Symantec Critical System Protection 5.2.9 Installation Guide

Symantec Critical System Protection Installation Guide

Documentation version: 5.2.9

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our Web site at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level

- Hardware information
- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apac@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing Symantec™ Critical System Protection

This chapter includes the following topics:

About Symantec Critical System Protection

Symantec™ Critical System Protection provides policy-based behavior control and detection for desktop and server computers. Symantec Critical System Protection provides a flexible computer security solution that is designed to control application behavior, block port traffic, and provide host-based intrusion protection and detection. Symantec Critical System Protection provides this security by controlling and monitoring how processes and users access resources.

Symantec Critical System Protection agents control behavior by allowing and preventing specific actions that an application or user might take. For example, a Symantec Critical System Protection prevention policy can specify that an email application may not spawn other processes, including dangerous processes like viruses, worms, and Trojan horses. The email application can still read and write to the directories that it needs to access.

Symantec Critical System Protection agents detect behavior by auditing and monitoring processes, files, log data, and Windows® registry settings. For example, a Symantec Critical System Protection detection policy can specify to monitor the Windows registry keys that the Welchia worm changes during infection and send an alert. As a result, Windows registry security-related events can be put into context and appropriate measures taken.

See "About installing Symantec Critical System Protection on Windows" on page 34.

See "Components of Symantec Critical System Protection" on page 12.

Components of Symantec Critical System Protection

Symantec Critical System Protection includes management console and server components, and includes agent components that enforce policies on computers. The management server and management console run on Windows operating systems. The agents run on Windows and UNIX operating systems.

The major components of Symantec Critical System Protection are as follows:

Management console	Coordinate, distribute, and manage policies and agents The management console lets you manage Symantec Critical System Protection policies and agents. The management console also lets you create user accounts, restrict the functions that users can access, modify policies, configure alerts, and run reports. See "Installing and configuring the management console" on page 49.
Management server	Store and correlate agent events and the policy library The management server stores policies in a central location and provides an integrated, scalable, flexible, agent, and policy management infrastructure. The management server coordinates policy distribution, and manages agent event logging and reporting. See "Installing the management server" on page 38.
Agent	Enforce policy on the endpoints Each Symantec Critical System Protection agent enforces rules that are expressed in policies, thereby controlling and monitoring application (process) and user behavior. See "Installing a Windows agent" on page 53.

See "About Symantec Critical System Protection" on page 11.

How Symantec Critical System Protection works

Symantec Critical System Protection controls and monitors what programs and users can do to computers. Agent software at the endpoints controls and monitors behavior based on policy.

The Symantec Critical System Protection policy library contains prevention and detection policies that you can use and customize to protect your network and endpoints, as follows:

- A prevention policy is a collection of rules that governs how processes and users access resources.

  For example, prevention policies can contain a list of files and registry keys that no program or user can access. Prevention policies can contain a list of UDP and TCP ports that permit and deny traffic. Prevention policies can deny access to startup folders. Prevention policies define the actions to take when unacceptable behavior occurs.

- A detection policy is a collection of rules that are configured to detect specific events and take action. An agent can enforce one or more detection policies simultaneously.

  For example, detection policies can be configured to generate events when files and registry keys are deleted; when known, vulnerable CGI scripts are run on Microsoft Internet Information Server (IIS); when USB devices are inserted and removed from computers; and when network shares are created and deleted.

You use the management console to manage agent policies, and customize how agents communicate with the management server.

Agents report events to the management server for storage and are viewed in the management console. Agent log rules control the events that are logged for that agent. Logged data includes event date and time, event type, importance rating, and any prevention action performed.

Symantec Critical System Protection includes queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about events, agents, and policies. You can also create your own queries and reports.

Secure Sockets Layer X.509 certificate-based channel encryption secures communication between the management console and the management server, and between the agent and the management server.

About Symantec Critical System Protection features

Key features of Symantec Critical System Protection are as follows:

Computer security	Offers a flexible computer security solution that includes the following features: ■ Day-zero protection: stop malicious exploitation of systems and applications; prevent introduction and spread of malicious code ■ Hardened systems: lock down OS, applications, and databases; prevent unauthorized executables from being introduced or run ■ Integrated firewall: blocks inbound and outbound TCP/UDP traffic; administrator can block traffic per port, per protocol, per IP address or range ■ Maintain compliance by enforcing security policies on clients and servers ■ Buffer overflow protection ■ Real-time File Integrity Monitoring detection on AIX, Windows, and Linux.

Policies	Out-of-the-box security policies offer the following features:
	■ Intrusion prevention
	  ■ Proactive security against day-zero attacks
	  ■ Protection against buffer overflow and memory-based attacks
	  ■ Out-of-the-box operating system hardening
	  ■ External device protection
	  ■ Administrative privilege de-escalation
	■ Intrusion detection
	  ■ Sophisticated policy-based auditing and monitoring
	  ■ Log consolidation for easy search, archival, and retrieval
	  ■ Advanced event analysis and response capabilities
	  ■ File and registry protection and monitoring
	■ Policies configured with easy enable or disable style options
	■ Includes application policies for Microsoft® interactive applications

Management console	Central management console lets administrators create and deploy policies, manage users and roles, view alerts, and run reports. Features include the following: ■ Configure agent properties to determine how agents communicate with the management server and which events agents send to the management server ■ Customize policy options to increase or decrease restrictions enforced by a policy ■ Import and export custom and third-party policies

Agent	Agents enforce policy on the endpoint. Features include the following: ■ Control behavior by detecting and preventing specific actions that an application or user might take ■ Configure polling interval, real-time notification, log consolidation, log rotation ■ Apply policies to agents and groups agents ■ Load policies without restart ■ Real-time File Integrity Monitoring.
Management server	Provides secure communication to and from agents and the management console. Features include the following: ■ Agents automatically register with the management server during installation ■ Sends configuration changes to agents ■ Real-time and bulk logging of agent events
Platform support	Symantec Critical System Protection offers broad platform support for the following operating systems: ■ Microsoft Windows ■ Sun™ Solaris™ ■ Red Hat® Enterprise Linux ■ SUSE® Enterprise Linux ■ IBM® AIX® ■ Hewlett-Packard® HP-UX® ■ Hewlett-Packard Tru64 UNIX®

See the *Symantec Critical System Protection Platform and Feature Matrix* for more information on supported operating systems and agent features supported on each operating system.

See "System requirements" on page 20.

About policies, agents, events, and reports

The Symantec Critical System Protection policy library contains prevention and detection policies that you can use and customize to protect your network. A prevention policy is a collection of rules that governs how processes and users access resources. A detection policy is a collection of rules that are configured to detect specific events and take actions.

Agents are installed on computers to protect the computers from malicious activity by enforcing a policy.

You use the management console to manage agent policies and customize how agents communicate with the management server.

Agents report events to the management server for storage and are viewed in the management console. Agent log rules control the events that are logged for that agent. Logged data includes event date and time, event type, importance rating, and any prevention action performed.

Symantec Critical System Protection includes queries and reports with charts, graphs, and tables that provide detailed and aggregated summary data about events, agents, and policies. You can also create your own queries and reports.

Where to get more information

Product manuals for Symantec Critical System Protection are available on the Symantec Critical System Protection installation CD. Updates to the documentation are available from the Symantec Technical Support and Business Critical Services (BCS) Web sites.

The Symantec Critical System Protection product manuals are as follows:

- *Installation Guide*
- *Administration Guide*
- *Prevention Policy Reference Guide*
- *Detection Policy Reference Guide*
- *Agent Guide*
- *Release Notes*
- *Platform and Feature Matrix*

Table 1-1 lists additional information that is available from the Symantec Web sites.

Table 1-1 Symantec Web sites

Type of information	Web address
Public Knowledge Base Releases and updates Manuals and other documentation Contact options	http://www.symantec.com/business/support/
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://www.symantec.com/business/critical-system-protection
Business Critical Services Web access	https://www-secure.symantec.com/platinum/

Chapter 2

Planning the installation

This chapter includes the following topics:

About planning the installation

You can install the management console and management server on the same computer or on separate computers. You can install agents on any computer. All computers must run a supported operating system.

About network architecture and policy distribution

When you install Symantec Critical System Protection for the first time for testing purposes, you do not need to consider network architecture and policy distribution.

You can install a management server and management console, along with a few agents, and become familiar with Symantec Critical System Protection operations. When you are ready to roll out policies to your production environment, you can roll out different policies that are based on computing needs, and prevention and detection levels.

Areas where computing needs and prevention and detection levels might differ include the following:

- Local workstations
- Remote annex workstations
- Computers that run production databases
- Computers that are located in demilitarized zones (DMZ) such as Web servers, mail proxy servers, public DNS servers
- Virtualized environment

Prevention policies pushed to local and remote workstations would most likely be less restrictive than prevention policies pushed to production databases and DMZ servers.

Detection policies pushed to local workstations, production databases, and DMZ servers would also differ. Detection policies pushed to production databases and DMZ servers are more likely to offer more signatures than policies pushed to workstations.

You can distribute different policies to different computers by creating agent groups with the management console and then associating the agents with one or more groups during agent installation. You first create the groups using the management console, set the different policies for the groups, and then associate the agents with the groups during installation. It is not necessary, however, to associate an agent with a group during installation. You can perform this operation after installation.

System requirements

System requirements fall into the following categories:

- Operating system requirements
- Hardware requirements

Before you install

Before you install Symantec Critical System Protection, install the following:

- .Net 2.0 Framework or later
  This is required for installing or upgrading the Symantec Critical System Protection manager and evaluation database on supported Windows operating systems. You can download .Net 2.0 Framework or later for 32- and 64-bit Windows operating system.
- Windows Installer 2.0 or higher
  This is required for installing or upgrading the Symantec Critical System Protection manager on supported Windows operating systems.

Operating system requirements

This section lists the Symantec Critical System Protection operating system requirements for the management server, management console, and agent.

The Symantec Critical System Protection operating system requirements for the management server, management console, and agent is available in the *Symantec Critical System Protection Platform and Feature Matrix*.

Download the latest *Symantec Critical System Protection Platform and Feature Matrix* from the following Web site:

Symantec™ Critical System Protection Platform and Feature Matrix

Solaris packages

The agent installation checks for the presence of Solaris system packages.

The following core system packages are required for computers running Solaris 8.0, Solaris 9.0, and Solaris 10.0 operating systems:

- SUNWcar Core Architecture, (Root)
- SUNWkvm Core Architecture, (Kvm)
- SUNWcsr Core Solaris, (Root)
- SUNWcsu Core Solaris, (Usr)
- SUNWcsd Core Solaris Devices
- SUNWcsl Core Solaris Libraries
- SUNWloc System Localization

The following extended system packages are required for computers running Solaris 10.0 operating systems:

- SUNWxcu4, XCU4 Utilities
  Utilities conforming to XCU4 specifications (XPG4 utilities)
- SUNWesu Extended System Utilities

- SUNWuiu8 Iconv modules for UTF-8 Locale

VMware support

Symantec Critical System Protection supports the following VMware® software:

- VMware Workstation v5.0.0 and v5.5.4
- VMware ESX v3.0.1 and v3.0.2
- VMWare ESX 3.5 Host
- VMWare ESX 4.1 Host

The following Symantec Critical System Protection agents are supported on VMware guest operating systems:

- Windows NT Server
- Windows 2000 Professional/Server/Advanced Server
- Windows XP Professional
- Windows Server 2003 Standard/Enterprise 32-bit
- SUSE Enterprise Linux 8, 9, 10
- Red Hat Enterprise Linux ES 3.0, 4.0
- Solaris 10

Hardware support includes x86, EM64T, and AMD64. VMware must also support this hardware.

Hardware requirements

Table 2-1 lists the recommended hardware for the Symantec Critical System Protection components.

Table 2-1 Recommended hardware

Component	Hardware	Specific OS (if applicable)
Management console	150 MB free disk space 512 MB RAM Pentium III 1.2 GHz	

Table 2-1 Recommended hardware *(continued)*

Component	Hardware	Specific OS (if applicable)
Management server	1 GB free disk space (all platforms and databases) 2 GB RAM Pentium III 1.2 GHz	
	EM64T	Windows Server 2003 Standard/Enterprise x64
	AMD™64	Windows Server 2003 Standard/Enterprise x64
Agent	100 MB free disk space (all platforms) 256 MB RAM Pentium III 1.2 GHz	
	Sun SPARC™ 450 MHz	Solaris 8, 9, 10
	Sun SPARC32, SPARC64	Solaris 10
	Hewlett-Packard PA-RISC 450 MHz	HP-UX on PARISC
	IBM PowerPC® (CHRP) 450 MHz	AIX
	x86	Windows NT Server Windows Server 2003 32-bit Windows XP Professional Red Hat Enterprise Linux ES 3.0, 4.0 SUSE Linux Enterprise 8, 9, 10 Sun Solaris 10 (IDS only in non-global zone)
	EM64T	Windows Server 2003 Standard/Enterprise x64 Red Hat Enterprise Linux ES 3.0, 4.0 SUSE Linux Enterprise 8, 9, 10 Sun Solaris 10 (IDS only in non-global zone)

Table 2-1 Recommended hardware *(continued)*

Component	Hardware	Specific OS (if applicable)
	AMD™64	Windows Server 2003 Standard/Enterprise x64 Red Hat Enterprise Linux ES 3.0, 4.0 SUSE Linux Enterprise 8, 9, 10 Sun Solaris 10 (IDS only in non-global zone)
	IA32	SUSE Linux Enterprise 8
	IA64	HP-UX on Itanium 2 Red Hat 4.0 (IDS only)
	Alpha	Tru64 5.1B-3

See the *Symantec Critical System Protection Platform and Feature Matrix* to determine the specific operating system versions supported and the specific agent features for each operating system version.

