Symantec Critical System Protection 5.2.9 Administration Guide

Symantec Critical System Protection Administration Guide

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Documentation version: 5.2.9

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

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 the management console commands
- Diagnosing problems with Symantec Critical System Protection

About Symantec Critical System Protection

Symantec™ Critical System Protection provides policy-based behavior control and detection for server and desktop computers. Symantec Critical System Protection provides a flexible computer security solution that controls application behavior, blocks port traffic, and provides host-based intrusion prevention and detection.

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.

About the Symantec Critical System Protection components

Symantec Critical System Protection includes management console and server components, and agent components that enforce policies on computers. The management server and management console run on Windows operating system. 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 user can access, modify policies, configure alerts, and run reports.

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.
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.

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

Policies

Out-of-the-box security policies offer the following features:

- Intrusion prevention
  Proactive security against day-zero attacks
  Protection against buffer over-flow 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/disable style options
- Includes application policies for popular 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 reboot

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* to determine the specific operating system versions supported and the specific agent features for each operating system version.

About the management console

The Symantec Critical System Protection management console provides an interface for users and administrators. It is used to manage Symantec Critical System Protection policies and agents, and perform administrative tasks such as creating user accounts, restricting the functions that users can access, and running reports.

Optionally, you can start and view Symantec Critical System Protection management console from a browser window. The Web console runs in Internet Explorer 8 and 9.

Accessing the management console from browser requires the following software and policies update:

- Management server version 5.2.4 or later.
- Policies 5.2.4 or later.

What you can do from the management console

Symantec Critical System Protection divides features and tasks that you can perform in the management console by pages. You can access the other pages in the management console from any page that you are currently viewing, without losing the state of each page.

Using the pages in the management console, you can do the following:

Home page	You can do the following from the Home page: ■ View statistics about the agents that generated recent events ■ View statistics about the network activity of the most recent events ■ View statistics about the number of agents registered with management server ■ View the current Symantec ThreatCon rating, which provides an overall view of global Internet security ■ Access common tasks and functions that you can perform on other pages in the management console ■ Run LiveUpdate to download and install updates to Symantec Critical System Protection policies and reports

Assets page

You can do the following from the Assets page:

- List all agents that are registered with the management server
- List agents that are registered with the management server and support prevention and detection features
- View the health of agent and not all soft ware on it
- Apply prevention and detection policies to agents and groups
- Apply prevention and detection configurations to agents and groups
- Configure agent health settings
- Register virtual agents that indirectly detect off-platform event data and associate the data with agents in the management console

Policies page

You can do the following from the Policies page:

- View policies enforced by agents
- Create and edit policies
- Organize policies in folders
- Copy and delete policies
- Import and export policies
- Run LiveUpdate to download and install updates to Symantec Critical System Protection policies

Configs page

You can do the following from the Configs page:

- View configurations applied to agents
- Create and edit configurations
- Configure communication between agents and the management server
- Configure which events agents send to the management server
- Configure detection parameters: file, event log, audit, registry, syslog, WTMP, BTMP, and C2 collectors
- Copy and delete configurations
- Import and export configurations

Monitors page

You can do the following from the Monitors page:

- View summaries and details of events produced by Symantec Critical System Protection
- Filter events by time: within the last hour, day, week, month, or year
- Use the Event Wizard to resolve events
- Search events based on criteria such as event type, time of occurrence, severity, source computer, and operating system
- Use real-time monitors to view events as they occur

Reports page	You can do the following from the Reports page: ■ Run predefined queries and reports with charts, graphs, and tables ■ Create custom queries and reports ■ Export report results to a file ■ Run LiveUpdate to download and install updates to Symantec Critical System Protection queries and reports
Alerts page	You can do the following from the Alerts page: ■ Send alerts using email and SNMP messages whenever an event matching an alert filter is observed by Symantec Critical System Protection ■ Create and edit alerts ■ Enable and disable alerts ■ Configure alert settings
Admin page	You can do the following from the Admin page: ■ Create, edit, and delete user accounts ■ Create roles and grant access to assets based on those roles ■ Configure audit settings to audit the execution of searches, queries, and reports ■ Configure Active Directory servers ■ Manage the Apache Tomcat server and Web applications ■ View server configuration on the console

Starting the management console

If you are starting the management console for the first time after installation, you must configure the console. Console configuration prompts you to enter a series of values that consist of port numbers, passwords, and a server name.

See the *Symantec Critical System Protection Installation Guide* for instructions on how to configure the management console after initial installation.

To start the management console

1. Click **Start > Programs > Symantec Critical System Protection > Management Console**.
2. In the Login dialog, in the User name and Password boxes, type your user name and password.
3. In the Login dialog, in the Server box, select the management server.
4. Click **Login**.

To start the management console from a browser

1. Open your web browser.
2. Type the following URL in the Address field:

   https://<ip or servername>:port/scsp

   By default, the Web server administration port number is 8081. If you change the port number during Symantec Critical System Protection installation, then you must substitute that port number in the URL.

Configuring the console to connect to different servers

You can open multiple management console windows that connect to different management servers in your network. For each management server, you need to configure the console.

To configure the console, specify the following:

New Server	A descriptive name for the management server.
Host	The host name or IP address of the management server computer. If you enter a host name, it must be a name that your local system can resolve into the management server's IP address.
Port	The management server port that was used during Symantec Critical System Protection installation. If you used the default port during installation, then use the default port (4443).
Admin Port	The Apache Tomcat administration port that was used during Symantec Critical System Protection installation. If you used the default admin port during installation, then use the default admin port (8081).

Use encrypted communications	Check **Use encrypted communications** to use Secure Sockets Layer (SSL) X.509 certificate-based channel encryption for Symantec Critical System Protection. Default: enabled 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**. If you uncheck **Use encrypted communications**, you must define the SSL connections in the server.xml file, found on the management server. See "Defining the SSL connections in server.xml" on page 26.

To configure the console to connect to different management servers

1. Click **Start > All Programs > Symantec Critical System Protection > Management Console**.
2. In the **Login** dialog box, click the green plus sign (+) icon.
3. In the **New Server Configuration** dialog box, specify the configuration information for the management server to which you want to connect.
4. In the **New Server Configuration** dialog box, click **OK** to save your changes.
5. Type the username for your new management server.
6. Click **Login**.
7. In the **Certificate** dialog box, select **Always accept this certificate**, and then click **OK**.
8. In the **Set Password** dialog box, type the password for the management server you want to set, and then click **Set**.

Defining the SSL connections in server.xml

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 do not want to use SSL X.509 certificate-based channel encryption for Symantec Critical System Protection, you must define the SSL connections in the server.xml file, found on the management server.

The server.xml file is located in the following directory:

<Server_Install_Root>\tomcat\conf

To define the SSL connections in server.xml

1 In the New Server Configuration dialog, uncheck **Use encrypted communications**.

2 Using Notepad or other text editor, edit server.xml.

3 In server.xml, define the SSL connection in the agent service tag.

Inside the agent service tag (look for <Service name="SSS-Agent-Service">), a Connector tag defines the default SSL connection. Immediately following this is a commented definition for a non-SSL connection. To enable non-SSL connections, uncomment the second connection, and change its port number if desired. The port that you specify must not be in use by any other programs on the system. To conserve resources, it is not recommended to leave both connectors uncommented unless you need to use both SSL and non-SSL communications.

4 In server.xml, define the SSL connection in the console service tag.

Inside the console service tag (look for <Service name="SSS-Console-Service">), there is a similar SSL connector and commented non-SSL connector. Follow the same instructions as for the agent connectors.

