Web Agent Issues • 178
Apache Web Agent Not Operating • 180
Apache Web server
  installing as service • 14
  installing on windows, caution • 14
Apply Changes to Sun Java System Web Server Files • 120
Assign Read Permissions to Samples and Error Files Directories • 92
Attempt to Access DMS Page Returns Error • 174
authentication schemes
  HTTP Basic over SSL • 112, 115
  SSL, configuring • 112, 115

using forms authentication • 149
X.509 client certificate and basic • 112, 115
X.509 client certificate and HTML Forms • 112, 115
X.509 client certificate or basic • 112, 115
X.509 client certificate or HTML Forms • 112, 115
X509 Client Certificate • 112, 115

B

Back Up Customized Files • 77
boostrap servers, configuring • 42, 67

C

CA Product References • iii
ca-wa-installer.properties File • 181
Certificate Authentication Entries Added • 205
Changes to the httpd.conf File • 198
Check Agent Start-up with LLAWP • 195
Check SmHost.conf File Permissions for Shared Secret Rollover • 148
Code Added to the magnus.conf File on UNIX Platforms • 190
Compile an Apache Web Server on a Linux System • 17
configuration
unattended mode, Windows • 145
Configuration Changes to Web Servers with Apache Web Agent • 197
Configuration Methods for Apache Web Agents on UNIX Systems • 126
Configuration Methods for Domino Web Agents on UNIX Systems • 141
Configurations Available for All Web Agents • 145
Configure a Domino Web Agent • 135
Configure a Domino Web Agent on Windows Systems • 135
Configure a Sun Java System Web Agent • 111
Configure an Apache Web Agent • 123
Configure an Apache Web Agent on Windows Systems • 124
Configure an Apache Web Agent Using GUI or Console Mode • 127
Configure an IIS Web Agent • 83
Configure Apache for Oracle 9.0.2/9.0.3 HTTP Server • 133
Configure Domino Web Agents in GUI or Console Mode • 142
Configure Sun Java System Web Agents Using GUI or Console Mode • 115
Configure the Web Server to Restart (Windows Only) • 188
Confirm that SiteMinder is protecting the Outlook Web Access web site • 109
Confirm the SiteMinder ISAPI filter appears first in the list • 102
Connectivity and Trusted Host Registration Issues • 171
Contact CA • iii

D

DLLs
adding, Domino Web Agent • 136
DMS
Admin account, modifying password • 27
dms.properties • 27
dmsencrytpkey
modifying DMSAdmin password • 27
documentation
installing, UNIX • 52
uninstalling
UNIX • 165
uninstalling on a UNIX system • 165
uninstalling on a Windows system • 163
Domino Web Agent
configuring/Windows • 137
Domino Agent Cannot Initialize When Local Configuration Mode is Used • 180
Domino Web Agent
adding DLLs • 136
Configuration Wizard, accessing • 137
configuring, UNIX • 141
installing, UNIX • 53
reconfiguring, Windows • 148
reinstalling, UNIX • 62
uninstalling, UNIX • 164
Domino Web Agent Issues • 180
Domino Web Agent Not Enabled but the Web Server has Started • 180

E

Enable Write Permissions for IBM HTTP Server Logs • 18
Enabling SHLIB Path for an Agent on Apache 2.0/HP-UX 11 • 133
Ensure LD_PRELOAD Variable Does Not Conflict with Existing Agent • 78

Entries Added to DSO Support Section • 199
Environment Variables Added or Modified by the Web Agent Installation • 207
Error Message During Upgrade • 175

F

Files Installed for Registration Services (UNIX) • 75
Fix the ServletExec CLASSPATH for DMS • 50
forms authentication scheme
  credential collection • 149

G

Gather information Needed to Complete the Agent Installation • 19
general information
  settings, unattended installation • 182
General Installation Issues • 172
General Preparations for All Web Agents • 19