Disabling Windows XP firewalls

Windows XP and Windows 2003 Server contain firewalls that are enabled by default. If these firewalls are enabled, you might not be able to establish network communications between the management console, management server, and agents.

Disabling Internet Connection Firewall

Windows XP with Service Pack 1 includes a firewall called Internet Connection Firewall that can interfere with network communications. If any of your computers run Windows XP, you can disable the Windows XP firewall before or after you install Symantec Critical System Protection components.

To disable Internet Connection Firewall

1. On the Windows XP taskbar, click **Start > Control Panel**.
2. In the Control Panel window, double-click **Network Connections**.

3 In the Network Connections window, right-click the active connection, and then click **Properties**.

4 On the Advanced tab, under Internet Connection Firewall, uncheck **Protect my computer and network by limiting or preventing access to this computer from the Internet**.

Disabling Windows Firewall

Windows XP with Service Pack 2 and Windows 2003 Server include a firewall called Windows Firewall that can interfere with network communications. If any of your computers run Windows XP with Service Pack 2 or Windows Server 2003, you can disable Windows Firewall before or after you install Symantec Critical System Protection components.

To disable Windows Firewall

1 On the Windows XP taskbar, click **Start > Control Panel**.

2 In Control Panel, double-click **Network Connections**.

3 In the Network Connections window, right-click the active connection, and then click **Properties**.

4 On the Advanced tab, under Internet Connection Firewall, click **Settings**.

5 In the Windows Firewall window, on the General tab, uncheck **On (recommended)**.

About using firewalls with Symantec Critical System Protection

To use Symantec Critical System Protection with a firewall, you need to configure the firewall to support communications by opening ports, or by specifying trusted services.

Note: All ports are default settings that you can change during installation.

You should note the following about using firewalls with Symantec Critical System Protection:

- The management server uses UDP port 1434 to query the MS SQL Server system and find the port used by the Symantec Critical System Protection instance. Once the MS SQL Server system returns the port for the Symantec Critical System Protection instance, the management server then connects to the instance using that port. Thus, your firewall must allow traffic from the

management server to the MS SQL Server system on UDP port 1434 and on the TCP port used by the Symantec Critical System Protection instance. You can get more information about MS SQL Server's use of ports at http://support.microsoft.com/default.aspx?scid=kb;EN-US;823938.

- The bulk log transfer feature of the Symantec Critical System Protection agent is implemented by the bulklogger.exe. If you have a host-based firewall that allows specific programs to access the Internet, you must allow bulklogger.exe as well as SISPISService.exe to access the Internet. The bulklogger.exe program uses the same ports as SISIPSService.exe. If you do not use the bulk log transfer feature, bulklogger.exe will not run.

Table 2-2 lists the services that you can permit to send and receive traffic through your firewalls.

Table 2-2 Components, services, and traffic

Component	Service	Traffic
Management console	Console.exe	Communicates with the management server using remote TCP ports 4443, 8006, and 8081.
Management server	SISManager.exe	Communicates with the management console using local TCP ports 4443, 8006, and 8081. Communicates with the agents using local TCP port 443. Communicates with remote production SQL servers using the remote TCP port that the SQL server uses for the server instance.
Agent	SISIPSService.exe sisipsdaemonbulklogger.exe	Communicates with the management server using local TCP port 2222, and remote TCP port 443.

About name resolution

To verify proper name resolution for the management server, use a utility, such as nslookup, to look up the host name for the management server. If you cannot resolve the host name of the management server, you will need to modify the DNS database or the host file that the client uses to look up host names.

About IP routing

As bastion hosts, firewalls traditionally incorporate some form of network address translation (NAT) between the two networks that the firewall bridges. For example, the management server may be on an internal network while the Agents are in a DMZ network, with a firewall between the two networks. Typically, the internal network IP addresses are hidden from the DMZ network, and are not routable from the DMZ network.

To allow the agents in the DMZ network to communicate with the management server on the internal network, use a DMZ IP address to represent the management server. Then, configure the firewall or router to forward requests for this IP address and port to the real, internal IP address of the management server. Open the agent port only if the agents are in a DMZ. Finally, configure the name database on the DMZ network to return the DMZ IP address for the management server instead of the internal IP address.

About intrusion prevention

The Symantec Critical System Protection agent installation kit includes an enable intrusion prevention option. When the enable intrusion prevention option is selected, the prevention features of Symantec Critical System Protection are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the management console.

When the enable intrusion prevention option is not selected, the prevention features of Symantec Critical System Protection are completely disabled for the agent. The IPS drivers are not loaded on the agent computer, and the agent does not accept prevention policies from the management console.

Symantec strongly recommends that you enable the intrusion prevention option when installing agents. Changing this option after installation (to disable or re-enable it) requires logging on to the agent computer, running the Agent Config Tool, and rebooting the agent computer.

If you are only interested in the detection features of Symantec Critical System Protection, Symantec recommends that you select the enable intrusion prevention option during agent installation, and use the Null prevention policy to avoid any blocking. If you later decide to use the prevention features of Symantec Critical System Protection, then you simply apply one of the prevention policies that are included with the product. Applying a policy requires no logging onto the agent computer, no running the agent config tool, no rebooting the agent computer.

By default, the enable intrusion prevention option is selected during Symantec Critical System Protection agent installation.

Symantec Critical System Protection supports intrusion prevention on computers that run Windows, Solaris, AIX, and Linux operating systems.

About simple failover

Symantec Critical System Protection includes simple failover. Should the primary management server fail, simple failover lets agents automatically switch to the next management server in an ordered list of alternate servers.

Simple failover enables you to deploy a set of front-end Tomcat servers without reconfiguring your IT infrastructure. The ordered list of management server host names or IP addresses is maintained by the Symantec Critical System Protection agent configuration.

Another use for simple failover is static load balancing. With static load balancing, you manually assign a set of agents to each Tomcat server. Each agent can fail to a different Tomcat server if its primary server becomes inaccessible.

How simple failover works

Simple failover works as follows:

- When the IPS Service starts up, it uses the first server in the ordered list of management servers. The first server in the ordered list is considered the primary management server; the remaining servers are alternate servers. The IPS Service uses server #1 as long as communication with the server is successful.
- At startup, the IPS Service always uses the first server in the ordered list of management servers, regardless of which server was in use when the IPS Service was shut down.
- When the ordered list of management servers changes, the IPS Service immediately attempts to connect to the first server in the new list.
- When communication with a server fails, the IPS Service uses the next server in the ordered list of management servers. When communication with the last server fails, the IPS Service uses the first server in the list. The IPS Service loops through the ordered list of management servers indefinitely.
- When the IPS Service switches to a new management server, it logs the action.
- Once the IPS Service fails away from the first server in the ordered list, it periodically checks if server #1 is back, based on the fail back interval.
  See "About the fail back interval" on page 29.
- When the fail back interval expires, the IPS Service checks if server #1 is available. If server #1 is available, the IPS Service starts using it immediately.

If server #1 is not available, the IPS Service continues to use the current alternate server; the IPS Service does not traverse the entire ordered list of management servers.

Simple failover with static load balancing works as described in the following example:

- Suppose you have two Tomcat servers pointing to a single database, and two agents.
- You initially configure Agent1 with a management server list of Tomcat1, Tomcat2. You initially configure Agent2 with a management server list of Tomcat2, Tomcat1.
- After installation completes, Agent1 should be talking to Tomcat1, and Agent2 should be talking to Tomcat2.
- Take Tomcat1 off the network.
- Agent1 should fail talking to Tomcat1 and switch to Tomcat2. Now both agents are talking to Tomcat2.
- Put Tomcat1 back on the network.
- Wait longer than the fail back interval.
- Agent1 should fail back to Tomcat1. Agent2 continues to use Tomcat2. Everything is back to the initial state; both agents should be communicating successfully with their original Tomcat servers.

About the fail back interval

Once an agent fails away from the first server in an ordered list, the agent periodically checks if the first server is back. The agent uses a fail back interval to determine when to perform this server check. By default, the agent performs the server check every 60 minutes.

For example, suppose you configured three management servers. The primary server #1 and alternate server #2 have failed; alternate server #3 is working. When the fail back interval expires, the agent checks if server #1 is available. If server #1 is available, the agent immediately starts using server #1. If server #1 is not available, the agent continues to use server #3; it does not recheck the ordered list of servers. The agent resets the fail back interval, so it can perform future server checks.

Specifying the management server list for an agent

To use simple failover for an agent, you must provide the list of primary and alternate management servers using one of the following methods:

- If you are installing Symantec Critical System Protection for the first time, you can provide the list of primary and alternate management servers during agent installation.
- If you are upgrading to Symantec Critical System Protection 5.1.1 or higher, you provide the list of primary and alternate management servers using the CSP_Agent_Diagnostics detection policy or the agent config tool.
  To use simple failover, you must upgrade the management server, management console, and agent to version 5.1.1 or higher.
  See "Migrating legacy installations of Symantec Critical System Protection" on page 101.

The primary and alternate management server host names or IP addresses configured for a single agent must be Tomcat servers that talk to a single Symantec Critical System Protection database. Using multiple databases can result in unexpected agent behavior.

The primary and alternate management servers must use the same server certificate and agent port.

About log files

Symantec Critical System Protection uses log files to record events and messages related to agent and management server activity.

Multiple versions of a log file may exist, as old versions are closed and new versions are opened. The versions are denoted by a number (for example, SISIDSEvents23.csv, sis-console.3.log).

See the *Symantec Critical System Protection Administration Guide* for more information on log files.

Table 2-3 lists the Symantec Critical System Protection agent log files.

Table 2-3 Agent log files

File name	Description	Default location
SISIPSService.log	This log file contains events that are related to the following: ■ Agent service operation ■ Applying policies and configuration settings ■ Communication with the management server	Windows:Program Files\Symantec\Critical System Protection\Agent\scsplog\ UNIX:/var/log/scsplog/

Table 2-3 Agent log files *(continued)*

File name	Description	Default location
SISIDSEvents*.csv	This log file contains all events recorded by the Symantec Critical System Protection agent. The asterisk in the file name represents a version number.	Windows:Program Files\Symantec\Critical System Protection\Agent\scsplog\ UNIX:/var/log/scsplog/

Table 2-4 lists the management server log files.

Table 2-4 Management server log files

File name	Description	Default location
sis-agent.*.log	This log file is used for agent activity. The asterisk in the file name represents a version number.	Windows:Program Files\Symantec\Critical System Protection\Server\Tomcat\logs
sis-alert.*.log	This log file is used for alert activity. The asterisk in the file name represents a version number.	Windows:Program Files\Symantec\Critical System Protection\Server\Tomcat\logs
sis-console.*.log	This log file is used for console activity. The asterisk in the file name represents a version number.	Windows:Program Files\Symantec\Critical System Protection\Server\Tomcat\logs
sis-server.*.log	This log file is used for general server messages. The asterisk in the file name represents a version number.	Windows:Program Files\Symantec\Critical System Protection\Server\Tomcat\logs

Table 2-5 Installation log files

File name	Operating System	Default location
Server \SISManagerSetup.log Console \SISConsoleSetup.log Agent \SISAgentSetup.log	Windows	On 32-bit operating system: C:\Program Files\Symantec\Critical System Protection\ On 64-bit operating system: C:\Program Files (x86)\Symantec\Critical System Protection\
/var/log/scsplog/ agent_install.log	Unix	-

What to do after installation

You can begin enforcing the Symantec Critical System Protection policies on agents immediately after agent installation and registration with the management server.

Symantec recommends that you first apply a policy to a few agents, and then verify that the agent computers are functioning properly with the applied policy.

See the *Symantec Critical System Protection Administration Guide* for information about applying policies to agents.

Chapter 3

Installing Symantec Critical System Protection on Windows

This chapter includes the following topics:

About installing Symantec Critical System Protection on Windows

If this is a first-time installation, you should install, configure, and test Symantec Critical System Protection components in a test environment.