5 Save the changes to server.xml.

6 Restart the Symantec Critical System Protection Server service.

Selecting a console view

The console views let you organize your agents independently for each feature. The agent groups in each view have no relationship to each other. When collecting policy and configuration data for an agent, Symantec Critical System Protection uses the rules for each console view to find the appropriate data and then sends that data to the agent.

Every console view has different set of console pages. Some pages function identically in each view, while other pages are customized for a view.

Table 1-1 Console views and their associated pages

Console view	Console pages
Home	■ Summary ■ Prevention ■ Detection

Table 1-1 Console views and their associated pages *(continued)*

Console view	Console pages
Assets	■ Network ■ Prevention ■ Detection
Policies	■ Prevention ■ Detection
Configs	■ Prevention ■ Detection
Monitor	■ Events ■ Alerts
Reports	■ Queries ■ Reports ■ Published Results
Admin	■ Users ■ Roles ■ Settings

Your selected console view is preserved as you move among the pages in the management console. You can access the other pages in the console from any page in which you are currently working without losing the state of each page. The management console remembers the last console view that you selected and displays that console view the next time you log on to the management console.

To select a console view

1. In the management console, click any tab.
2. Under the selected tab, click any view.

Refreshing the console pages

The console pages do not refresh automatically. You should manually refresh the console pages to ensure that the information is current.

To manually refresh the Home page

◆ In the management console, on top-right, click **Refresh**.

Setting console preferences

Console preferences comprise general preferences and Monitors page preferences. You can access console preferences from any page in the management console.

General preferences are as follows:

Recent Event Count

The maximum number of events on which the Home page statistics are based. The default setting is 500 events. Depending on the size of or the number of events that are generated in your network, you might want to increase or decrease this value.

Recent Events (hours)

The number of hours on which the Home page statistics are based. The default setting is the last 12 hours (events that occurred in the last 12 hours).

Direct connection to the Internet

Manual proxy configuration

Indicate how the management console connects to the Internet, to view threat alerts. Symantec posts Internet threat alerts, which warn of Internet vulnerabilities. You can view these threat alerts from the management console Home page.

Select one of the following check boxes to indicate how the management console connects to the Internet:

- Direct connection to the Internet
  Check **Direct connection to the Internet** if you use a direct connection to the Internet. By default, this check box is selected.
- Manual proxy configuration
  Check **Manual proxy configuration** if you use a manual proxy configuration. Type the HTTP proxy and port number.

Monitors page preferences are as follows:

Number of events per page (Monitors)

The number of events per page that are shown on the Monitors page. The default setting is 500.

Show event preview by default

Check **Show event preview by default** to view events and event details in the same window. You can continue to display the Event Details window even when this check box is selected.

When changing this setting, you must restart the management console for the setting to take effect.

By default, this check box is selected.

Number of events per page (Search)

The number of events per page that are shown in the search windows. The default setting is 500.

Get old events no farther back than n events	The age of the events that are shown in real-time monitors. The default setting is two days. For example, if the value set is two days, then real-time monitors display events that were logged during the past two days.
On startup, get no more than [n] events	The number of events to accept at a time on startup of real-time monitors. The default setting is 100 events.
Check for new events every n minutes	How many minutes real-time monitors poll for events. The default setting is 1 minute.
Fetch a maximum of n events at a time	The number of events that real-time monitors accept at a time. The default setting is 500 events.

To set console preferences

1. In the management console, on top-right, click **Preferences**.
2. In the Console Preferences dialog, on the General tab, specify the general preferences.
3. In the Console Preferences dialog, on the Monitors tab, specify the Monitors page preferences.

Console timeout

You can set a timeout value for the console. The sis-server.properties file contains the configuration values. This file is located in the C:\Program Files\Symantec\Critical System Protection\Server\tomcat\conf directory. You must edit this file manually to set console timeout. If you have multiple Tomcat servers in your Symantec Critical System Protection Server installation, ensure that you edit each server to get consistent timeout behavior.

For example, to turn on this feature and set the console to lock after 15 minutes of inactivity, add the following lines to sis-server.properties file:

sissession.autologin.enabled=false

sissession.timeout=15

Table 1-2 Console timeout configuration values

Value	Description
sisession.autologin.enabled	When the value is set to true, the console automatically logs on again when the session expires. When the value is set to false, the console prompts the user to enter their password to continue the session.
sissession.timeout	Sets the desired interval of inactivity before the session times out, in minutes.

Accessing Help

If you use Internet Explorer, you may get a security warning or blocked content errors from Internet Explorer Enhanced Security when you try to access the Symantec Critical System Protection help in the console. This issue occurs when a combination of Internet Explorer Enhanced Security and Security Zone GPOs blocks Web access to the help URL in the Symantec Critical System Protection management console. You may or may not be able to add the site to your Trusted sites zone. The **Add** button may not be available, or you may see an error.

Following are some actions that may display the Help system on your computer:

- Add the URL for Symantec Critical System Protection to your Trusted sites zone.
- Disable Internet Explorer Enhanced Security.
- Change the Internet zone security level to **Medium-high**.
- If the Symantec Critical System Protection URL has been added to Restricted Sites, you may need to remove the URL from the Restricted Sites list.

Domain Policy may also need to be adjusted before you can make changes to Internet Options > Security. For example, Domain Policy may prohibit adding URLs to your Trusted sites zone, under Computer Configuration > Administrative Templates > Windows Components > Internet Explorer:

- Security Zones: Use only machine settings
- Security Zones: Do not allow users to change policies
- Security Zones: Do not allow users to add or delete sites

Note: Refer to the following Microsoft article, if you use Internet Explorer 7 on Windows XP, Vista, or Server 2003 and this issue affects you:

You cannot add a Web site to the "Trusted sites" zone when Internet Explorer 7 is installed even when the user account belongs to the Administrators group

Verifying agent deployment and configuration

After installing Symantec Critical System Protection, you can verify your agent deployment and configuration, as follows:

Table 1-3 Steps to verifying agent deployment and configuration

Step	Action	Description
1	Verify agent registration	View the Assets page to verify that your agents registered successfully with the management server. See "Verifying agent registration with the management server" on page 33.
2	View agent and group configuration	View agent and group properties to obtain an overview of how your agents and groups are pre-configured. See "Determining how an agent is configured" on page 34. See "Determining how a group is configured" on page 35.
3	Learn about agent log files	Become familiar with the agent log files. See "About agent log files" on page 35.
4	View agent log rules	View log rules to determine which events are pre-configured for transmission to the management server. See "Viewing log rules that are applied to an agent" on page 36.
5	View detection parameters	View detection parameters to determine how the detection features of your agents operate. See "Viewing detection parameters applied to an agent" on page 36.
6	View communication parameters	View communication parameters to determine how agents are pre-configured to communicate with the management server. See "Viewing communication parameters applied to an agent" on page 38.

Table 1-3 Steps to verifying agent deployment and configuration *(continued)*

Step	Action	Description
7	View event logging parameters	View logging parameters to determine how agents are pre-configured for event logging. See "Viewing event logging parameters applied to an agent" on page 39.

Verifying agent registration with the management server

Upon initial installation, all agents automatically register with the management server and are assigned to the Network group in the Master view. You can verify agent registration by viewing the Assets page in the Master view. The Master view lets you monitor your entire agent deployment.

Your agent deployment includes the SCSP Manager virtual agent that was automatically created during installation. SCSP Manager collects all server-related events. SCSP Manager is registered into the Virtual Agents folder in the Network group, in the Master view.

See "About the SCSP Manager virtual agent" on page 87.

To verify agent registration with the management server

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Network**.
3. To view your deployed agents, in the Network Assets tree, click **Network**.
4. To view the SCSP Manager virtual agent, in the Network Assets tree, click the **Virtual Agents** folder.