H

Host Configuration File
  modifying, Windows • 42, 67
  purpose • 42, 62, 67
  settings, unattended installation • 183
Host Configuration Object
  definition • 20
  installation requirement • 20
Host Registered, but the SMHost.conf file has been Deleted • 172
How to Prepare a Windows System for a Web Agent Installation • 12
How to Configure a Domino Web Agent on UNIX Systems • 139
How to Configure a SiteMinder Web Agent on IIS 6.0 • 91
How to Configure a SiteMinder Web Agent on IIS 7.0 • 83
How to Configure a SiteMinder Web Agent to Protect Microsoft Outlook Web Access • 100
How to Configure Any Web Agent in Unattended Mode • 145
How to Configure the ServletExec Servlet Engine for JSP Password Services for an IIS Web Server • 157
How to Configure the ServletExec Servlet Engine for JSP Password Services on a Sun Java System Web Server in the UNIX Operating Environment • 158
How to Prepare a Domino System for a Web Agent Installation • 17
How to Prepare a Linux System for a Web Agent Installation • 16
How to Prepare a UNIX System for a Web Agent Installation • 14
How to Prepare for a Web Agent Installation • 11
How to Prepare for a Web Agent Upgrade • 77
How to Set Up Additional Agent Components • 149
How to Set Up Your Environment for JSP Password Services • 156
How to Stop an Unattended Installation in Progress on Windows • 36
How to Tune the Solaris 10 Resource Controls • 154
How to Use a Non-Default IIS Website • 12
HP-UX
  uninstalling, Sun Java System Web Agent • 164
HTTP Basic over SSL authentication scheme • 112, 115
httpd.conf
  modifying for Apache • 198

I

IBM Hot Fix Required for Domino 6.5.2 • 18
IBM HTTP Server
  Agent configuration • 126
  installing Agent • 19, 53
Identify Policy Servers for Trusted Host Registration • 183
IIS 6.0 Web Agents and Third-Party Software on the Same Server • 94
IIS Web Agent
  configuring • 85
  IIS 6.0, prerequisites • 91
  reconfiguring • 148
  reinstalling • 36
Improve Server Performance with Optional httpd.conf File Changes • 130
Increase the Agent's Size Limit for Uploaded Files • 95
Install a Servlet Engine for Registration Services (Optional) • 25
Install a Web Agent on a UNIX System • 51
Install a Web Agent on a Windows System • 31
Install an Apache Web Server on Windows as a Service for All Users • 14

Install the Correct Agent for a Web Server • 19
Install the Web Agent Documentation on UNIX Systems • 52
Install the Web Agent on a UNIX System • 53
Installation and Configuration Log Files • 41, 55
Installation History Log File • 37, 61
installer.properties file
description • 58
installer.properties, description • 34, 146
installing
documentation, UNIX • 52
installing Web Agents
Apache • 53
Domino/UNIX • 53
on UNIX • 53
Sun Java System/UNIX • 53

J

JSP Password Services
required modifications, Windows • 155

L

Lack of Write Permissions on Host Configuration File • 170
LD_PRELOAD
setting, Apache/Linux • 131
Library Path for the Web Server is Set for UNIX Systems • 197
Linux
compiling Apache server • 17
LoadFile Entries Added for Apache 2.x on HP-UX 11i • 205
LoadModule Entries Added • 200
Location of the Installation Failure Log • 173

M

magnus.conf File Additions for Windows Platforms • 190
Manually Configure a Sun Java System Web Server • 119
Metabase Error When Configuring An IIS Web Agent • 175
Microsoft Visual C++ 2005 Redistributable Package (x64) Prerequisite • 12
mime.types File Additions for Windows and UNIX Platforms • 194
Miscellaneous Issues • 176
Miscellaneous Web Server Preparations • 18
mod_sm.c Entry Added to ClearModuleList • 201
Modify General Information • 182
Modify the Apache 2.0 httpd.conf File for Agents on IBM HTTP Servers • 18
Modify the DMS Admin Password for Registration Services • 27
Modify the ServletExecAS Startup Script to Run Registration Services with ServletExecAS (UNIX only) • 28
Modify the SmHost.conf File (UNIX) • 67
Modify the SmHost.conf File (Windows) • 42
multiple bootstap servers, configuring • 42, 67

N

Name the Trusted Host Name and Host Configuration Object • 188
Netscape Browser Won't Open PDFs • 176
Netscape. See iPlanet Web Server • 85, 124
No Connection From Trusted Host to Policy Server • 172
Notes About Uninstalling Web Agents • 161
NT. See Windows • 137

O

obj.conf
modifications made by Agent • 189
obj.conf File Additions for UNIX Platforms • 193
obj.conf File Additions for Windows Platforms • 191
One Installation Hangs During Multiple Installations on the Same System • 173
Operating System Tuning • 151