You should install the Symantec Critical System Protection in the order listed:

- Management server
- Management console
- Agent

You can install the management console and management server on the same computer or on separate computers. You can install agents on any computer. All computers must run a supported operating system.

The management server and management console are supported on Windows operating systems.

Note: The installation directory names for the management console and management server must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII and non-printable ASCII characters are not supported.

About port mapping

When you install the Symantec Critical System Protection components, you must specify port through which the components communicate. In a few instances, these ports must match.

Table 3-1 shows the Symantec Critical System Protection ports that must have matching numbers.

Table 3-1 Port mapping

Management server	Management console	Agent
Agent Port		Agent Port
Console Port	Port	
Web server Administration Port	Admin Port	

Bypassing prerequisite checks

The Windows installation kit lets you bypass some of the prerequisite checks for agent and management server installation. You can use this feature if you know the installation kit is incorrectly failing a prerequisite.

When you use the bypass prerequisite checks feature, the installation kit displays all errors and warnings about prerequisite check failures. However, instead of terminating the installation, you may choose to continue.

When you run the installation kit in interactive mode, you are asked if you want to continue. When you run the installation kit in silent mode, the prerequisite failure is logged and the installation continues.

To enable the bypass prerequisite checks feature, do the following:

- (Agent only) For silent installs, set the ENABLE_BYPASS_CHECKS variable to a nonzero value.
- For interactive installs, the presence of the file scsp-check-bypass.txt, either in the installer directory or %temp% folder will confirm the bypass enabling.

The Windows installation kit does not remove the scsp-check-bypass.txt file upon successful installation.

You can bypass the following checks when installing the Symantec Critical System Protection agent:

- Agent install disk space checks that are performed apart from Windows Installer (MSI) engine
- Service user account (allow domain users or local users even though the installer can not confirm the required rights and privileges)
- Existence of AppFire 4.5

You can bypass the following checks when installing the Symantec Critical System Protection management server:

- Existence of AppFire 4.5
- Disk space checks
- User privilege and rights check for service user account
- Microsoft Data Access (MDAC) version

About installing a database linked to a SQL Server instance

The Symantec Critical System Protection installation lets you locally install an SQL Server 2005 Express evaluation database, and also lets you locally or remotely install an evaluation or production database linked to an instance of SQL Server. All installations allocate 100 MB for the database. SQL Server automatically allocates more space when it is needed.

If you elect to install a database linked to an instance of SQL Server, Symantec recommends that you first install a new instance of SQL Server that conforms to the installation requirements. You can install a database to an older, existing instance, but the instance must be configured properly or your database installation will fail. For example, if the authentication configuration is not set to Mixed Mode, your installation will fail.

About SQL Server installation requirements

You can install the SQL Server on the same machine that you plan to install Symantec Critical System Protection management server, or on a different machine.

The Symantec Critical System Protection Manager supports Microsoft SQL Server 2005 and all newer versions. This includes all "editions", e.g. Express, Standard, etc., and includes all service packs.

The following information applies to the SQL Server software.

When you install the instance of SQL Server, do the following:

- Do not accept the default instance name. Use SCSP (the default when you install Symantec Critical System Protection management server), or some other name. Type the same name when installing Symantec Critical System Protection management server.
  A database named scspdb, the default, will be created in this instance when you install Symantec Critical System Protection management server.
- Set authentication configuration to Mixed Mode (Windows authentication and SQL Server authentication).
- Set the sa password when you set Mixed Mode authentication. You will type this password when you install Symantec Critical System Protection management server.

After you install the instance of SQL Server, you must do the following:

- (SQL Server 2000) Apply SQL Server Service Pack 4.

- Select to authenticate using SQL Server credentials.
- Register the instance.
  Registering the instance also starts the instance.

When you register the instance of SQL Server, you must do the following:

- Set the authentication mode to SQL Server authentication.
- Configure the connection option to log on automatically through SQL authentication with the sa account, and type the sa password.
- If registration fails due to authentication failure, display the properties available from the server messages dialog box, and type the sa password again.

After you register the instance, you must do the following:

- Use the networking utility to verify that NamedPipes and TCP/IP are enabled protocols. If they are not enabled, enable them.

You are then ready to install Symantec Critical System Protection management server.

About installing on computers that run Windows 2000

If you want to install Microsoft SQL Server and Symantec Critical System Protection management server on different computers, and if the computer on which you want to install Symantec Critical System Protection management server runs Windows 2000 Professional or Server, you must first upgrade the Microsoft Data Access Components (MDAC) version on that computer. If you do not upgrade the MDAC version, your installation will fail.

By default, Windows 2000 Professional and Server with Service Pack 4 install MDAC version 2.5 Service Pack 3. You must upgrade MDAC on that computer to version 2.7 SP1 or higher to be compatible with the MDAC version installed by Microsoft SQL Server.

If the MDAC version is less than the required minimum, the installation will direct you to the MDAC installer on the installation CD, and then abort the installation. You must install the minimum version of MDAC, and then restart the management server installation.

You can also download the latest MDAC version from the Microsoft Web site. The Web site also makes an MDAC Component Checker available for download that tells you what version of MDAC is on your computers.

Configuring the temp environment variable

The installation packages unpack installation files into the directory that is specified by the TEMP environment variable. The volume that contains this directory must have at least 200 MB of available disk space. If this volume does not have the required disk space, you must change your TEMP environment variable or your installation will fail.

Note: After successful management server and management console installation, SISManagerSetup.log and SISConsoleSetup.log appear in the \Server and \Console directories respectively. If installation is not successful or cancelled, the log files appear in the directory specified by the TEMP environment variable.

To configure the temp environment variable

1. At a command prompt, type **set**, and then press **Enter**.
2. Write down the value that appears for TEMP.
3. Check the disk space for the volume that is specified for TEMP.
4. If the volume does not contain enough disk space, in a command prompt, type the following command to change the volume and directory:

   ```
   set temp=<volume>.\<directory path>
   ```

5. Press **Enter**.

Installing the management server

The management server coordinates events from agents, and provides database access to the Symantec Critical System Protection management console. The management server secures communication with other components by using SSL to encrypt the communication channel.

You must log on to an Administrator account to install the management server.

About installation types and settings

When installing the management server, you can install the following installation types:

- Evaluation installation that runs SQL Server 2005 Express on the local system
  You can install an evaluation installation of SQL Server 2005 Express. The CD installs the server and database automatically.

- Evaluation installation that uses existing MS SQL instance
  You can install an evaluation installation on SQL Server. The SQL Server instance must exist and be running before you perform the installation. The SQL Server can be local or remote.
- Production installation with Tomcat and database schema
  You can install a production installation that installs Tomcat and creates the database schema. This option installs on SQL Server. The SQL Server instance must exist and be running before you perform the installation. The SQL Server can be local or remote.
- Tomcat component only
  You can install a production installation that only installs the Tomcat component, and points to a remote database. This option requires that you provide the file paths to a server.xml file and a server-cert.ssl file from an installed management server.

Warning: The management server installation makes network connections to populate both the evaluation and production databases. For local installations, these connections are internal. Quite often, host-based firewalls either block these connections or display messages that prompt you to decide whether to allow the connections. In both situations, the connections time out and the database is not set up correctly.

Before starting the management server installation, do one of the following:

- Permit all programs to initiate connections on port 1433 or your site-specific SQL Server port. Several programs connect to the database during the installation process.
- Disable all host-based firewalls on the management server computer and on the database server if it is on a remote computer. You can enable the firewalls after installation completes.

Management server installation settings and options

Installation prompts you to enter a series of values consisting of port numbers, user names, passwords, and so forth. Each database that you can install uses different default settings and options for the management server and database. Also, some settings for evaluation installation are hard-coded, while the same settings for production are variables that you can change. For example, the database name scspdb is hard-coded for evaluation installation, but is a variable that you can change for production installation.

Table 3-2 describes the management server installation settings and options.

Table 3-2 Management server installation settings

Setting	Default/options	Description
Installation type	Evaluation Installation, Install SQL Server 2005 Express on the local system You have the following options: Evaluation installation: ■ Install SQL Server 2005 Express on the local system ■ Use an existing MS SQL instance Production installation: ■ Install Tomcat and create the database schema ■ Install Tomcat Component ONLY	Select the type of installation. If you install a database on SQL Server, the instance must be running. The Install Tomcat Component Only option requires that you provide the file path to the following files from an installed management server: ■ server.xml ■ server-cert.ssl
Destination Folder	C:\Program Files\Symantec\Critical System Protection\Server	The directory location for the management server.
Agent port	443	The port that is used to communicate with the agent. If you install on a computer that runs a Web server, you must either stop the Web server from running permanently, or enter a different port number. This number maps to the Agent Port number that is used when installing the agent. See See "About the installation settings and options" on page 54. See See "About port mapping" on page 34.

Table 3-2 Management server installation settings *(continued)*

Setting	Default/options	Description
Console port	4443	The port that is used to communicate with the management console. This number maps to the Port number that is used when configuring the management console. See See "Configuring the management console" on page 50. See See "About port mapping" on page 34.
Web server shutdown port	8006	The port that is used to shut down the management server.
Web server administration port	8081	The port that is used to administer the management server. This number maps to the Admin Port number that is used when configuring the management console. See See "Configuring the management console" on page 50. See See "About port mapping" on page 34.
SQL Server 2005 Express Install Path	C:\Program Files\Symantec\Critical System Protection\Server You have the following options: ■ SQL Eval: NA ■ SQL Prod: NA	The directory in which to install the SQL Server 2005 Express server.
SQL Server 2005 Express Data Path	C:\Program Files\Symantec\Critical System Protection\Server You have the following options: ■ SQL Eval: NA ■ SQL Prod: NA	The directory in which to install the SQL Server 2005 Express database.

Table 3-2 Management server installation settings *(continued)*

Setting	Default/options	Description
Service user name	LocalSystem You have the following options: ■ SQL Eval: hard-coded ■ SQL Prod: variable	The account that is used to start the management server services. For a SQL Production installation, you can specify a different account that exists on the computer. This account must have administrator privileges. Enter the account using <domain>\<username> format.
Host name	Current host IP address You have the following options: ■ SQL Eval: variable ■ SQL Prod: variable	The IP address or fully qualified host name of the computer on which you install the SQL database.
Database Instance	SCSP You have the following options: ■ SQL Eval: variable ■ SQL Prod: variable	The name of the SQL Server instance. The instance must be running.
sa Username	sa You have the following options: ■ SQL Eval: variable ■ SQL Prod: variable	The user name for the SQL Server built-in sa account. You can accept the default and proceed with the normal installation, or you can specify the password for a privileged user account.
sa password	none You have the following options: ■ SQL Eval: Must match existing password ■ SQL Prod: Must match existing password	The password that is associated with the database sa account. The password must be 8 to 19 characters long, not begin with _ and contain at least two two-letter characters. The password must contain only letters, numbers, #, @, and _. The password cannot contain =. If you install a SQL database, you must type the same sa password that is used on the SQL Server.

Table 3-2 Management server installation settings *(continued)*

Setting	Default/options	Description
Database name	SCSPDB You have the following options: ■ SQL Eval: hard-coded ■ SQL Prod: variable	The name of the SQL Server instance. If you install to a production database, the instance name must exist.
Enable Unicode Storage	enabled	This option is used by production installation, install Tomcat and create the database schema. The option is for use with international operating systems.
SCSP Database Owner user name	scspdba You have the following options: ■ SQL Eval: hard-coded ■ SQL Prod: variable	The name of the account that is used to administer the database. The installation creates this account and password.
SCSP Database Owner user password	none You have the following options: ■ SQL Eval: hard-coded to the sa password that you type ■ SQL Prod: variable	The password that is associated with the database owner user account, which is used for installations and upgrades. The password must be 8 to 19 characters long, not begin with _ and contain at least two two-letter characters. The password must contain only letters, numbers, #, @, and _. The password cannot contain =.
SCSP Database Guest user name	scspdba You have the following options: ■ SQL Eval: NA ■ SQL Prod: variable	The name of the account that is used to access the database with read-only guest privileges.

Table 3-2 Management server installation settings *(continued)*

Setting	Default/options	Description
SCSP Database Guest user password	none You have the following options: ■ SQL Eval: NA ■ SQL Prod: variable	The password that is associated with the database guest user account. The password must be 8 to 19 characters long, not begin with _ and contain at least two two-letter characters. Also, the password must contain only letters, numbers, #, @, and _. The password cannot contain =.

Installing evaluation installation that runs SQL Server 2005 Express on the local system

This evaluation installation option installs a management server that runs a local SQL Server 2005 Express evaluation database.