About the management server health icon

In the management console menu bar, the overall health of the connection between the management server and the database is indicated by one of the following icons:

- A green circle icon indicates that the management server is running.
- A red circle icon indicates that a management server or database error has occurred.

About the agent pane

The agent pane lists the agents in a selected policy or configuration group. The agent pane is located on the right side of the Assets page. The bottom half of the agent pane lists details about a selected agent.

The agent pane comprises the following columns of information about each agent:

Agent Health	The first column in the agent pane. It indicates whether an agent is in contact with the management server.
Feature State	The second column in the agent pane. It appears in the Master view and Prevention view. Each prevention feature supported by the management console has a Feature State column.
Name	The host name of the agent computer.
IP Address	The IP address of the agent computer.
Policy	The name of the prevention policy applied to the agent. A folder icon is shown after the policy name if the agent gets its policy from a group.
Version	The Symantec Critical System Protection software version installed on the agent computer.
OS	The agent operating system.
Last Contact	The date and time that the agent last contacted the management server to request policy and configuration updates.

See “About the agent pane” on page 84.

Determining how an agent is configured

You can obtain an overview of how an agent is configured by viewing agent properties. You can view agent properties to determine which policies and configurations are applied to an agent, and in which groups an agent resides. You can view agent properties to track agent event file activities. You can view agent properties to list the agent that most recently collected a virtual event for a virtual agent.

You can view agent properties to track the health of an agent. Agent health is denoted by a green/yellow/red circle icon. A green icon indicates that an agent is online. A yellow icon indicates that an agent is possibly offline. A red icon indicates that an agent is offline. Separate yellow/red default values are provided for native and virtual agents.

To obtain an overview of agents that support prevention or detection features, view agent properties in the Prevention view or Detection view. To obtain an overview of your entire agent deployment, view agent properties in the Master view, as illustrated in the following instructions.

To determine how an agent is configured

1. In the management console, click **Assets**.
2. On the **Assets** page, select an agent, and then right-click **Properties**.
3. In the agent properties dialog box, click a tab to view the properties for the selected agent.
4. In the agent properties dialog box, on the **General** tab, click **Configure Health** to view agent health settings.
5. Click **OK**.

See “Viewing and configuring agent and group properties” on page 89.

Determining how a group is configured

You can obtain an overview of how a group is configured by viewing group properties. You can view group properties to determine which policies and configurations are applied to a group.

See “Viewing group properties” on page 97.

About agent log files

Symantec Critical System Protection agent log files contain events processed by an agent. Agent log files are stored on a local agent computer. Multiple versions of a log file may exist, as old versions are closed and new versions are opened.

You can view the events in a log file to verify the operation of an agent computer, to troubleshoot connectivity problems in your network, to track failed attempts by users to access information or to log on to computers.

The agent log files are as follows:

SISIDSEvents*.csv	Contains all events recorded by an agent. If bulk logging is enabled for the agent, this file is uploaded to the management server. The asterisk in the file name represents a version number. Bulk logging captures events to compressed log files instead of transmitting all events in real-time to the database for storage.

SISIPSRTEvents*.csv	Contains real-time events processed by the an agent. The is a temporary file that is used to speed processing of real-time events. All of the events in the file (as configured in the agent's log rules) are forwarded to the management server. The file is deleted once processing is complete (that is, the file is rolled over). The asterisk in the file name represents a version number.

To learn more about agent log files:

See "About agent log files" on page 257.

Viewing log rules that are applied to an agent

Agents use log rules to determine which events to send to the management server.

Agents that support prevention features use prevention log rules. Upon initial installation, the default prevention log rules are applied to agents when they register with the management server.

Agents that support detection features use detection log rules. Upon initial installation, the default detection log rules are applied to agents when they register with the management server.

To view log rules that are applied to an agent

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. In the left-hand pane, under **Asset Configs**, select a configuration group.
4. On the **Assets** page, in the agent pane, select an agent, and then right-click **View Config**.
5. In the configuration dialog box, click the **Log Rules** tab to view the log rules that are applied to the selected agent.
6. Click **OK**.

See "About prevention configurations" on page 159.

See "About detection configurations" on page 160.

Viewing detection parameters applied to an agent

Detection parameters control how the detection features of an agent operate. Agents that support detection features use detection parameters. Upon initial installation, the default detection parameters are applied to agents when they register with the management server.

Detection parameters comprise the following:

File Collector

The file collector determines how agents monitor files. Intruders often attempt to replace critical system files with Trojan horse versions, or alter system files to create a back door for future intrusions. The file collector detects changes to these system critical files.

The file collector is valid for agents that are installed on supported Windows and UNIX operating systems. By default, the file collector is enabled.

Event Log Collector

The event log collector looks for matches in the Windows event log. By default, the event log collector is enabled.

Audit Collector

The audit collector monitors events from Windows standard system audit logs. The system audit log sources in Windows are Security, Application, and System. By default, the audit collector is enabled.

Registry Collector

The registry collector watches for changes made to registry keys on the Windows operating system. By default, the registry collector is enabled.

Syslog Collector

The syslog collector watches for syslog daemon tampering on UNIX-based operating systems. By default, the syslog collector is enabled.

WTMP Collector

The WTMP collector monitors the WTMP logging system on UNIX-based operating systems. By default, the WTMP collector is enabled.

BTMP Collector

The BTMP collector monitors the BTMP logging system on UNIX-based operating systems. By default, the BTMP collector is enabled.

C2 Collector

The C2 collector monitors the C2 audit logging system on Solaris, Linux, HP-UX, and AIX operating systems. By default, the C2 collector is disabled.

To view detection parameters applied to an agent

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Detection**.
3. In the left-hand pane, under **Asset Configs**, select a configuration group.
4. On the Assets page, in the agent pane, select an agent, and then right-click **View Config**.
5. In the configuration dialog box, click the **Parameters** tab to view the detection parameters that are applied to the selected agent.
6. Click **OK**.

See “About detection configurations” on page 160.

Viewing communication parameters applied to an agent

Communication parameters control how agents communicate with the management server.

Upon initial installation, the default communication parameters are applied to agents when they register with the management server.

Communication parameters comprise the following:

Polling Interval

The polling interval is the frequency at which an agent polls the management server for configuration changes. Upon initial agent installation, polling interval is set to 300 seconds.

Polling interval is the most reliable method for agents to obtain configuration changes.

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. The agent uses a user-specified port to communicate with the management server.

Upon initial agent installation, real-time notification is enabled.

Port

The port that is used by the agent to communicate with the management server, for use with real-time notification.

Upon initial agent installation, port is set to 2222.

Connection Timeout

The connection timeout is the TCP/IP connection timeout for connections initiated by an agent to the management server.

Upon initial agent installation, connection timeout is set to 30 seconds.

To view communication parameters applied to an agent

1. In the management console, click **Assets**.
2. Under the Assets tab, click **Prevention** or **Detection**.
3. In the left-hand pane, under **Common Configs**, select a common configuration group.
4. On the Assets page, in the agent pane, select an agent, and then right-click **View Config**.

5 In the **Default Common Parameters** dialog box, click the **Communication** tab to view the communication parameters that are applied to the selected agent.

6 Click **OK**.

See “About common configurations” on page 153.

Viewing event logging parameters applied to an agent

Event logging parameters control how agents log events.

Upon initial installation, the default event logging parameters are applied to agents when they register with the management server.

Event logging parameters comprise the following:

Enable log consolidation

Log consolidation controls when an agent consolidates similar log events into a summary event that is sent to the management server. Similar log events that occur consecutively, within a user-specified summary delay period, are consolidated into a summary event. The summary event includes a count of the number of similar log event occurrences.

Log consolidation only occurs for prevention events.

Upon initial agent installation, log consolidation is enabled. The delay is set to one minute.