P

Password Services • 155
configuring JSP version, Windows • 155
JSP version • 155
Password Services and Forms Directories • 24
Password Services and Forms Template Changes During Upgrades • 78
Password Services Implementations • 155
Policy Server
checking configuration • 20
initial connection with Agent • 62
registering a trusted host, UNIX • 62
settings, unattended installation • 183
Policy Server Requirements • 20
Preparation • 11
Prepare an Unattended Configuration • 146
Prepare an Unattended Installation on UNIX • 58

Prepare an Unattended Installation on Windows • 34
Prepare for Password Services • 23
Prepare for Registration Services (Optional) • 25
prerequisites for installation
Web Agents, UNIX • 12
Preservation of Any WebAgentTrace.conf File Changes • 19
properties files
dms.properties • 27
Put the Agent Filter and Extension Before Other Third-Party Filters • 98

R

Reconfigure a Web Agent • 148
Reconfigured Web Agent Won't Operate • 178
reconfiguring
Web Agent, Windows • 148
Register a Trusted Host • 182
Register a Trusted Host in GUI or Console Mode • 63
Register Multiple Trusted Hosts on One System (UNIX) • 74
Register Multiple Trusted Hosts on One System (Windows) • 47
Register Your System as a Trusted Host on UNIX • 62
Register Your System as a Trusted Host on Windows • 38
registering a trusted host
on UNIX platform • 62
registering trusted hosts
administrator rights • 20
registering multiple hosts • 47, 74
Registration Services
installed files • 48
requirements for Web Agent • 25
Registration Services Installed Files (Windows) • 48
Reinstall a Web Agent on UNIX • 62
Reinstall the Web Agent on Windows • 36
re-installing
Web Agents, UNIX • 62
Web Agents, Windows • 36
Repair ServletExec's CLASSPATH for JSP Password Services (Windows) • 24
Replace Existing Read-only Files • 78
Required HP-UX Patches • 15
Required Linux Libraries • 17
Required Linux Patches • 16
Required Solaris Patches • 15
Re-register a Trusted Host Using the Registration Tool (UNIX) • 69
Re-register a Trusted Host Using the Registration Tool (Windows) • 44
Results of Running the Configuration Wizard After an Upgrade • 78
Review the Upgrade Procedure • 77
Run a Console Mode Installation on UNIX • 56
Run a GUI Mode Installation on UNIX • 54
Run a GUI Mode Installation on Windows • 32
Run an Unattended Configuration • 146
Run an Unattended Installation on UNIX • 59
Run an Unattended Installation on Windows • 35
Run the Configuration Wizard for a Domino Web Agent on Windows • 137
Run the Configuration Wizard for an IIS Web Agent • 85, 96
Run the Configuration Wizard on Windows • 112

S

Select a Web Server for Configuration • 184
servlet engine
required, Registration Services • 25
ServletExec
repairing classpath, DMS • 24, 50
with registration services • 28
Set JRE in PATH Variable Before Uninstalling the Web Agent • 162
Set LD_PRELOAD for Using X.509-based Auth Schemes with Domino 6.5.3/SuSe8 Linux System • 131
Set Library Path and Path for Oracle 10g Web Server Running in Apache 2.x Mode • 198
Set the Default Web Site Directory Location and Execute Permissions • 104, 108
Set the Directory Security for the Exchange Web Site • 106
Set the Directory Security for the Exchweb Web Site • 108
Set the DISPLAY For Web Agent Installations on UNIX • 14
Set the LD_ASSUME_KERNEL for Apache Agent on SuSE Linux 9 for zSeries • 132
Set the LD_PRELOAD Variable for an Oracle 10G Web Server on Linux • 131
Set the LD_PRELOAD Variable for Apache Agent Operation • 130