Before performing the installation, you should note the following:

- The management server installation installs the server and database automatically.
- During the management server installation, you must create and enter a password that will be associated with the database sa account.

To install evaluation installation that runs SQL Server 2005 Express on the local system

1. Insert and display the installation CD, and then double-click **server.exe**.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Installation Type** panel, click **Evaluation Installation**, click **Install SQL Server 2005 Express on the Local System**, and then click **Next**.
5. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.

6 In the **Server Configuration** panel, accept or type new port values, and then click **Next**.

If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.

7 In the **Database Selection** panel, change the default server and database directory locations if necessary.

The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.

8 In the **Database Selection** panel, in the Password and Confirm Password boxes, type the password that will be associated with the database sa account, type the password again to confirm, and then click **Next**.

9 In the **Ready to Install the Program** panel, click **Install**.

10 When the **InstallShield Wizard Completed** panel appears, click **Finish**.

Installing evaluation installation using existing MS SQL instance

This evaluation installation option installs the management server with a local or remote evaluation database on SQL Server.

Before performing the installation, you should note the following:

- Your SQL Server instance must exist and be running before you start the installation.
- The sa account must already exist and you must provide the accurate password for the sa account during the management server installation.

To install evaluation installation that uses existing MS SQL instance

1 Insert and display the installation CD, and then double-click **server.exe**.

2 In the **Welcome** panel, click **Next**.

3 In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.

4 In the **Installation Type** panel, click **Evaluation Installation**, then click **Use an Existing MS SQL Instance**, and then click **Next**.

5 In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.

6 In the **Server Configuration** panel, accept or type new port values, and then click **Next**.

If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.

7 In the **Database Selection** panel, specify the database parameters, and then click **Next**.

Host Name	Type the IP address or fully qualified domain name of the SQL Server.
Database Instance	Type the name of the existing SQL Server instance on which you want to install the database.
sa Privileged User	Accept or change the sa user name.
Password Confirm Password	Type the same password that is used on the SQL Server, type the password again to confirm.

8 In the **Ready to Install the Program** panel, click **Install**.

9 When the **InstallShield Wizard Completed** panel appears, click **Finish**.

Installing production installation with Tomcat and database schema

This production installation option installs Tomcat and creates the database schema. The option installs the management server with a local or remote production database on SQL Server.

Before performing the installation, you should note the following:

- Your SQL Server instance must exist and be running before you start the installation.
- The sa account must already exist and you must provide the accurate password for the sa account during the management server installation.
- All other accounts (owner, guest, and internal accounts) must not exist in the instance. The management server installation creates these accounts and aborts if it cannot create them.
- The database name that you enter into the management server installation must not exist in the instance. The management server installation creates these accounts and aborts if it cannot create them.

To install production installation with Tomcat and database schema

1. Insert and display the installation CD, and then double-click **server.exe**.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Installation Type** panel, click **Production Installation**, click **Install Tomcat and create the database schema**, and then click **Next**.
5. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
6. In the **Server Configuration** panel, accept or type new port values, and then click **Next**.

   If you enter port numbers that are in use, error messages appear until you enter port numbers that are not in use.
7. In the **Service User Configuration** panel, do one of the following:

   Click **Use Local System Account**, and then click **Next**.

   Click **Use an alternate Account**, type a user name in the Username box using <domain>\<username> format, type the same password in the Password and Confirm Password boxes, and then click **Next**.
8. In the **Database Selection** panel, specify the database parameters, and then click **Next**.

Host Name	Type the IP address or fully qualified domain name of the SQL Server.
Database Instance	Type the name of the existing SQL Server instance on which you want to install the database.
sa Privileged User	Accept or change the sa user name.
Password Confirm Password	Type the same password that is used on the SQL Server, type the password again to confirm.

9. In the **Database Configuration** panel, specify the database parameters, and then click **Next**.

Database Name	Type the name of the database to install.

Enable Unicode Storage	The option is for use with international operating systems.
SCSP Database Owner	Under SCSP Database Owner, do the following: ■ In the User name box, type the name of the SCSP Database Owner. ■ In the Password and Confirm Password boxes, type the password that is associated with the SCSP Database Owner, and then type the password again to confirm.
SCSP Database Guest User	To create an SCSP database guest user, do the following under SCSP Database Guest User: ■ Select **Create a Guest User**. ■ In the User name box, type the guest User name. ■ In the Password and Confirm Password boxes, type the password that is associated with the SCSP Database Guest User, and then type the password again to confirm.

10 In the **Ready to Install the Program** panel, click **Install**.

11 When the **InstallShield Wizard Completed** panel appears, click **Finish**.

Installing Tomcat component only

This production installation option installs only the Tomcat component. You can use this option to point multiple Tomcat servers to a single management server database on a dedicated system. The Tomcat only option is useful if you want to create a set of identical Tomcat servers for load balancing or failover.

The Tomcat only option requires that you provide the file path to the following files from an installed management server:

- server.xml file
- server-cert.ssl

These files are located in the default management server installation directory:

You should do the following changes in the server.xml as mentioned below:

- If the primary server is installed on 32-bit operating system and the secondary server is installed on 64-bit operating system or vice-versa, then you should modify the keystoreFile path for server-cert.ssl file in server.xml on Tomcat-only server.

  On 32-bit operating system, the keystoreFile path is C:\Program Files\Symantec\Critical System Protection\Server\server-cert.ssl and on 64-bit

operating system, the keystoreFile path is C:\Program Files(x86)\Symantec\Critical System Protection\Server\server-cert.ssl.

- The URL for resources Database-Console and Database-Agent cannot contain localhost or 127.0.0.1 in the server.xml file on Tomcat-only server. You must use the IP address or the host name of the primary server.

C:\Program Files\Symantec\Critical System Protection\Server

Note: If the management server database is on a Tomcat system instead of a dedicated system, you must specify the real IP (not localhost) for the initial installation.

To install Tomcat component only

1. Insert and display the installation CD, and then double-click **server.exe**.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Installation Type** panel, click **Production Installation**, click **Install Tomcat component ONLY**.
5. In the **Installation Type** panel, specify the file paths to server.xml and server-cert.ssl from an installed management server, and then click **Next**.
6. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

   The directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
7. In the **Service User Configuration** panel, do one of the following:

   Click **Use Local System Account**, and then click **Next**.

   Click **Use an alternate Account**, type a user name in the Username box using <domain>\<username> format, type the same password in the Password boxes, and then click **Next**.
8. In the **Ready to Install the Program** panel, click **Install**.
9. When the **InstallShield Wizard Completed** panel appears, click **Finish**.

Installing and configuring the management console

After you install the management console, you must configure the management console before you can use it.

You must log on to an Administrator account to install the management console.

Installing the management console

By default the management console is installed in the following directory:

C:/Program Files/Symantec/Critical System Protection/Console

Management console installation does not prompt you to enter port numbers or server names. You enter this information after installation.

To install the management console

1. On the installation CD, double-click **console.exe**.
2. In the **Initial installation** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Destination Folder** panel, change the folder if necessary, and then click **Next**.

   The installation directory name must contain printable ASCII characters only. Multi-byte, double-byte, hi-ASCII, and non-printable ASCII characters are not supported.
5. In the **Ready to Install the Program** panel, click **Install**.
6. When the **InstallShield Wizard Completed** panel appears, click **Finish**.

Configuring the management console

Configuration prompts you to enter a series of values consisting of port numbers, passwords, and a server name. In a few instances, the port numbers must match the port numbers that were specified during management server installation.

Table 3-3 describes the management console configuration settings and options.

Table 3-3 Management console configuration settings

Setting	Default	Description
Server name	Localhost Server	The name of the management server that you want to manage from the management console. This value is used for user interface identification purposes only, and appears on the Login window. The name can be any value.
Host	local host	The IP address or fully qualified host name of the management server computer that you want to manage from the management console.
Port	4443	The Console Port number that was used during management server installation. See See "Management server installation settings and options" on page 39. See See "About port mapping" on page 34.
Admin port	8081	The Web server Administration Port number that was used during management server installation. See See "Management server installation settings and options" on page 39. See See "About port mapping" on page 34.

Table 3-3 Management console configuration settings *(continued)*

Setting	Default	Description
Use encrypted communications	Enabled	Check **Use encrypted communications** to use Secure Sockets Layer (SSL) X.509 certificate-based channel encryption for Symantec Critical System Protection. SSL X.509 certificate-based channel encryption secures communication between the management console and the management server, and between the agent and the management server. If you feel that your system provides adequate firewall security and you do not want to use SSL X.509 certificate-based channel encryption for Symantec Critical System Protection, uncheck **Use encrypted communications**. After you uncheck **Use encrypted communications**, you must edit the server.xml file, found on the management server, in the <Server_Install_Root>\tomcat\conf directory. See the *Symantec Critical System Protection Administration Guide* for instructions on editing server.xml.
Password	none	The password that is associated with the symadmin user name, which you create the first time you start the management console.

To configure the management console

1. Click **Start > Programs > Symantec Critical System Protection > Management Console**.
2. In the **Login** window, click the green plus sign icon.
3. In the **New Server Configuration** panel, replace New Server with the name that you want to use to identify your server.
4. In the **New Server Configuration** panel, specify the server configuration parameters, and then click **OK**.
5. In the **Login** window, type symadmin in the User name box, select the new server that you added, and then click **Login**.
6. In the **Verify Server Certificate** panel, select **Always accept this certificate**, and then click **OK**.
7. In the **Set Password** panel, in the Password and Confirm Password boxes, type the password to associate with the symadmin user name, type the password again to confirm.

Installing a Windows agent

The Symantec Critical System Protection agent enforces policy on the endpoints. Each agent enforces rules that are expressed in policies, thereby controlling and monitoring application (process) and user behavior.

You must log on to an Administrator account to install a Windows agent.

Note: Windows agents must be restarted after installation or upgrade.

About the SSL certificate file

The Windows agent installation requires access to a copy of the SSL certificate file that was created during management server installation. The certificate file is named Agent-cert.ssl, and is located in the management server installation directory. The default management server installation directory is as follows:

C:\Program Files\Symantec\Critical System Protection\Server

To place the certificate on a computer that does not run the management server, do the following:

- On the management server that will be used to manage the agent, locate the server installation directory and copy Agent-cert.ssl to removable media.

Optionally, you can copy the file from mapped network drives or network shares.

- On the computer on which the agent will be installed, create a directory and then copy Agent-cert.ssl into the directory.
  The directory path name cannot contain spaces.

About the installation settings and options

Installation prompts you to enter a series of Windows agent values consisting of port numbers, management server name, and so forth.

Note: The agent does not support IP aliases. If your network card is bound to more than one IP address, the agent uses the first IP address on the network card.

Table 3-4 describes the Windows agent installation settings and options.

Table 3-4 Windows agent installation settings

Setting	Default	Description
Installation Directory	C:\Program Files\Symantec\Critical System Protection\Agent	The installation directory for the agent.
Logs File Directory	C:\Program Files\Symantec\Critical System Protection\Agent	The installation directory prefix for the <prefix dir>/scsplogs subdirectory. The installation creates an scsplog folder under the folder that you specify.
Agent Name	Host name of agent computer	The agent name. After installation, you can change the agent name using the management console.
Polling Interval	300 seconds	The interval that the agent uses to poll the management server for policy and configuration updates.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Enable Intrusion Prevention	Enabled	Indicates whether to enable intrusion prevention. When enabled, the prevention features of Symantec Critical System Protection are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the management console. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.exe tool in the \Agent\IPS\bin directory with the -i option, and restart the computer. The -i option toggles the intrusion prevention service on and off. Symantec strongly recommends that you enable intrusion prevention.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Enable Real-time Notification	Enabled	Indicates whether to enable real-time notification. In addition to using the polling interval, agents can use real-time notification to obtain configuration changes. With real-time notification, the management server sends a real-time notification message to an agent as configuration changes occur. Upon receiving the notification, the agent queries the management server for the changes. When real-time notification is disabled, the management server does not send any messages to the agent and relies on the polling interval to update the agent.
Notification port	2222	The port that is used to receive real-time notifications from the management server. You can change this port after installation using the management console to change the agent properties.
Primary Management Server	localhost	The IP address or fully qualified host name of the management server that will manage the agent.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Agent Port	443	The Agent Port number that was used during management server installation. See See "Management server installation settings and options" on page 39. See See "About port mapping" on page 34.
Alternate Management Servers	none	An ordered list of optional alternate management servers used for failover. For each alternate management server, specify the IP address or fully qualified host name. Specify the servers in a comma-separated list. See "About simple failover" on page 28.
Management Server Certificate	none	The directory location of the SSL certificate file, Agent-cert.ssl. The installation requires access to a copy of the SSL certificate file that was created during management server installation. The file is located in the management server installation directory. All primary and alternate management servers must use the same certificate file. See "About the SSL certificate file" on page 53.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Common Configuration Group	none	The name of an existing common configuration group for this agent to join. An agent is placed in the default common configuration group (named Common Configuration), unless you specify another configuration group that already exists in the management console. After installation, you can change the group assignment using the management console.
Prevention Configuration Group	none	The name of an existing prevention configuration group for this agent to join. An agent is placed in the default prevention configuration group (named Configuration), unless you specify another configuration group that already exists in the management console. After installation, you can change the group assignment using the management console.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Prevention Policy Group	none	The name of an existing prevention policy group for this agent to join. An agent is placed in the default prevention policy group (named Policy), unless you specify another policy group that already exists in the management console. After installation, you can change the group assignment using the management console.
Detection Configuration Group	none	The name of an existing detection configuration group for this agent to join. An agent is placed in the default detection configuration group (named Configuration), unless you specify another configuration group that already exists in the management console. After installation, you can change the group assignment using the management console.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Detection Policy Group	Windows	The name of an existing detection policy group for this agent to join. You can specify multiple groups using commas between the group names. You may optionally include the name of an existing detection policy domain in the group path/name. You may include the domain name with or without the group name. An agent is placed in the default Policy/Windows detection policy group, unless you specify another policy group that already exists in the management console. After installation, you can change the group assignment using the management console.