Enable log rotation

Log rotation determines how and when agents rotate event log files. When an agent rotates an event log file, the current log file is closed and nothing more is written to it. A new log file is opened with the same base file name. Once a log file is rotated, the old file might still be in use by the agent. Although no new records are written to the log file, the agent might still have to process events and send them to the management server.

Agent log files are compressed into .zip files when processing is finished. The .zip files are stored in the archive subdirectory if the agent is not configured to delete them after processing.

The frequency at which agents rotate log files is based on one of the following parameters:

- File size
  Agents can rotate log files based on log file size. When a log file reaches a user-specified size, a new log file is started.
- Time interval
  Agents can rotate log files based on a user-specified time interval (monthly, weekly, daily, hourly).

Upon initial agent installation, log rotation is enabled. Log files are rotated based on file size, which is set to 10 MB.

Enable bulk log transfer

Bulk log transfer lets you collect events of long-term interest without burdening the network or flooding the Symantec Critical System Protection database.

If bulk log transfer is enabled, the agent log file is transmitted to the management server, where it is stored. When you are ready to load the events into the database, you run the Bulk Loader Utility. This utility interprets a compressed bulk log file and populates the database with the events from the file.

Upon initial agent installation, bulk log transfer is disabled.

Delete log files after processing

Delete log files after processing deletes an event log file after Symantec Critical System Protection reads the events in the file.

Upon initial agent installation, the option to delete log files after processing is disabled.

Stop/restart logging at disk usage	An agent monitors the used disk space on the disk that contains the agent log files, to avoid filling the disk completely. The agent checks the percentage of used disk space at each polling interval. If the percentage of used disk space exceeds the configured stop logging threshold, the agent stops logging events to the log file. Logging remains off until the percentage of used disk space drops below the configured start logging threshold. At this point, the agent restarts logging events to the log file. When stopping or restarting logging, the agent generates a log message, which appears on the Monitors page. Upon initial agent installation, stop logging at disk usage is set to 95 percent, restart logging at disk usage is set to 85 percent.
Reader/writer limit	The reader limit and the writer limit control how an agent processes events that are sent to the Monitors page. The reader limit is the maximum number of events processed before an agent pauses. By pausing after a specified number of events, the agent avoids consuming too many system resources. Increasing the reader limit lets the agent consume more resources, but gets events to the Monitors page more quickly. Decreasing the reader limit reduces the resources that the agent consumes, but gets events to the Monitors page more slowly. The writer limit is the maximum number of events that an agent can send in a single TCP/IP connection. Creating a TCP/IP connection is overhead, and sending multiple events in a single connection reduces the average overhead per event. Upon initial agent installation, reader limit is set to 1000 events, writer limit is set to 10 events.

To view event logging parameters applied to an agent

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. In the left-hand pane, under **Common Configs**, select a common configuration group.
4. On the Assets page, in the agent pane, select an agent, and then right-click **View Config**.
5. In the **Default Common Parameters** dialog box, click the **Logging** tab to view the event logging parameters that are applied to the selected agent.
6. Click **OK**.

See "About common configurations" on page 153.

Applying the Symantec policies to agents or groups

Symantec Critical System Protection includes a library of prevention and detection policies that were developed by Symantec security experts. You can begin enforcing the Symantec Critical System Protection policies on your agents immediately after agent installation and registration with the management server.

Table 1-4 outlines the steps to enforcing the Symantec Critical System Protection policies.

Table 1-4 Enforcing the Symantec Critical System Protection policies

Step	Action	Description
1	Review the pre-configured policies included with Symantec Critical System Protection	The *Prevention Policy Reference Guide* describes the prevention policies included with Symantec Critical System Protection. The *Detection Policy Reference Guide* describes the detection policies included with Symantec Critical System Protection.
2	Adjust the policies to meet your environment needs	You can apply the policies out of the box to your agents and policy groups. You can adjust the policies to meet specific environment needs. Use the management console to adjust the policies.
3	Test a policy on a few agents	Set up a test environment and apply a policy to a few agents. Test the policy, verifying that the agent computers function properly with the applied policy. To verify that an agent computer functions property with an applied policy, view the events that the agent sent to the management server. See "Viewing event activity" on page 46.
4	Apply the policies to your agents	If the agent computers perform as designed in a test environment, then you are ready to apply the policy on a broader scale. You might want to implement a pilot in the production environment, so that you can fine-tune the restrictions enforced by the policies.

Applying a Symantec prevention policy to an agent or group

Symantec Critical System Protection prevention policies protect against inappropriate modification of system resources. You can use the prevention policies with supported Windows, Solaris, AIX, and Linux operating systems.

See the *Symantec Critical System Protection Prevention Policy Reference Guide*.

Before you apply a prevention policy to an agent, please note the following:

- You can select the global disable prevention policy option to temporarily disable the policy. The disable prevention policy option is useful if you want to test a prevention policy. The disable prevention policy option logs policy violations, but does not enforce them. This lets you gather information about how a computer performs, without running the risk of preventing critical aspects of your computer operation.
  See "Disabling prevention on an agent computer" on page 44.
- Upon agent installation, the Null prevention policy is applied to every agent that registers with the management server. The Null prevention policy offers no protection for an agent computer.
- The Null prevention policy and the disable prevention policy option both offer no protection for an agent computer. The Null prevention policy does not log policy violations. The disable prevention policy option logs policy violations.

To apply a Symantec prevention policy to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention**.
3. On the Assets page, select an agent or policy group, and then right-click **Apply Policy**.
4. In the **Set Policy Wizard** dialog box, double-click the **Symantec** folder to list the Symantec policies.

   If you are applying a policy directly to an agent, the operating system is selected for you. If you are applying a policy to a policy group, you must select the operating system.
5. In the **Set Policy Wizard** dialog box, select a Symantec policy, and then click **Next**.
6. If you do not want to enforce the Symantec prevention policy at this time, in the **Set Policy Wizard** dialog box, select the **Disable Prevention** check box, and then click **Next**.
7. If prompted, select the merge option, and then click **Next**.

   See "About merging policy options" on page 108.

8. In the Set Policy Wizard dialog, review the policy summary, and then click **Finish** to apply the Symantec prevention policy to the agent or policy group that you selected.
9. In the management console, click **Refresh** to update the view.
10. Verify that the agent computer functions properly with the applied policy.

    See "Verifying prevention policies" on page 141.

Disabling prevention on an agent computer

There may be occasions when you want to disable prevention on an agent computer. For example, you may need to install or uninstall software on the agent computer, or use the agent computer to access blocked resources such as files and networks.

You can disable prevention on an agent computer as follows:

- Apply the Null prevention policy to the agent
  The Null prevention policy provides no protection for an agent computer. It does not log policy violations.
- Enable the global disable prevention policy option in a prevention policy that is applied to the agent
  The global disable prevention policy option in the Symantec Critical System Protection prevention policies temporarily disables policy prevention for an agent computer. The policy violations are logged by the agent, but are not enforced.
  See "Editing a workspace policy" on page 132.
- Override an agent's prevention policy using the policy override tool
  The policy override tool overrides prevention policy enforcement on agent computers that run supported Windows and UNIX operating systems. The prevention policy that is applied to an agent computer must be configured for policy override.
  See "Overriding prevention policy enforcement" on page 49.

Applying a Symantec detection policy to an agent or group

Symantec Critical System Protection detection policies monitor events and syslogs, and report abnormal behavior. You can use the detection policies with supported Windows and UNIX operating systems.

Symantec Critical System Protection detection policies include the following features:

- 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

See the *Symantec Critical System Protection Detection Policy Reference Guide*.

By default, no detection policies are applied to agents when they register with the management server.