Set the LD_PRELOAD Variable for SSL Configuration on an IBM HTTP Server 2.0.47/Linux AS 3.0 System • 131
Set the Web Agent Environment Variables After Installation • 60
Set Web Agent Variables when using apachectl Script • 61
Settings Added to the Sun Java System Server Configuration • 189
shared memory segments, tuning • 152
Shut Down LLAWP • 169
SiteMinder Administrator
for registering hosts • 20
smget Error Message When Web Server Starts • 177
SmHost.conf
creating, UNIX • 62
description • 42, 67
modifying, Windows • 42, 67
purpose • 62
SmInitFile Entry Added • 201
Solaris Settings for Certain Apache 1.3 Type Web Servers • 15
Specify the Host Configuration File • 183
SSL authentication schemes, configuring • 112, 115
Stop an Unattended Installation in Progress on UNIX • 59
Stop LLAWP When Stopping IBM HTTP Server 2.0.47 • 170
Stronghold Web server
installing an Agent • 19, 53
using Apache Agent • 126
Sun Java System Web Agent
increasing shared memory • 152
reconfiguring, Windows • 148
reinstalling, UNIX • 62
reinstalling, Windows • 36
tuning shared memory • 152
uninstalling, UNIX • 164
Sun Java System Web Agent Issues • 177
Sun Java System Web server
changes to obj.conf • 189
Sun Java System Web Server Fails at Runtime • 178
Supported Operating Systems and Web Servers • 12
supported platforms
UNIX • 12

T

Troubleshoot Agent Start-Up/ShutDown with LLAWP • 168
Troubleshooting • 167
trusted host
definition • 20, 62
registering multiple hosts • 47, 74
registering, UNIX • 62
settings, unattended installation • 182, 188
Trusted Host Registration Fails • 171
Tune the Shared Memory Segments • 152

U

unattended configuration
Windows • 145
unattended installation
installer.properties file, description • 58
installer.properties, description • 34, 146
preparing • 34, 58, 146
running, UNIX • 59
running, Windows • 35, 146
UNIX • 57
Windows • 34
Unattended Installation • 181
Unattended Installations on UNIX • 57
Unattended Installations on Windows • 34
Uninstall a Web Agent • 161
Uninstall a Web Agent from a UNIX System • 164
Uninstall a Web Agent from a Windows System • 163
Uninstall Documentation from a Windows System • 163
Uninstall Documentation from UNIX Systems • 165
uninstalling
documentation
UNIX • 165
uninstalling Web Agent documentation
UNIX • 165
Windows • 163
UNIX platforms
Agent, Stronghold server • 126
configuring an Apache Web Agent • 127
data needed to install Agent • 19
installation prerequisites • 12
installing an Agent • 53
installing, Domino Web Agent • 53
installing, Sun Java System Web Agent • 53

reinstalling a Web Agent • 62
Upgrade a Web Agent to r12.0 SP2 • 77
Upgrade a Web Agent to r12.0 SP2 on UNIX Systems • 81
Upgrade a Web Agent to r12.0 SP2 on Windows Systems • 79
upgrading
back up custom files • 77
forms templates • 78
general procedure • 77
password services templates • 78
pre-upgrade issues • 77
replacing read-only files • 78
running Configuration Wizard, results • 78
setting LD_PRELOAD • 78
Use Active Directory for Registration Services (Windows Only) • 26
Use Registration Services • 25

W

Web Agent
Apache, configuring • 124, 127
Apache, configuring, console mode • 127
Apache, configuring, GUI mode • 127
Domino/Windows, configuring • 137
IBM HTTP server, configuring • 126
IIS, configuring • 85
installing, UNIX platforms • 53
modifying httpd.conf, Apache • 198
reconfiguring, Windows • 148
reinstalling, UNIX • 62
reinstalling, Windows • 36
supported UNIX platforms • 12
uninstalling documentation, Windows • 163
uninstalling, UNIX • 164
Web Agent Configuration Wizard
accessing, Apache Web Server • 85, 112, 124
accessing, Domino Web Server • 137
Web Agent Not Shown in Add/Remove Programs Control Panel • 174
Web Agent Start Up and Shut Down Issues (IBM HTTP Server) • 169
web server configuration
restarting Windows, unattended instal • 188
settings, unattended installation • 184
Web Server Starts but Web Agent Not Enabled • 177
WEB_SERVER_INFO Variables • 185
Windows
configuring an IIS Web Agent • 85
Domino Web Agent, configuring • 137
reinstalling a Web Agent • 36
uninstalling documentation • 163
Windows platforms
configuring an Apache Web Agent • 124

X

X.509 client certificate and basic authentication schemes • 112, 115
X.509 client certificate and HTML Forms authentication schemes • 112, 115
X.509 client certificate or basic authentication schemes • 112, 115
X.509 client certificate or HTML Forms authentication schemes • 112, 115
X509 Client Certificate authentication scheme • 112, 115