Table 3-4 Windows agent installation settings *(continued)*

Setting	Default	Description
Use LocalSystem account Use an alternate account	Use LocalSystem account	The service user name account that registers services for the agent. Do one of the following: ■ Select **Use LocalSystem account** to accept the default LocalSystem account. ■ Select **Use an alternate account** to select a different account. In the Username box, type the user name for the alternate account. In the Password boxes, type the password twice. The alternate account must have Administrator privileges. If the account does not exist, it will be created. If a domain account is specified, type the user name in the format <domain>/<username>. Consult your system administrator before selecting an alternate account.

Installing the Windows agent software

The installation CD contains the following executable for installing the agent software:

agent.exe — Use agent.exe to install the agent software on computers that run supported Windows operating systems.

To install the Windows agent software

1. On the installation CD, double-click **agent.exe**.
2. In the **Welcome** panel, click **Next**.
3. In the **License Agreement** panel, select **I accept the terms in the license agreement**, and then click **Next**.
4. In the **Destination Folder** panel, change the folders if necessary, and then click **Next**.
5. In the **Agent Configuration** panel, accept or change the default settings, and then click **Next**.

   Ensure that **Enable Intrusion Prevention** is checked.
6. In the **Management Server Configuration** panel, in the Primary Management Server box, type the fully qualified host name or IP address of the primary server that is used to manage this agent.

   If you changed the Agent Port setting during management server installation, in the Agent Port box, type a port number that matches.
7. (Optional) In the **Management Server Configuration** panel, in the Alternate Management Servers box, type the fully qualified host name or IP address of the alternate servers that are used for failover for this agent.

   Type the servers in a comma-separated list.
8. In the **Management Server Configuration** panel, accept the directory for the SSL certificate Agent-cert.ssl, or click **Browse** to browse to and locate Agent-cert.ssl.

   Access to a copy of the SSL certificate Agent-cert.ssl is required to connect to the management server. All primary and alternate management servers must use the same certificate.
9. In the **Management Server Configuration** panel, click **Next**.
10. (Optional) In the **Agent Group Configuration** panel, in the group boxes, type the group names that you created with the management console.

    You may add multiple detection policy group names separated with commas. You may include the name of an existing detection policy domain in the group path/name.
11. In the **Agent Group Configuration** panel, click **Next**.
12. In the **Service User Configuration** panel, accept the default LocalSystem account or specify an alternate account, and then click **Next**.

13 In the **Ready to Install the Program** panel, confirm the installation parameters, and then click **Install**.

14 When the installation completes, click **Finish**.

A message displays if the intrusion prevention driver requires a restart.

Silent agent installation

You must log on to an Administrator account to install a Windows agent.

You can perform a silent installation of Windows agent using the agent.exe executable and InstallShield and Windows Installer commands. The following command structure shows the sequencing:

agent.exe <InstallShield commands> "<Windows Installer commands> <installation properties>"

The following examples show a command string:

```
agent.exe /s /v"MANAGEMENT_SERVER=192.168.1.103
SSL_CERT_FILE=c:\Agent-cert.ssl
-l*v+! %temp%\SISAgentSetup.log /qn"
```

You create command strings using the following:

- InstallShield commands
- Microsoft Windows Installer commands
- Installation properties

Note: Copying and pasting command lines into the command window can result in silent installation failure. If you copy and paste command lines into the command window, make sure that there are no line breaks or spaces in between command lines.

Displaying InstallShield commands

For a list of InstallShield commands, you can display Help for the agent installation command. The important commands are /s, which suppresses the initialization dialog, and /v, which specifies that the values that follow are Windows Installer commands.

Note: You must enclose the command string that follows /v in quotations.

To display InstallShield commands

1. Insert the installation CD into your computer.
2. Display a command prompt, and navigate to the agent installation directory.
3. Type and run one of the following commands:

```
agent.exe ?
```

Microsoft Windows Installer commands

See the Microsoft documentation for information about standard Microsoft Windows Installer commands and additional logging levels.

Table 3-5 describes the optional basic commands that are used for installations.

Table 3-5 Optional Installer commands

Command	Default	Description
/qn	none	Install silently
-l*v+! <log filename>	none	Log all events except for the v argument (*), create a verbose log file (v), append to the existing log file (+), flush each line to the log (!), to a file named <log filename> that either exists or is created. If the path includes spaces, use quotation marks.
INSTALLDIR=<path>	C:\Program Files\Symantec\Critical System Protection\Agent	Designate a custom path on the target computer where <path> is the specified target directory. If the path includes spaces, use quotation marks. Escape the internal quotation marks, as in the following example: `agent.exe /s /v"INSTALLDIR= \"E:\Program Files\....Symantec \System Critical Protection\Agent\ " -l*v+! c:\agent-install.log /qn"`

Table 3-5 Optional Installer commands *(continued)*

Command	Default	Description
REBOOT=<val>	Based on operating system	Whether or not to restart a computer after installation, where <val> is a valid argument. If REBOOT=<val> is not specified in the command line, the computer will not reboot. Valid arguments are as follows: ■ Force (prompts for restart) ■ Suppress (prevents most restarts) ■ ReallySuppress (prevents all restarts as part of the installation process)

Installation properties

Table 3-6 describes the Windows agent installation settings and options.

Table 3-6 Windows agent installation settings

Setting	Default	Description
MANAGEMENT_ SERVER=<val>	localhost	The IP address or fully qualified host name of th management server that will manage the agent. Required
ALT_MANAGEMENT _SERVERS=<server1, server2,...>	none	An ordered list of alternate management servers f For each alternate management server, specify address or fully qualified host name. Specify the a comma-separated list. Optional See "About simple failover" on page 28.
PROTOCOL=<val>	https	Select https or http communications.
SSL_CERT_FILE=<val>	none	The directory location of the SSL certificate file Agent-cert.ssl. Example: C:\Agent\Agent-cert.ssl See "About the SSL certificate file" on page 53. Optional

Table 3-6 Windows agent installation settings *(continued)*

Setting	Default	Description
ENABLE_BYPASS_CHECKS	none	Indicates whether to enable the bypass prerequisite c feature. To enable, set the variable to a nonzero valu Optional
NOTIFICATION_ENABLE =<val>	True	Indicates whether to enable notification, where <val valid argument (True, False). Optional
AGENT_NAME=<name>	Host name of agent computer	The agent name. After installation, you can modify the agent name usi management console. Optional
AGENT_PORT=<val>	443	The Agent Port number that was used during manag server installation. See See "Management server installation settings an options" on page 39. See See "About port mapping" on page 34. Optional
LOG_DIR=<val>	C:\Program Files\Symantec\Critical System Protection\Agent	The installation directory prefix for the <prefix dir>/scsplogs subdirectory. Optional
POLLING_INTERVAL=<val>	300 seconds	The interval that the agent uses to poll the managem server for policy and configuration updates. Optional

Table 3-6 Windows agent installation settings *(continued)*

Setting	Default	Description
IPS_ENABLE=<val>	True	The switch for enabling or disabling intrusion p where <val> is a valid argument (True, False). Optional When enabled, the prevention features of Syman System Protection are enabled for the agent. The are loaded on the agent computer, and the agen prevention policies from the management cons If you disable intrusion prevention and want to the future, you must run the sisipsconfig.exe to \Agent\IPS\bin directory with the -i option, and computer. The -i option toggles the intrusion pr service on and off. Symantec strongly recommends that you enabl prevention.
NOTIFICATION_PORT=<val>	2222	The port that is used to receive broadcast alerts management server, where <val> is a valid port This property is only used when NOTIFICATIO is True. Optional
COMMON_CONFIG_ GROUP=<val>	Common Configuration	The name of an existing common configuration this agent to join. An agent is placed in the default common confi group, unless you specify another configuration already exists in the management console. After installation, you can change the group ass using the management console. Optional
IPS_CONFIG_GROUP=<val>	Configuration	The name of an existing prevention configuratio this agent to join. An agent is placed in the default prevention cor group, unless you specify another configuration already exists in the management console. After installation, you can change the group ass using the management console. Optional

Table 3-6 Windows agent installation settings *(continued)*

Setting	Default	Description
IPS_POLICY_GROUP=<val>	Policy	The name of an existing prevention policy group for agent to join. An agent is placed in the default prevention policy g unless you specify another policy group that already in the management console. After installation, you can change the group assignm using the management console. Optional
IDS_CONFIG_GROUP=<val>	Configuration	The name of an existing detection configuration gro this agent to join. An agent is placed in the default detection configura group, unless you specify another configuration grou already exists in the management console. After installation, you can change the group assignm using the management console. Optional
IDS_POLICY_GROUP=<val>	Windows	The name of an existing detection policy group for this to join. You can specify multiple groups using comm between the group names. You can optionally include the name of an existing det policy domain in the group path/name. You can inclu domain name with or without the group name. An agent is placed in the default Windows detection group in the default Policy domain, unless you specif another domain/policy group that already exists in t management console. After installation, you can change the group assignm using the management console. Optional

Table 3-6 Windows agent installation settings *(continued)*

Setting	Default	Description
SERVICE_USER=<val> SERVICE_PW=<val> SERVICE_CONFPW=<val>	LocalSystem none none	SERVICE_USER is the account that registers ser the agent. If you change the default of LocalSyst format <domain>\<user name>. SERVICE_PW is the password for SERVICE_USI SERVICE_CONFPW is the confirmation of the pa SERVICE_USER. **Note:** If you use any of these properties, you mu three properties.

Downloading and importing policy source

The management server installation kit installs compiled Symantec Critical System Protection policies in the management server database.

After you install the management server and management console, you can download and import read-only copies of the policy source. The easiest way to download and import the policy source is to run Symantec Critical System Protection LiveUpdate™.

To download and import policy source

1. On the computer that runs the Symantec Critical System Protection management console, click **Policies**.
2. Click LiveUpdate icon on the toolbar.
3. In the LiveUpdate dialog box, click **Check** to check for source policy packs.
4. In the LiveUpdate dialog box, select the source policy packs that you want to download and import into the management server database, and then click **Install**.
5. In the LiveUpdate dialog box, click **Finish**.

Uninstalling Symantec Critical System Protection

To uninstall Symantec Critical System Protection, you need to uninstall each component separately. You can uninstall the components in any order. If the agent runs on a computer that also runs the management server or management console, disable policy prevention on the agent by setting the Null policy or by using the policy override tool.

Uninstalling an agent using Add or Remove Programs

Agent uninstallation uses the Windows Add or Remove Programs utility.

If the agent enforces policy prevention, it prevents you from removing agent-related files, the management server, and management console. If a service user account was created during installation, the account is not removed during uninstallation.

Use one of the following methods to disable policy prevention on the agent:

- Start the management console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).
- If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention.
  See the *Symantec Critical System Protection Policy Override Guide*.

To uninstall an agent

1. Disable policy prevention on the agent computer.
2. On the computer that runs the agent, click **Start > Settings > Control Panel > Add/Remove Programs**.
3. Click **Symantec Critical System Protection Agent**, and then click **Remove**.
4. Follow and complete the prompts until uninstallation completes.
5. Restart the agent computer.

Silent uninstallation of an agent

You can perform an silent uninstallation of an agent using the agent.exe or agent-windows-nt.exe executable and InstallShield and Windows Installer commands.