To apply a detection policy to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Detection**.
3. On the Assets page, select an agent or policy group, and then right-click **Apply Policy**.
4. In the **Set Policy Wizard** dialog box, double-click the **Symantec** folder to list the Symantec policies.

   If you are applying a policy directly to an agent, the target operating system is selected for you. If you are applying a policy to a policy group, you must select the target operating system.
5. In the **Set Policy Wizard** dialog box, select one or more Symantec policies, and then click **Next**.

   To select multiple detection policies, hold down the Shift or Ctrl key while selecting the policies.
6. If prompted, select the merge option, and then click **Next**.

   See "About merging policy options" on page 108.
7. In the Set Policy Wizard dialog, review the policy summary, and then click **Finish** to apply the Symantec detection policies to the agent or group that you selected.
8. In the management console, click **Refresh** to update the view.
9. Verify that the agent computer functions properly with the applied policies.

Applying detection policies to the default OS-specific groups

The following OS-specific detection policy groups are set up during Symantec Critical System Protection installation:

- AIX
- HP-UX
- Linux

- Solaris
- Tru64 UNIX
- Windows

By default, these OS-specific policy groups do not have any detection policies applied to them. If you apply detection policies to these groups, the policies are automatically applied to agents when they register with the management server.

Viewing event activity

You can verify the operation of an agent computer by viewing the events that were reported by the agent. Events are informative, notable, and critical activities that concern the Symantec Critical System Protection agent and management server. The agent logs events to the management server, and the management console lets you view summaries and details of those events. Agent log rules determine which events the agent sends to the management server.

The key methods that you can use and the locations where you can view event activity are as follows:

- Home page
- Monitors page
- Agent event viewer
- Agent event file health
- Object-specific events
- Event Wizard, Event Agent, Event Details, Event Policy commands

Viewing events generated in your network

You can use the Home page in the management console to obtain an overview of events that are generated in your network.

The Home page includes the following information:

Agent Prevention Summary	Displays statistics about the agents that generated recent prevention events.
Network Actions	Displays statistics about the network activity of the most recent events.
Agent Statistics	Displays statistics about agents that support the prevention features and detection features of Symantec Critical System Protection.

Agent Detection Summary	Displays statistics about the agents that generated recent detection events.
Event Rule Summary	Displays statistics about recent rules.

Viewing events reported by the management server

You use the Monitors page in the management console to display events reported to the management server from your entire agent deployment. The Monitors page features filtered event summaries, ad-hoc event searches, and event-specific details. Real-time monitors show events as they are sent in real time to the management server.

See “Viewing agent properties” on page 89.

See “Resolving events” on page 182.

Viewing agent, event, and Internet statistics

You can view current agent, event, and Internet statistics that indicate the health and status of your network. You can identify problem computers and threats to your network's security by analyzing this information.

The Home page provides the following statistical information about your network:

Agent Event Summary pane

Displays statistics about the agents that generated recent events. The statistics include the agent computer name, event categories, and the number of events per category. The Agent Event Summary pane is sorted by the descending total number of events for each agent, which causes the agents that generate the most events to be at the top of the list. The length of the bar chart for each agent shows the proportion of the recent events that belong to that agent.

Event Type Distribution pane

Displays statistics about the most recent events. The statistics include event type, disposition (deny, allow, error, failure, success), and the number of events per disposition. The Event Type Distribution pane is sorted by the descending total number of events for each event type, which causes the event types with the most events to be at the top of the list. The length of the bar chart for each event type shows the proportion of the recent events that belong to that type.

Agent Statistics pane

Displays statistics about the number of agents that are registered to the management server.

Threat Level pane	Displays the Symantec ThreatCon rating, and the date and time that the Threat Level was last updated. This rating provides an overall view of global Internet security. You can view important information about current threats and security risks, definition updates that are currently available, and network security tips that prevent intrusions.

You can also obtain statistics for agents that support prevention features and for agents that support detection features.

To view agent, event, and Internet statistics

◆ In the management console, click **Summary**.

About the Symantec queries and reports

Symantec Critical System Protection includes predefined queries and reports that provide an overall view of your deployed environment, as well as prevention, detection, and management activity. The graphical reporting capabilities include tables, pie charts, and graphs (line, bar, and area).

The Symantec queries can help you identify groups with policies that provide no protection or only partial protection. The queries can help you identify agents that are disconnected from the network for a period of time or that are experiencing network connectivity issues.

About updating Symantec policy and report packs

Symantec Critical System Protection LiveUpdate downloads policy packs and report packs. Policy packs contain revisions to Symantec prevention and detection policies. Report packs contain revisions to Symantec queries and reports. For each content type, you can download a single update, all available updates, or any combination of the available updates. LiveUpdate automatically downloads and imports your selected content into the management server database.

Note: If you have a valid serial number for Symantec Critical System Protection, you can use the Symantec FileConnect Web site to download policy and report packs. If you have a valid contract ID for Symantec Platinum Support, you can use the Platinum Support Web site to download policy and report packs.

After downloading the policy or report packs, you must import the content into the Symantec Critical System Protection management server database.

See “Importing and exporting policies” on page 137.

See "Importing queries and reports" on page 219.

Before you run LiveUpdate, you should note the following:

- You must explicitly check for updates to Symantec Critical System Protection content.
- Symantec Critical System Protection content is downloaded in separate policy packs and report packs.
- During LiveUpdate, the management console is locked; you cannot access other management console tasks. A Cancel button lets you abort LiveUpdate.
- When run from the management console, LiveUpdate downloads and imports compiled policy packs into the management server database.
- Each Symantec Critical System Protection content type is distributed independently. LiveUpdate can recognize one content type (for example, prevention policy packs) as up-to-date and another content type (for example, detection policy packs) as out-of-date.
- All content types are queried and can be downloaded, whether or not any agents exist that can use the content. For example, if you use prevention policies but do not use detection policies, you are still notified of updates to detection policies.
- When an update is available, the entire policy pack or report pack is downloaded.

Overriding prevention policy enforcement

As the Symantec Critical System Protection administrator, you can allow all users or specific users and user groups to override a prevention policy on an agent computer.

To allow a user to override a prevention policy, you configure the global policy override option.

See the *Symantec Critical System Protection Prevention Policy Reference Guide*.

To override a prevention policy, users use the policy override tool.

About user accounts

User accounts provide secure access to the Symantec Critical System Protection management console.

When you create a user account, you must assign one or more roles to the account. The roles that you assign determine what functions the user can perform in the management console. You can assign predefined roles or custom roles.

Symantec Critical System Protection includes five predefined roles: Administrators, Authors, Guests, Managers, and Query Tool Users. The default account (symadmin) that was created during Symantec Critical System Protection installation is assigned the Administrators role.

See "Creating a user account" on page 236.

Increasing the amount of memory used for the console

The default heap space for the Symantec Critical System Protection console is 512 MB. At times, it is possible that the console may need even more memory to function properly. If so, you can use the following procedure to increase the heap space.

To temporarily increase the amount of memory used for the console

1. Open a window with a command prompt on the computer that runs the console.
2. Change directory to `drive:\Program Files\Symantec\Critical System Protection\Console`.
3. Type the following command:

   console.exe -J-Xmx1024m

To permanently increase the amount of memory used for the console

1. Right-click the management console desktop shortcut icon, and then click **Properties**.
2. On the **Shortcut** tab, add the following to the end of the **TARGET** property:

   -J-Xmx1024m

About the management console commands

The following tables list popular management console commands. Many of the commands are available from a menu and by right-clicking a selected agent, policy, or configuration. Some commands are available as tool bar icons.

Table 1-5 Symantec Critical System Protection commands

Command	Console page	Description
Refresh	All	Apply pending agent updates.
Preferences	All	Set general and Monitors page preferences.
Help > Contents and Index	All	Display Symantec Critical System Protection Help.
Help > Online Support	All	Go to the Symantec web site support page.
Edit Policy	Assets	Edit a policy applied to an agent or group.
Apply Policy	Assets	Apply a policy to an agent or group.
Save Applied Policy	Assets	Save an applied policy as a workspace policy.
Clear Policy	Assets	Clear a policy applied to an agent or group.
Move To Move Back	Assets	Move an agent to a group. Move an agent back to its previous group.
Rename	Assets	Modify the name of an agent.
View Config	Assets	View a configuration applied to an agent or group.
Apply Config	Assets	Apply a configuration to an agent or group.
Clear Config	Assets	Clear a configuration applied to an agent or group.
New Virtual Agent	Assets	Manually register a virtual agent.
Properties	Assets	View properties for an agent or group.
Delete	Assets	Delete an agent in the Master view. Delete an agent from a detection policy group.
Edit Policy	Policies	Edit a workspace policy.
New Policy	Policies	Create a workspace policy.
New Folder	Policies	Create a policy folder.
Copy Policy	Policies	Make a copy of a workspace policy.
Update Policy	Policies	Update a workspace policy with Symantec policy packs.
Copy Options	Policies	Copy all policy options from one workspace policy to another workspace policy.

Table 1-5 Symantec Critical System Protection commands *(continued)*

Command	Console page	Description
Copy Custom Controls	Policies	Copies the options to control a custom program from one workspace policy to another workspace policy.
Apply Policy	Policies	Apply a workspace policy to an agent or group.
Reapply Policy	Policies	Reapply a (modified) workspace policy to an agent or group.
Move To	Policies	Move a workspace policy to a folder.
Import Policy	Policies	Import a workspace policy from a file.
Export Policy	Policies	Export a workspace policy to a file.
Rename Policy	Policies	Rename a workspace policy.
Delete Policy	Policies	Delete a workspace policy.
Create Default	Policies	Create default workspace policies for all policies in an installed Symantec Critical System Protection policy pack.
Properties	Policies	List the agents and groups to which a workspace policy is applied.
New Config	Configs	Create a workspace configuration.
New Folder	Configs	Create a configuration folder.
Copy Config	Configs	Make a copy of a workspace configuration.
Apply Config	Configs	Apply a workspace configuration to an agent or group.
Reapply Config	Configs	Reapply a (modified) workspace configuration to an agent or group.
Move To	Configs	Move a workspace configuration to a folder.
Import Config	Configs	Import a workspace configuration from a file.
Export Config	Configs	Export a workspace configuration to a file.
Rename Config	Configs	Rename a workspace configuration.
Delete Config	Configs	Delete a workspace configuration.

Table 1-5 Symantec Critical System Protection commands *(continued)*

Command	Console page	Description
Properties	Configs	List the agents and groups to which a workspace configuration is applied.
Event Details	Monitors	View details for a selected event. You can invoke Event Details from Recent Events tabs and History tabs.
Event Agent	Monitors	View the properties of the agent that reported a selected event.
Event Policy	Monitors	Display the policy that caused a selected event. You can invoke Event Policy from Recent Events tabs.
Event Wizard	Monitors	Resolve events shown on the Monitors page. You can invoke Event Wizard from Recent Events tabs.
New Monitor (button)	Monitors	Create a new real-time monitor.
New Folder	Reports	Create a query or report folder.
Rename Folder	Reports	Rename a query or report folder.
Delete Folder	Reports	Delete a query or report folder.
New Query New Report	Reports	Create a query or report.
Edit Query Edit Report	Reports	Edit a query or report.
Run Query Run Report	Reports	Run a query or report.
Copy Query Copy Report	Reports	Make a copy of a query or report.
Move To	Reports	Move a query or report to a folder.

Table 1-5 Symantec Critical System Protection commands *(continued)*

Command	Console page	Description
Publish Query Publish Report	Reports	Save a snapshot of the graphic or tabular results from running a query or report.
Export Published Results	Reports	Export a published query or report to.zip file.
Import Published Results	Reports	Import a published query or report from.zip file.
Export as PDF	Reports	Export a published report to .pdf file.
Export as HTML	Reports	Export a published report to html or .htm file.
Export Query Export Report	Reports	Export a query or report to .zip file.
Import Query Import Report	Reports	Import a query or report from .zip file.
Delete Query Delete Report	Reports	Delete a query or report.
Rename Query Rename Report	Reports	Rename a query or report.
LiveUpdate	Home, Policies, Reports	Download and update Symantec policy and report packs.

Diagnosing problems with Symantec Critical System Protection

Symantec provides batch scripts that you can run to collect agent and management server information. Symantec uses this information to diagnose problems with Symantec Critical System Protection.

Do the following if you experience problems with Symantec Critical System Protection:

1. Run the scripts to collect agent and management server information.
2. Save the output files produced by the batch scripts.
3. Contact Symantec Support for further instruction.

   To find out how to contact Symantec, visit the Symantec Support Web site:

   http://www.symantec.com/techsupp/enterprise/

Collecting information on agent computers

To collect agent information, you run the agent collect info script. You can run the script from an agent computer or the management console.

Running the collect info script from a Windows agent computer

To collect information on a Windows agent computer, you can run the collect info script directly from the agent computer.

To run the collect info script from a Windows agent computer

1. Log on to a Windows agent computer.
2. Click **Start > Programs > Symantec Critical System Protection> Collect Agent Info**.

   You see the following messages:

```
Collecting Install Logs...
Collecting Event Logs...
Collecting System Info...
Collecting Registry Info...
Collecting IPS Service Settings...
Collecting IDS Service Logs and Settings...
Collecting Logs...
Collecting IPS Driver Settings...
Collecting SCSP Environment Settings...
Zipping Info...
Cleaning Up...
*** Please send the ZIP file:
*** D:\Temp\20060720_133411_001_CW_MACHINENAME.zip
*** to Symantec support
Press any key to continue...
```

Running the collect info script from a UNIX agent computer

To collect information on a Solaris, Linux, AIX, HP-UX, or Tru64 agent computer, you can run the agent collect info script directly from the agent computer.

To run the collect info script from a UNIX agent computer

1. Log on to a UNIX agent computer.
2. Navigate to the following directory:

   /opt/Symantec/scspagent/IPS/tools/
3. At a command prompt, type and run the following command:

   ```
   # ./getagentinfo.sh
   ```

   You see the following messages:

   ```
   Collecting Install Logs...
   Collecting System Info...
   Collecting syslog Files...
   Collecting System Startup Info...
   Collecting SCSP Logs...
   Collecting SCSP IPS Configuration Settings...
   Collecting SCSP IDS Configuration Settings...
   Zipping Info...
   Cleaning Up...
   *** Please send the Info File:
   ***   /tmp/20060720_133411_001_CW_MACHINENAME.tar.Z
   *** to Symantec
   ```

Running the collect info script from the management console

To collect information about a Windows or UNIX agent computer to which you do not have login access, you use the CSP_Agent_Diagnostics detection policy. A version of the 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 run the collect info script from the management console

1. Log on to the management console as an administrator.
2. In the management console, under **Policies** tab, click **Detection**.
3. On the **Policies** page, in the Workspace pane, edit the **CSP_Agent_Diagnostics** policy.

4. In the **CSP_Agent_Diagnostics** dialog box, under **Policy Settings**, click **Diagnostic functions**.
5. In the **CSP_Agent_Diagnostics**dialog box, check **Select a function to run on the agent**, and then click **Edit**.
6. In the **Value** box, select **Run the collect info script**.
7. Click **OK** to save the policy changes.
8. Apply the policy to the agent.