The following command structure shows the sequencing:

MsiExec.exe /X{<PRODUCT CODE>} /qn /l*v!+ <UNINSTLL LOG FILE>

The <PRODUCT CODE> is the Symantec Critical System Protection uninstall string necessary for MsiExec.exe. It is in the following directory:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall

For Windows 2008 64-bit system, the <PRODUCT CODE> is in the following directory:

HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Uninstall

Browse the list of IDs. Locate the Symantec Critical System Protection agent application by looking at the properties in the right pane. Note the UinstallString string, and copy and modify it. For example:

MsiExec.exe /X{3D24482F-98BD-48DD-AA62-8B24BFDE7329} /qn /l*v!+ C:\SISAgentUninstall.log

The system restart is suppressed after the uninstallation.

See "Silent agent installation" on page 63.

Uninstalling the management console

Management console uninstallation uses the Windows Add or Remove Programs utility.

If the computer that runs the management console also runs the agent, use one of the following methods to disable policy prevention on the agent:

- Start the management console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).
- If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention.
  See the *Symantec Critical System Protection Policy Override Guide*.

To uninstall the management console and database

1. Disable policy prevention on the agent computer.
2. Click **Start > Settings > Control Panel > Add/Remove Programs**.
3. Click **Symantec Critical System Protection Management Console**, and then click **Remove**.
4. Follow and complete the prompts until uninstallation completes.

Uninstalling the management server and database

Management server uninstallation uses the Windows Add or Remove Programs utility.

If the computer that runs the management server also runs the agent, disable policy prevention on the agent. The management server may also use SQL Server database to store data.

Use one of the following methods to disable policy prevention on the agent:

- Start the management console, and set the policy for the target agent to the Null prevention policy (sym_win_null_sbp).

- If the policy on the computer that runs the agent is not Null and permits policy override, use the policy override tool to disable policy prevention.
  See the *Symantec Critical System Protection Policy Override Guide*.

To uninstall the management server and database

1. Disable policy prevention on the agent computer.
2. Click **Start > Settings > Control Panel > Add/Remove Programs**.
3. Click *Symantec Critical System Protection Management Server*, and then click **Remove**.
4. Follow and complete the prompts until uninstallation completes.
5. (Optional) Do one of the following:

   If you installed the evaluation database, click **Microsoft SQL Server 2005 Express**, and then click **Remove**.

   If you installed the evaluation or production database on SQL Server, drop the database that you created during installation, which is scspdb by default.
6. Follow and complete the prompts until uninstallation completes.
7. Delete the C:\Program Files\Symantec\Critical System Protection\Server directory.
8. Delete the file in C:\Program Files\Common Files\Symantec Shared\SCSP directory.
9. Restart the computer.

Temporarily disabling Windows agents

You can temporarily disable Symantec Critical System Protection Windows agents.

Temporarily disabling Windows 2000, Windows Server 2003, or Windows XP Professional agents

To temporarily disable agents that run on Windows 2000, Windows Server 2003, or Windows XP Professional, you must boot the agent computer in safe mode and then reset the prevention policy to the built-in Null policy.

Warning: You should perform these procedures only in emergency situations.

To temporarily disable Windows 2000, Windows 2003, or Windows XP agents

1 Boot the agent computer in safe mode.

Refer to your Microsoft Windows documentation for instructions on booting in safe mode.

2 Reset the prevention policy to the built-in Null policy.

Resetting the prevention policy to the built-in Null policy

Run the sisipsconfig.exe tool with the -r option to reset the prevention policy to the built-in Null policy. On Windows, sisipsconfig.exe is located the following directory:

Note: To run the agent config tool (sisipsconfig.exe), you must have administrative privilege.

C:\Program Files\Symantec\Critical System Protection\Agent\IPS\bin

To reset the prevention policy

1 On the agent computer, open a command prompt.

2 At a command prompt, type the following command, and then press Enter:

```
sisipsconfig -r
-----------------------------------------------
Agent Configuration Tool version 5.0.0.240
-----------------------------------------------
The agent will now use the built-in policy
c:\>
```

3 Reboot the agent computer, and then start the management console.

In the management console, on the Assets page, the agent is marked with an exclamation point (!) to indicate a policy error. When you select the agent, the following message appears in the Details pane, on the Policies tab:

! Policy Errors:

** Policy error has occurred at 17-Nov-2005 05:55:56 EST

Driver is using the built-in policy and not the assigned policy.

4 In the management console, apply the desired policy to the agent, and then give appropriate permissions to the desired programs.

Reinstalling Windows agents

You can perform an unattended reinstall of Windows agents using the agent.exe or agent-windows-nt.exe executable and InstallShield and Windows Installer commands. Reinstalling a Windows agent is useful if an agent becomes corrupted. Reinstalling a Windows agent is equivalent to uninstalling an agent and then installing the same version of that agent.

The following examples show a command string:

```
agent.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"
```

or

```
agent-windows-nt.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"
```

See “Silent agent installation” on page 63.

See “Unattended Windows agent migration” on page 102.

Chapter 4

Installing UNIX agents

This chapter includes the following topics:

About installing UNIX agents

Installation prompts you to enter a series of values.

Please note the following UNIX agent installation requirements:

- UNIX agents do not support IP aliases. If your network card is bound to more than one IP address, the agent uses the first IP address on the network card.
- You must install UNIX agents as root. UNIX agents require root privileges to run.
- Directory path names cannot contain spaces.
- If you transfer UNIX agent installation .bin files from a Windows computer to a UNIX computer using FTP or some other file transport method, you must use binary transfer mode. Otherwise the installation files will be corrupted.
- If you are installing a Solaris, Linux, HP-UX, AIX, or Tru64 agent on a system that supports non-English character sets, the destination directory that you

choose for the agent must contain only ASCII characters. If you include any non-ASCII characters in the path, the installation will fail.

Table 4-1 describes the agent installation settings.

Table 4-1 UNIX agent installation settings

Setting	Default	Description
Installation Directory	/opt/Symantec	The Installation directory prefix for the <prefix dir>/scspagent subdirectory. The directory path name cannot contain spaces.
Logs File Directory	/var/log	The installation directory prefix for the <prefix dir>/scsplogs subdirectory.
Enable Real-time File Integrity Monitoring	/opt/Symantec/scspagent/Data	Enables real-time event logging on the agent.
Protocol	https	Select https or http communications.
Primary Management Server	127.0.0.1	The IP address or fully qualified host name of the primary management server that will manage the agent.
Alternate Management Servers	none	A comma-separated list of alternate management servers. For each alternate management server, specify the IP address or fully qualified host name. Optional See "About simple failover" on page 28.
Management Server Certificate	/tmp/agent-cert.ssl	The directory location of the SSL certificate file, agent-cert.ssl, obtained from the Symantec Critical System Protection management server installation directory. You must copy this file from the management server to the specified location before starting the installation. The directory path name cannot contain spaces. All primary and alternate management servers must use the same certificate file. Required
Agent Name	Host name of agent computer	The name of the agent computer. After installation, you can change the agent name through the management console.

Table 4-1 UNIX agent installation settings *(continued)*

Setting	Default	Description
Agent Locale	POSIX®	Symantec Critical System Protection agent locale setting.
Agent Port	443	The Agent Port number that was used during management server installation. See See "Management server installation settings and options" on page 39.
Agent Polling Interval	300 seconds	The interval that the agent uses to poll the management server for policy and configuration updates.
Notification Port	2222	The port that is used to receive alerts from the management server. You can also change this port after installation by using the management console to change the properties of the agent.
Agent Notifications	Enable	When enabled, the agent listens on the Notification port to alerts from the management server. The alerts instruct the agent to immediately update to a new policy or configuration. This feature requires an unblocked notification port.
Util Service Port	2323	This installation setting supports the policy override tool for Solaris and Linux. You use the policy override tool to override prevention policy enforcement. You can change this value during installation.
Enable IPS Feature	Enable	When enabled, prevention is enabled on the agent.
Common Config Group	none	The name of an existing common configuration group for this agent to join. You use common configuration groups to apply communication and event logging parameters to agents. An agent is placed in the default common configuration group, unless you specify another configuration group that already exists in the management console. After installation, you can change the group assignment using the management console.

Table 4-1 UNIX agent installation settings *(continued)*

Setting	Default	Description
Prevention Config Group	none	The name of an existing prevention configuration group for this agent to join. You use prevention configuration groups to apply log rules to agents. An agent is placed in the default prevention configuration group, unless you specify another configuration group that already exists in the management console.After installation, you can change the group assignment using the management console.
Prevention Policy Group	none	The name of an existing prevention policy group for this agent to join. You use prevention policy groups to apply prevention policies to agents. An agent is placed in the default prevention policy group, unless you specify another policy group that already exists in the management console.After installation, you can change the group assignment using the management console.
Detection Configuration Group	none	The name of an existing detection configuration group for this agent to join. You use detection configuration groups to apply detection parameters and log rules to agents. An agent is placed in the default detection configuration group, unless you specify another configuration group that already exists in the management console. After installation, you can change the group assignment using the management console.

Table 4-1 UNIX agent installation settings *(continued)*

Setting	Default	Description
Detection Policy Group	One of the following: ■ AIX ■ HP-UX ■ Linux ■ Solaris ■ Windows ■ Tru64	The name of an existing detection policy group for this agent to join. You can specify multiple groups by using commas between the group names. You can optionally include the name of an existing detection policy domain in the group path/name. You can include the domain name with or without the group name. An agent is placed in one of the default OS-specific detection policy groups in the default Policy domain, unless you specify another domain/policy group that already exists in the management console. After installation, you can change the group assignment using the management console.

Bypassing prerequisite checks

The UNIX installation kit lets you bypass some of the prerequisite checks for agent installation. You can use this feature if you know the installation kit is incorrectly failing a prerequisite.

To enable the bypass prerequisite checks feature, run touch as superuser:

```
touch /etc/scsp-check-bypass
```

You can use the bypass prerequisite checks feature to bypass the following prerequisite checks:

- Verify that the installation kit is being run by the root user
- Perform OS platform and version checks
- Perform package dependencies checks
- Perform file system/disk space usage checks

When the bypass prerequisite checks feature is used, the installation kit displays all errors and warnings about prerequisite check failures. However, instead of terminating the installation, you may choose to continue.

When you run the installation kit in interactive mode, you are asked if you want to continue. When you run the installation kit in silent mode, the prerequisite failure is logged and the installation continues.

The installation kit removes the /etc/scsp-check-bypass file upon a successful installation. Thus, creating the file enables the feature for one installation only.

Warning: Use of the bypass prerequisite checks feature does not guarantee that the installation will be successful if a non-recoverable error is bypassed. Please use this feature with caution.

Installing an agent in verbose mode

Ports that are used for communications between an agent and the management server must be available on the agent computer and must match the values used during management server installation. The default settings are 443 and 2222.

After agent installation, you should assign a prevention policy and one or more detection policies to the agent using the management console.

See the *Symantec Critical System Protection Administration Guide* for information on assigning policies.

Before you install an agent, you need to place the SSL certificate on the computer that is targeted for installation. The certificate file is on the management server in the \Symantec\Critical System Protection\Server directory. The file is named agent-cert.ssl.

To place the certificate on the computer that is targeted for installation, do the following:

- On the management server that will be used to manage the agent, locate the file named agent-cert.ssl in the \Server directory.
- On the computer on which the agent will be installed, create a directory and then copy the file agent-cert.ssl into the directory using FTP in binary mode or some other protocol.

The directory path name cannot contain spaces.

To install an agent in verbose mode

1. Open a Terminal window and become superuser.
2. Insert the installation CD and if necessary, mount the volume.
3. Type and run the following command:

```
cd /mnt/cdrom
```

4 Type and run one of the following commands:

Sun Solaris 8.0/9.0	**./agent-solaris-sparc.bin**
Sun Solaris 10 SPARC	**./agent-solaris10-sparc.bin**
Sun Solaris 10 x86	**./agent-solaris10-x86.bin**
Sun Solaris 11 SPARC	**agent-solaris11-sparc.bin**
Sun Solaris 11 x86	**agent-solaris11-x86.bin**
Red Hat Enterprise Linux ES 3.0	**./agent-linux-rhel3.bin**
Red Hat Enterprise Linux ES 4.0 (32-bit)	**./agent-linux-rhel4.bin**
Red Hat Enterprise Linux ES 4.0 (64-bit)	**./agent64-linux-rhel4.bin**
Red Hat Enterprise Linux ES 4.0 (IA64)	**./agent-linux-rhel4-ia64.bin**
Red Hat Enterprise Linux 5.1/5.2 (32-bit)	**./agent-linux-rhel5.bin**
Red Hat Enterprise Linux 5.1/5.2 (64-bit)	**./agent64-linux-rhel5.bin**
SUSE Enterprise Linux 8	**./agent-linux-sles8.bin**
SUSE Enterprise Linux 9	**./agent-linux-sles9.bin**
SUSE Enterprise Linux 10 (32-bit)	**./agent-linux-sles10.bin**
SUSE Enterprise Linux 10 (64-bit)	**./agent64-linux-sles10.bin**
HP-UX on PA-RISC	**./agent-hpux-hppa.bin**
HP-UX on Itanium	**./agent-hpux-ia64.bin**
AIX	**./agent-aix.bin**

Tru64 UNIX	`./agent-tru64.bin`

5 Please indicate whether you agree to the license agreement.

6 Follow the prompts until the installation completes.

7 On Solaris, AIX, or Linux, restart the computer if prevention was enabled.

Installing an agent in silent mode

You can use the silent installation for UNIX installations.