   See “Applying a policy to an agent or policy group” on page 106.

   See “Clearing a policy applied to an agent or group” on page 110.
9. Log on to the management server to get the collect info output file.

   Get the collect info output file from the server directory:C:\Program Files\Symantec\Critical System Protection\Server\logfiles\<hostname>\<date>\

Collecting information on the management sever

To collect management server information, you run the server collect info batch script C:\Program Files\Symantec\Critical System Protection\Server\tools\getserverinfo.bat.

To collect information on the management server

1. On the management server computer, navigate to the following directory:

   C:\Program Files\Symantec\Critical System Protection\Server\tools
2. Double-click `getserverinfo.bat`..

   You see the following messages:

   ```
   Collecting Install Logs...
   Collecting System Info...
   Collecting Registry Info...
   Collecting App Server Logs and Settings...
   Collecting Database Logs and Settings...
   Zipping Info...
   Cleaning Up...
   *** Please send the ZIP file:
   *** D:\Temp\sis_server_MACHINENAME_07201350.zip
   *** to Symantec support
   Press any key to continue...
   ```

Chapter 2

Using the Home page

This chapter includes the following topics:

Viewing the Home page

The Home page provides current agent, event, and Internet security statistics that indicate the health and status of your network. You can identify problem computers and threats to your network's security by analyzing this information.

You can do the following activities from the Home page:

- View statistics for your entire network.
- View statistics for agents that support prevention features.
- View statistics for agents that support detection features.
- View the Symantec ThreatCon rating.
- Access popular management console tasks.

You can view the Home page in all three console views. Each view presents a customized view of agent and event statistics.

To view the Home page

1. In the management console, click **Home**.
2. To display a pop-up tool tip, place your cursor over a hypertext link or a bar chart.

Running queries

The Home page contains hyperlinks to Symantec Critical System Protection queries. When you click a link, Symantec Critical System Protection runs the corresponding query.

For example, when you click the **Registered Agents** link in the **Agent Statistics** pane, Symantec Critical System Protection does the following:

- Displays the Reports page in the management console.
- Runs the query that provides statistics on registered agents.
- Displays the query results.

Refreshing the Home page

The information on the Home page automatically refreshes when you log on to the management console and whenever you return to the Home page from another page in the management console.

You can manually refresh the Home page, as well as the other pages in the management console, to ensure that the information is current.

To manually refresh the Home page

◆ In the management console, click **Refresh**.

Setting the event count in the console preferences

You use console preferences to set the recent event count (the maximum number of events) on which the Home page statistics are based. The default setting is 500 events. Depending on the size of or the number of events that are generated in your network, you might want to increase or decrease this value.

See “Setting console preferences” on page 29.

Using the Home page in the Summary view

The Home page in the Summary view provides current agent, event, and Internet security statistics for your network.

About the Agent Event Summary pane

The **Agent Event Summary** pane lets you view statistics about the agents that generated recent events. The statistics include the agent computer name, event categories (prevention, detection, management), and the number of events per category.

The **Agent Event Summary** pane includes the SCSP Manager virtual agent, which collects all server-related events. SCSP Manager is registered into the Virtual Agents folder in the Network group, in the Summary view.

See “About the SCSP Manager virtual agent” on page 87.

The **Agent Event Summary** pane is sorted by the descending total number of events for each agent, which causes the agents that generate the most events to be at the top of the list. The length of the bar chart for each agent shows the proportion of the recent events that belong to that agent.

For troubleshooting purposes, you can view additional event details. To view all events generated for an agent, click the agent computer name. To view a summary of all generated events, click the **Summary** link.

About the Event Type Distribution pane

The **Event Type Distribution** pane lets you view statistics about the most recent events. The statistics include event type, disposition (deny, allow, error, failure, success), and the number of events per disposition.

The **Event Type Distribution** pane is sorted by the descending total number of events for each event type, which causes the event types with the most events to be at the top of the list. The length of the bar chart for each event type shows the proportion of the recent events that belong to that type.

For troubleshooting purposes, you can view additional event details. To view all events for an event type, click the event type link. To view a summary of all event types, click the **Summary** link.

About the Agent Statistics pane

The Agent Statistics pane lets you view statistics about the number of agents that are registered to the management server.

You can view the following statistics:

Registered agents	Displays statistics for agents in the Summary view.
Windows agents	Displays statistics for Windows agents.
UNIX agents	Displays statistics for UNIX agents.
Native agents	Displays statistics for real agents running Symantec Critical System Protection agent on the local machine.
Virtual agents	Displays statistics for virtual agents.
Offline agents	Displays statistics for agents that are offline.
Agents with null prevention policy	Displays statistics for agents using the null prevention policy.
Agents with no detection policy	Displays statistics for agents that are not using a detection policy.
Agents with errors	Displays statistics for agents with errors.
Agents with policy updates	Displays statistics for agents with pending policy updates.
Agents with configuration updates	Displays statistics for agents with pending configuration updates.

About the Threat Level pane

The Threat Level pane lets you view the Symantec ThreatCon rating, and the date and time that the Threat Level was last updated. This rating provides an overall view of global Internet security. You can also view important information about current threats and security risks, definition updates that are currently available, and network security tips that prevent intrusions.

Viewing Threat Level details

You can view additional details about current threats by accessing the Symantec™ Security Response Web site from the Threat Level pane.

To view Threat Level details

1. In the management console, click **Home**.
2. Under the **Home** tab, click **Summary**.
3. Under **Threat Level**, click the **ThreatCon** icon.

   The Symantec Security Response home page appears.

About the Quick Links pane

The **Quick Links** pane provides the following links:

Manage Assets	Display the Assets page.
View Events	Display the Monitors page.
Run Reports	Display the Reports page.
New Alert	Display the Alerts page, and then display the dialog for creating an alert to send email and SNMP messages when specific events are observed by Symantec Critical System Protection.
New User	Display the Admin page, and then display the dialog to create a new user account for accessing the management console. See "Creating a user account" on page 236.
New Role	Display the Admin page, and then display the dialog to create a custom role. See "Creating a custom role" on page 240.
LiveUpdate	Run LiveUpdate to download and install updates to Symantec Critical System Protection policies and reports. See "About updating Symantec policy and report packs" on page 48.

Using the Home page in the Prevention view

The Home page in the Prevention view provides current agent and event statistics for agents that support the prevention features of Symantec Critical System Protection.

About the Agent Prevention Summary pane

The **Agent Prevention Summary** pane lets you view statistics about the agents that generated recent prevention events. The statistics include the agent computer name, action (deny, allow) and the resource type (network, file, registry, overflow, syscall).

The **Agent Prevention Summary** pane is sorted by the descending total number of prevention events for each agent, which causes the agents that generate the most events to be at the top of the list. The length of the bar chart for each agent shows the proportion of the recent events that belong to that agent.

For troubleshooting purposes, you can view additional prevention event details. To view all prevention events generated for an agent, click the agent computer name. To view a summary of all generated prevention events, click the **Summary** link.

About the Network Actions pane

The **Network Actions** pane lets you view statistics about the network activity of the most recent events. These statistics include the IP addresses that appear in recent events, and a bar chart that indicates how the events were handled (deny in/out, allow in/out).

The **Network Actions** pane is sorted by the descending total number of events for each IP address, which causes the IP addresses that generate the most events to be at the top of the list. The length of the bar for each IP address reflects the proportion of the recent events that originated or were sent to the remote address.

For troubleshooting purposes, you can view additional agent details. To view all actions for a remote address, click the remote address link. To view a summary of all actions, click the **Summary** link.

About the Agent Statistics pane

The **Agent Statistics** pane lets you view statistics about agents that support the prevention features of Symantec Critical System Protection.