Note: The required options for silent installation are -silent, -server, and -cert.

Table 4-2 describes the settings that are used with the installation commands.

Table 4-2 UNIX agent installation settings

Setting	Default	Description
-help	none	You can run the installer with the –help switch to get a list of all the switches.
-rtfim		Install Real-time File Integrity Monitoring.
-version	none	Displays the installation package version information. Installation does not occur.
-silent	Interactive	Installs silently without user prompts. Uses default settings if they are not set by installation options. Required
-allowreboot	No reboot	Initiates an automatic restart after installation completes, if intrusion prevention is enabled after installation. Applies to IPS agents.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
–altroot	none	Used with Solaris Jumpstart. In a Jumpstart environment, the system where the install takes place is booted from a temporary OS instance. The alternate root is necessary to ensure that files get installed in the correct place, relative to real OS instance, and not the temporarily booted instance.
-server=<addr>	127.0.0.1	The management server IP address or fully qualified host name. Required
-altservers=<server1,server2,...>	none	A comma-separated list of alternate management servers. For each alternate management server, specify the IP address or fully qualified host name. Optional See “About simple failover” on page 28.
-prefix=<dir>	/opt/Symantec	The installation directory prefix for the <prefix dir>/scspagent subdirectory. The directory path name cannot contain spaces.
-logdir=<dir>	/var/log/scsplog	The installation directory prefix for the <prefix dir>/scsplog subdirectory. If the directory does not exist, it is created.
-protocol=<protocol>	https	Select https or http communications.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
-cert=<file>	/tmp/agent-cert.ssl	The directory location of the SSL certificate file, agent-cert.ssl, obtained from the Symantec Critical System Protection management server installation directory. You must copy this file from the management server to the specified location before starting the installation. The directory path name cannot contain spaces. All primary and alternate management servers must use the same certificate file. Required
-agentname=<name>	Host name of agent computer	The name of the agent computer. After installation, you can change the agent name through the management console.
-locale=<locale setting>	POSIX	Symantec Critical System Protection agent locale setting.
-comCfgGrp=<group>	none	The name of an existing common configuration group for this agent to join. The group must exist and appear in the management console.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
-ipsCfgGrp=<group>	none	The name of an existing prevention configuration group for this agent to join. The group must exist and appear in the management console.Applies to IPS agents.
-ipsPolGrp=<group>	none	The name of an existing prevention policy group for this agent to join. The group must exist and appear in the management console. Applies to IPS agents.
-idsCfgGrp=<group>	none	The name of an existing detection configuration group for this agent to join. The group must exist and appear in the management console.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
-idsPolGrp=<group>	OS-specific group The OS-specific group is one of the following: ■ AIX ■ HP-UX ■ Linux ■ Solaris ■ Tru64 ■ Windows	The name of an existing detection policy group for this agent to join. You can specify multiple groups by using commas between the group names. You can optionally include the name of an existing detection policy domain in the group path/name . You can include the domain name with or without the group name. An agent is placed in one of the default OS-specific detection policy groups in the default Policy domain, unless you specify another domain/policy group that already exists in the management console. After installation, you can change the group assignment using the management console.
-agentport=<port>	443	The Agent Port number that was used during management server installation. See See "Management server installation settings and options" on page 39.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
-notifyport=<port>	2222	The notification port that is used to receive broadcast alerts from the management server. You can also change this port after installation by using the management console to change the properties of the agent.
-notify=<0|1>	1 (Enable)	Indicates whether to enable notification. When enabled, the agent listens on the notification port to broadcast alerts from the management server. The broadcast alerts instruct the agent to immediately update to a new policy. This feature requires an unblocked notification port.
-poll=<sec>	300	The polling interval, in seconds, that the agent uses to poll the management server for policy updates.
-svcport=<port>	2323	This installation setting supports the policy override tool for Solaris and Linux agents. The policy override tool overrides prevention policy enforcement. Use this switch to change the port value during silent install.

Table 4-2 UNIX agent installation settings *(continued)*

Setting	Default	Description
-disableIps	Enable	Indicates whether to enable intrusion prevention for Solaris or Linux agents. When enabled, the prevention features of Symantec Critical System Protection are enabled for the agent. The IPS drivers are loaded on the agent computer, and the agent accepts prevention policies from the management console. To disable intrusion prevention, include the -disableIps installation option in the command string. If you disable intrusion prevention and want to enable it in the future, you must run the sisipsconfig.sh tool in the /scspagent/IPS directory with the -i option, and restart the computer. The -i option toggles the intrusion prevention service on and off. Symantec strongly recommends that you enable intrusion prevention.

Use the -silent option and other options to perform a silent installation.

The following command string shows an example of a silent installation:

```
./agent-aix.bin -silent -prefix=/opt/Symantec -server=192.168.1.1
 -cert=/var/tmp/agent-cert.ssl -agentport=443
```

To install an agent in silent mode

1. Follow the procedures and steps that are used to install an agent in verbose mode, up to and including mounting the installation CD drive.

   See "Installing an agent in verbose mode" on page 80.

2. Type and run the following command after replacing <os> with agent-solaris-sparc.bin, agent-solaris10-sparc.bin, agent-solaris10-x86.bin, agent-solaris11-sparc.bin, agent-solaris11-x86.bin, agent-linux-rhel3.bin, agent-linux-rhel4.bin, agent64-linux-rhel4.bin, agent-linux-rhel4-ia64.bin, agent-linux-rhel5.bin, agent64-linux-rhel5.bin, agent-linux-sles8.bin, agent-linux-sles9.bin, agent-linux-sles10.bin, agent64-linux-sles10.bin, agent-hpux-hppa.bin, agent-hpux-ia64.bin, agent-aix.bin, and agent-tru64.bin :

   ```
   ./agent-<os>.bin -silent <additional options>
   ```

3. If you did not specify the -allowreboot option, restart the computer if intrusion prevention is enabled on Solaris, AIX, or Linux.

   If the agent fails to install correctly, review the /var/log/scsplog/agent_install.log file.

Uninstalling agents using package commands

You can uninstall the agents by using native operating system package commands. The package name for the agent is SYMCcsp.

When the uninstaller completes, it reports an uninstall status.

To uninstall agents using package commands

1. (Solaris/Linux) Start the management console, and set the policy for the agent to uninstall to the Null policy.

   The agent prevents you from installing and removing agent-related files if it is enforcing a restrictive prevention policy.

   If the Solaris or Linux agent is not communicating with the management console, disable the agent, and then continue with the uninstall.

   See "Disabling and enabling Solaris agents" on page 91.

   See "Disabling and enabling Linux agents" on page 93.

2. Open a Terminal window on the computer that runs the agent to uninstall, and become superuser.

3 On Solaris, type and run the following command:

```
pkgrm SYMCcsp
```

On Solaris, run the following command to restart the computer:

```
init 6
```

4 On Linux, type and run the following command:

```
rpm -e SYMCcsp
```

On Linux, run the following command to restart the computer:

```
init 6
```

5 On AIX, type and run the following command:

```
rpm -e SYMCcsp
```

On AIX, if the installation completes successfully, run the following command to restart the computer:

```
shutdown -Fr now
```

6 On HP-UX, type and run the following command:

```
swremove SYMCcsp
```

7 On Tru64, type and run the following command:

```
setld -d SYMCSP520
```

8 (Solaris, and Linux) If the uninstall completes successfully, run the following command to restart the computer:

```
init 6
```

9 On AIX, iIf the uninstall completes successfully, run the following command to restart the computer:

```
shutdown -Fr
```

Computers running HP-UX does not require restart. If you have enabled IPS or File Integrity Monitoring (FIM), you must restart the system.

Disabling and enabling UNIX agents

You can temporarily and permanently disable UNIX agents. If you permanently disable an agent, the agent daemons stop immediately and disable startup upon restart. It does not disable the agent daemons. Upon restart, the agent daemons continue to load and enforce the currently-applied policies.

Disabling and enabling Solaris agents

This section describes how to disable and enable Solaris agents.

Temporarily disabling the IPS driver

If you have performance issues with Solaris agents, you may need to temporarily disable the intrusion prevention driver. You should do this only if there are serious performance issues that you suspect are being caused by the IPS driver, or if you have applied a prevention policy that is not allowing you to access the system in any way.

After you disable the driver, apply the Null prevention policy or a prevention policy in which prevention was disabled. Reboot the system.

Warning: You should perform these procedures only in emergency situations.

To temporarily disable the IPS driver

1. Interrupt the boot cycle with a Stop-a or break sequence.
2. At the ok prompt, type and run the following command:

   ```
   boot -as
   ```

   You must include the s switch in the boot command to boot into single-user mode. If you omit the s switch, then once the system boots into multi-user mode, it will enable the Symantec Critical System Protection driver.
3. When the boot sequence asks for the location of your /etc/system file, type one of the following:

   ```
   /etc/system-pre-sisips
   ```

   ```
   /dev/null
   ```

Permanently disabling Solaris agents

If you have performance issues with Solaris agents, you may need to permanently disable them.

The following procedure disables an agent, not the driver. The driver will still be running.

Warning: You should perform these procedures only in emergency situations.

To permanently disable Solaris agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/etc/init.d/sisipsagent stop

/etc/init.d/sisidsagent stop
```

3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:

```
mv /etc/init.d/sisipsagent /etc/init.d/sisipsagentOFF

mv /etc/init.d/sisidsagent /etc/init.d/sisidsagentOFF
```

Enabling a disabled Solaris agent

You can enable a Solaris agent that was previously disabled.

To enable a disabled Solaris agent

1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:

```
mv /etc/init.d/sisipsagentOFF /etc/init.d/sisipsagent

mv /etc/init.d/sisidsagentOFF /etc/init.d/sisidsagent
```

3. Type and run the following command to restart the computer:

```
init 6
```

Disabling and enabling Linux agents

This section describes how to disable and enable Linux agents.

Temporarily disabling the IPS driver

If you have performance issues with Linux agents, you may need to temporarily disable the intrusion prevention driver. You should do this only if there are serious performance issues that you suspect are being caused by the IPS driver, or if you have applied a prevention policy that is not allowing you to access the system in any way.

After you disable the driver, apply the Null prevention policy or a prevention policy in which prevention was disabled. Reboot the system.

Warning: You should perform these procedures only in emergency situations.

To temporarily disable the IPS driver

- During the boot cycle, add the string SISIPSNULL to the boot options. The agent and kernel mode driver do not load, and the policy is not enforced.

Permanently disabling Linux agents

If you have performance issues with Linux agents, you may need to permanently disable them.

The following procedure disables an agent, not the driver. The driver will still be running.

Warning: You should perform these procedures only in emergency situations.

To permanently disable Linux agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/etc/init.d/sisipsagent stop

/etc/init.d/sisidsagent stop
```

3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:

```
mv /etc/init.d/sisipsagent /etc/init.d/sisipsagentOFF

mv /etc/init.d/sisidsagent /etc/init.d/sisidsagentOFF
```

Enabling a disabled Linux agent

You can enable a Linux agent that was previously disabled.

To enable a disabled Linux agent

1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:

```
mv /etc/init.d/sisipsagentOFF /etc/init.d/sisipsagent

mv /etc/init.d/sisidsagentOFF /etc/init.d/sisidsagent
```

3. Type and run the following command to restart the computer:

```
init 6
```

Disabling and enabling HP-UX agents

This section describes how to disable and enable HP-UX agents.

Temporarily disabling HP-UX agents

Warning: You should perform these procedures only in emergency situations.

To temporarily disable HP-UX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/sbin/init.d/sisipsagent stop

/sbin/init.d/sisidsagent stop
```

Permanently disabling HP-UX agents

If you have performance issues with HP-UX agents, you may need to permanently disable them.

Warning: You should perform these procedures only in emergency situations.

To permanently disable HP-UX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/sbin/init.d/sisipsagent stop

/sbin/init.d/sisidsagent stop
```

3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:

```
mv /sbin/init.d/sisipsagent /sbin/init.d/sisipsagentOFF

mv /sbin/init.d/sisidsagent /sbin/init.d/sisidsagentOFF
```

Enabling a disabled HP-UX agent

You can enable a HP-UX agent that was previously disabled.

To enable a permanently disabled HP-UX agent

1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:

```
mv /sbin/init.d/sisipsagentOFF /sbin/init.d/sisipsagent

mv /sbin/init.d/sisidsagentOFF /sbin/init.d/sisidsagent
```

3. Type and run the following commands to start the agents:

```
/sbin/init.d/sisipsagent start

/sbin/init.d/sisidsagent start
```

Disabling and enabling AIX agents

This section describes how to disable and enable AIX agents.

Temporarily disabling AIX agents

Warning: You should perform these procedures only in emergency situations.

To temporarily disable AIX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/etc/rc.sisipsagent stop

/etc/rc.sisidsagent stop
```

Permanently disabling AIX agents

If you have performance issues with AIX agents, you may need to permanently disable them.

Warning: You should perform these procedures only in emergency situations.

To permanently disable AIX agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/etc/rc.sisipsagent stop

/etc/rc.sisidsagent stop
```

3. Comment the agent startup commands from the /etc/inittab file by adding a colon (:) at the front of the rcsisipsagent and rcsisidsagent lines.

   This causes the agents to not start at the next reboot.

Enabling a disabled AIX agent

You can enable an AIX agent that was previously disabled.

To enable a permanently disabled AIX agent

1. Open a Terminal window and become superuser.
2. Uncomment the agent startup commands from the /etc/inittab file by removing the colon (:) at the front of the rcsisipsagent and rcsisidsagent lines.

   This causes the agents to start at the next reboot. The lines should look like the following:

```
rcsisipsagent:23456789:wait:/etc/rc.sisipsagent start >/dev/console 2>&1

rcsisidsagent:23456789:wait:/etc/rc.sisidsagent start >/dev/console 2>&1
```

3. Type and run the following commands to restart the agents:

```
/sbin/init.d//sisipsagent start

/sbin/init.d//sisidsagent start
```

Disabling and enabling Tru64 agents

This section describes how to disable and enable Tru64 agents.

Temporarily disabling Tru64 agents

Warning: You should perform these procedures only in emergency situations.

To temporarily disable Tru64 agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/sbin/init.d/sisipsagent stop

/sbin/init.d/sisidsagent stop
```

Permanently disabling Tru64 agents

If you have performance issues with Tru64 agents, you may need to permanently disable them.

Warning: You should perform these procedures only in emergency situations.

To permanently disable Tru64 agents

1. Open a Terminal window and become superuser.
2. Type and run the following commands:

```
/sbin/init.d/sisipsagent stop

/sbin/init.d/sisidsagent stop
```

3. Type and run the following commands to rename the agent scripts, which temporarily break any symbolic links in the rc#.d startup scripts:

   If the machine is a member of a TruCluster, and the agent is installed on multiple cluster members (with a shared physical disk), perform the following actions to disable the agent on a single cluster:

```
cd /cluster/members/\{memb\}/sbin/init.d/

mv sisipsagent sisipsagentOFF

mv sisidsagent sisidsagentOFF
```

   If the machine not is a member of a TruCluster, is configured as a single member cluster, or if you want to disable the agent on all clusters, perform the following actions:

```
mv /sbin/init.d/sisipsagent /sbin/init.d/sisipsagentOFF

mv /sbin/init.d/sisidsagent /sbin/init.d/sisidsagentOFF
```

Enabling a disabled Tru64 agent

You can enable a Tru64 agent that was previously disabled.

To enable a permanently disabled Tru64 agent

1. Open a Terminal window and become superuser.
2. Type and run the following commands, which rename the sisipsgent scripts:

   If the machine is a member of a TruCluster, and the agent is installed on multiple cluster members (with a shared physical disk), perform the following actions to re-enable the agent on a single cluster:

   ```
   cd /cluster/members/\{memb\}/sbin/init.d/

   mv sisipsagentOFF sisipsagent

   mv sisidsagentOFF sisidsagent
   ```

   If the machine is a member of a TruCluster, is configured as a single member cluster, or if you want to re-enable the agent on all clusters, perform the following actions:

   ```
   mv /sbin/init.d/sisipsagentOFF /sbin/init.d/sisipsagent

   mv /sbin/init.d/sisidsagentOFF /sbin/init.d/sisidsagent
   ```

3. Type and run the following commands to start the agents:

   ```
   /sbin/init.d/sisipsagent start

   /sbin/init.d/sisidsagent start
   ```

Monitoring and restarting UNIX agents

The Health Check feature monitors and restarts UNIX agents in the event of an unexpected termination. This feature is available through the use of a crontab entry, which calls the daemon startup scripts at regular intervals with a health_check parameter.

For example, to monitor the UNIX agents every hour, add the following lines to the crontab file:

```
0 * * * * /etc/init.d/sisipsagent health_check

0 * * * * /etc/init.d/sisidsagent health_check
```

```
0 * * * * /etc/init.d/sisipsutil health_check (Solaris and Linux Only)
```

Use the appropriate crontab file for the UNIX platform:

- AIX
  Crontab: /var/spool/cron/cronttabs/root
  Scripts: /etc/rc.sisidsagent, /etc/rc.sisipsagent
- HP-UX
  Crontab: /var/spool/cron/crontab.root
  Scripts: /sbin/init.d/sisidsagent, /sbin/init.d/sisipsagent
- Linux
  Crontab: /var/spool/cron/tabs/root
  Scripts: /etc/init.d/sisidsagent, /etc/init.d/sisipsagent, /etc/init.d/sisipsutil
- Solaris
  Crontab: /var/spool/cron/crontabs/root
  Scripts: /etc/init.d/sisidsagent, /etc/init.d/sisipsagent, /etc/init.d/sisipsutil
- Tru64
  Crontab: /var/spool/cron/crontabs/root
  Scripts: /sbin/init.d/sisidsagent, /sbin/init.d/sisipsagent

---

Note: The scripts keep the last five core files generated in the agent's respective home directory (/opt/Symantec/scspagent/IDS/bin and /opt/Symantec/scspagent/IPS). To change this setting, modify the MAX_CORES=5 value in the scripts.

Troubleshooting agent issues

ISSUE: An NFS server that does not respond on an agent computer causes the agent installation to hang.

SOLUTION: Press Ctrl+C to exit the installation, and then run df -k. If this causes the agent computer to hang, and you are sure that a mounted share is causing the problem, forcefully unmount the share that is not responding by typing and running the following command:

```
umount -f <mount-point>
```

Chapter 5

Migrating to the latest version

This chapter includes the following topics:

Migrating legacy installations of Symantec Critical System Protection

You can migrate legacy installations for the following Symantec Critical System Protection software:

- Symantec Critical System Protection 5.0.0 (server, console, agent)
- Symantec Critical System Protection 5.0.1 (server, console, agent)
- Symantec Critical System Protection 5.0.5 (server, console, agent)
- Symantec Critical System Protection 5.1.0 (server, console, agent)

When migrating legacy installations for Symantec Critical System Protection, you should note the following:

- If you upgrade the management server, then you must also upgrade the management console to the same version, and vice versa. The management server and management console must be the same version.
- Upgrading the agent is optional; you can use agent 5.0.0, agent 5.0.1, agent 5.0.5, or agent 5.1 with the latest version of the management server and management console. However, if you upgrade the agent to the latest version, then you must also upgrade the management server and management console.
- To use simple failover, you must upgrade the management server, management console, and agent to version 5.1.1 or higher.

After upgrading, you use the CSP_Agent_Diagnostics detection policy or the agent config tool to specify the alternate management servers for the agent. See "Specifying the management server list for an agent" on page 103.

- You cannot upgrade Symantec Critical System Protection 4.5. You must uninstall the Symantec Critical System Protection 4.5 software (server, console, and agent) and then install the latest version.

See "Unattended Windows agent migration" on page 102.

Software migration is straightforward. When you install the Symantec Critical System Protection software (server, console, and agent), the installation kit automatically detects legacy installations and migrates the Symantec Critical System Protection software to the latest version.

Providing scspdba password during management server upgrade

During a management server upgrade, you are asked for the password to the scspdba account. If you chose the Evaluation installation when you initially installed the management server, the scspdba password is the same as the sa account password that you specified during the installation. Enter that same password during the upgrade. If you chose the Production installation, you entered the password for this account (the Database Owner account) during the initial installation of the management server. Enter that same password during the upgrade.

If you do not remember the scspdba password, you should change it in the database using SQL Server tools. This account is used strictly for upgrading the software; it is not used operationally by the management server. So changing the password in the database is safe—there is no corresponding change needed for the management server.

If you changed the name of the database owner account during a Production installation, you should enter that account name during the upgrade as well. You should not use the sa account during the upgrade.

Unattended Windows agent migration

You can perform an unattended migration of Windows agents using the agent.exe or agent-windows-nt.exe executable and InstallShield and Windows Installer commands.

The following examples show a command string:

```
agent.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"
```

or

```
agent-windows-nt.exe /s /v"/qn /l*v!+ %temp%\SISAgentSetup.log"
```

See "Silent agent installation" on page 63.

Specifying the management server list for an agent

This section explains how to specify the primary management server and optional alternate management servers for an agent.

See "About simple failover" on page 28.

You can use the following:

- CSP_Agent_Diagnostics detection policy
- Agent config tool

Using the CSP_Agent_Diagnostics detection policy

A version of the CSP_Agent_Diagnostics detection policy is available for Windows and UNIX agents.

See the *Symantec Critical System Protection Detection Policy Reference Guide* for information about the CSP_Agent_Diagnostics policy.

To use the CSP_Agent_Diagnostics detection policy

1. Log on to the management console as an administrator.
2. In the management console, on the Policies page, in the Symantec folder, edit the CSP_Agent_Diagnostics policy.
3. Enable **Modify the management server list used by the agent**, and then click **Specify a comma-separated list of servers**.
4. In the Value box, type the primary management server, followed by any optional alternate management servers.

   You must specify the primary management server as the first server, followed by any optional alternate servers. Specify the IP address or fully qualified host name of each server in the list. All the servers in the list must use the same server certificate and agent port.
5. Click **OK** to save the policy changes.
6. Apply the policy to the agent.

   The policy modifies the management server list immediately after being applied to the agent.

7 In the management console, monitor the events on the Monitors page to determine if the management server list was modified.

8 Clear the policy from the agent.

Using the agent config tool

You use the agent config tool to do the following:

- After upgrading to Symantec Critical System Protection agent 5.1.1 or higher, add alternate management servers to an agent's configuration
- Change the primary or alternate management servers used by an agent
- Change the fail back interval used by an agent
- Display the current management server list and fail back interval used by an agent
- Test the connection information for a management server

The agent config tool is located in the following directories on an agent computer:

- On Windows, sisipsconfig.exe is located in the agent/ips/bin directory.
- On UNIX-based operating systems, the sisipsconfig tool is named sisipsconfig.sh. It is located in the agent/ips directory.

Table 5-1 lists the management server-related agent config tool commands:

Table 5-1 Agent config tool commands

Command	Syntax	Description
-host	Windows: sisipsconfig -host primary[,alternate1,alternate2,...] UNIX: sisipsconfig.sh –host primary[,alternate1,alternate2,...]	Set the IP address or fully qualified host name of the primary management server and optional alternate management servers used by the agent. The list of management servers must comprise the primary management server, which is always the first server in the list. The remaining optional servers in the list are considered alternate servers. You may specify any number of optional alternate management servers. The management server list that you specify will replace the current management server list used by the agent. You cannot reorder or edit an existing management server list. The management server host names or IP addresses configured for a single agent must be Tomcat servers that talk to a single Symantec Critical System Protection database. Using multiple databases can result in unexpected agent behavior. The management servers must use the same server certificate and agent port.

Table 5-1 Agent config tool commands *(continued)*

Command	Syntax	Description
-failbackinterval	Windows: sisipsconfig -failbackinterval num_mins UNIX: sisipsconfig.sh -failbackinterval num_mins num_mins = number of minutes Default: 60 minutes	Set the fail back interval, in minutes, for the agent to try to communicate with the primary management server. Once an agent fails away from the first (primary) server in the management server list, the agent periodically checks if the first server is back. The agent uses a fail back interval to determine when to perform this server check.
-view	Windows: sisipsconfig -view UNIX: sisipsconfig.sh -view	Display all values that are configurable through the agent config tool. The configurable values include the management server list and fail back interval.
-test	To test first server in list (default): ■ Windows: sisipsconfig -t ■ UNIX: sisipsconfig.sh -t To test nth server in list: ■ Windows: sisipsconfig -t n ■ UNIX: sisipsconfig.sh -t n	Test the connection information for a server in the management server list.

To specify the management server list for an agent

1. At a command prompt, locate the folder that contains the agent config tool, and then navigate to that directory.
2. At a command prompt, type `sisipsconfig -host` (Windows) or `sisipsconfig.sh -host` (UNIX), followed by a comma-separated list of server host names or IP addresses, and then press Enter.

Index

M

N

P

R

S

T

U

V

W