You can view the following statistics:

Registered agents	Displays statistics for agents in the Prevention view.
Windows agents	Displays statistics for Windows agents.
Solaris agents	Displays statistics for Solaris agents.
Linux agents	Displays statistics for Linux agents.
Offline agents	Displays statistics for agents that are offline.
Unprotected agents	Displays statistics for agents with no protection.

Agents with null policy	Displays statistics for agents with the null prevention policy.
Agents with errors	Displays statistics for agents with errors.
Agents with policy updates	Displays statistics for agents with pending policy updates.
Agents with configuration updates	Displays statistics for agents with pending configuration updates.

About the Quick Links pane

The **Quick Links** pane provides the following links:

Manage Assets	Display the Assets page.
New Prevention Policy	Display the Policies page, and then display the dialog to create a new prevention policy. See "Creating a workspace policy" on page 119.
New Common Config	Display the Configs page, and then display the dialog to create a new common configuration. See "Creating a common configuration" on page 166.
New Prevention Config	Display the Configs page, and then display the dialog to create a new prevention configuration. See "Creating a prevention configuration" on page 166.
View Events	Display the Monitors page.
Run Reports	Display the Reports page.
LiveUpdate	Run LiveUpdate to download and install updates to Symantec Critical System Protection policies and reports. See "About updating Symantec policy and report packs" on page 48.

Using the Home page in the Detection view

The Home page in the Prevention view provides current agent and event statistics for agents that support the detection features of Symantec Critical System Protection.

About the Agent Detection Summary pane

The **Agent Detection Summary** pane lets you view statistics about the agents that generated recent detection events. The statistics include the agent computer name, event type, and the number of events per type.

The **Agent Prevention Summary** pane is sorted by the descending total number of detection events for each agent, which causes the agents that generate the most events to be at the top of the list. The length of the bar chart for each agent shows the proportion of the recent events that belong to that agent.

For troubleshooting purposes, you can view additional event details. To view all detection events generated for an agent, click the agent computer name. To view a summary of all generated detection events, click the **Summary** link.

About the Event Rule Summary pane

The **Event Rule Summary** pane lets you view statistics about recent rules. The statistics include the rule name, event severity, and the number of events per severity.

The **Event Rule Summary** pane is sorted by the descending total number of rules, which causes the rules with the highest counts to be at the top of the list. The length of the bar for each rule reflects the proportion of the recent events that belong to that rule.

For troubleshooting purposes, you can view additional rule details. To view counts for a rule, click the rule link. To view a summary of all rules, click the **Summary** link.

About the Agent Statistics pane

The **Agent Statistics** pane lets you view statistics about agents that support the detection features of Symantec Critical System Protection.

You can view the following statistics:

Registered agents	Displays statistics for agents in the Detection view.
Windows agents	Displays statistics for Windows agents.
Solaris agents	Displays statistics for Solaris agents.
Linux agents	Displays statistics for Linux agents.
AIX agents	Displays statistics for AIX agents.
HP-UX agents	Displays statistics for HP-UX agents.

Tru64 agents	Displays statistics for Tru64 agents.
Offline agents	Displays statistics for agents that are offline.
Agents with no policy	Displays statistics for agents with no detection policy.
Agents with errors	Displays statistics for agents with errors.
Agents with policy updates	Displays statistics for agents with pending policy updates.
Agents with configuration updates	Displays statistics for agents with pending configuration updates.

About the Quick Links pane

The **Quick Links** pane provides the following links:

Manage Assets	Display the Assets page.
New Detection Policy	Display the Policies page, and then display the dialog to create a new detection policy. See "Creating a workspace policy" on page 119.
New Common Config	Display the Configs page, and then display the dialog to create a new common configuration. See "Creating a common configuration" on page 166.
New Detection Config	Display the Configs page, and then display the dialog to create a new detection configuration. See "Creating a detection configuration" on page 167.
View Events	Display the Monitors page.
Run Reports	Display the Reports page.
LiveUpdate	Run LiveUpdate to download and install updates to Symantec Critical System Protection policies and reports. See "About updating Symantec policy and report packs" on page 48.

Chapter 3

Managing assets

This chapter includes the following topics:

About assets

Assets are the computers on which agents are installed. Agents are the software that you install on the computers that you want to protect. In most cases, the terms are used synonymously.

Symantec Critical System Protection agents support prevention and detection features. Agents that support prevention features 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. However, the email application can still read and write to the directories that it needs to access.

Agents that support detection features control behavior by detecting suspicious activity and taking action. For example, a Symantec Critical System Protection detection policy can take action when it detects an attempt by an unauthorized user to gain illegitimate access to a system. No action would be taken for failed attempts that resulted from normal behavior such as an expired password or a user forgetting a password.

An agent is compatible with a policy if the following is true:

- The agent and the policy have the same operating system.
- The agent's version is greater than or equal to the policy's minimum agent version.
- The agent supports the policy type.

Viewing the Assets page

You use the Assets page in the management console to apply policies and configurations to agents, and to monitor the health of your agents.

You can do the following activities from the Assets page:

- Determine how agents communicate with the management server, and which events agents send to the management server.
- View information about the agents in your network, including which policies are enforced on agents, and how the agents are configured.
- View a list of agents that run on Windows, Solaris, Linux, AIX, and HP-UX operating systems.
- Apply policies and configurations to agents and groups.
- Delete an agent's record from the management server database.

To view the Assets page

1. In the management console, click **Assets**.
2. (Optional) On the Assets page, click the size arrows to expand or collapse the panes.

About asset search

Symantec Critical System Protection includes a search function that lets you perform a search for the assets. You can use the search box or **Advanced Search** link in the console to search for the assets. The search results contain details about the asset in the **Asset Search** pane such as software version, IP address, group, history, and so on. You can select an asset and perform several actions on it. For example, you can clear the configurations that are applied to an agent, rename an agent, add an agent to a specific group, and so on.

You can also export the search results to a comma-separated value file.

You can use a combination of search filters for quick search of assets. These search filters appear in the **Asset Search** dialog box.

Table 3-1 Available asset search filters

Filters	Description
Source Machine	Search agents by agent name, host name, or IP address.
Version	Search agents based on their version.
Domain Name	Search agents based on their domain name.
OS Type	Search agents based on their operating system type.
OS Version	Search agents based on their operating system version.
Health	Search agents based on their health status, such as green, yellow, or red.
Has Pending Changes?	Search agents that are flagged for pending policy or config changes.
Has errors?	Search agents that have policy or config errors.
Has a Prevention Policy directly assigned?	Search agents that have a directly assigned prevention policy.

Table 3-1 Available asset search filters *(continued)*

Filters	Description
Has Prevention enabled?	Search agents with prevention enabled.
Has a Detection Policy directly assigned?	Search agents that have a directly assigned detection policy.
Has a Common Config directly assigned?	Search agents that have a directly assigned common config.
Has a Prevention Config directly assigned?	Search agents that have a directly assigned prevention config.
Has a Detection Config directly assigned?	Search agents that have a directly assigned detection config.

See "Searching assets by attributes" on page 72.

Searching assets by attributes

You can use the **Asset Search** window to search assets based on their attributes, such as agent name, IP address, domain name. Symantec Critical System Protection provides several search filters that you can use to optimize your search result.

Table 3-2 Search actions

Action	Description
Double-click	Open the agent **Properties** dialog box. See "Viewing agent properties" on page 89.
Properties	List the attributes of an agent in the Agent **Properties** dialog box. See "Viewing agent properties" on page 89.
Rename	Modify the name of an agent. See "Modifying an agent name" on page 106.
Move To	Move an agent to a group.
Move Back	Move an agent back to its previous group.

Table 3-2 Search actions *(continued)*

Action	Description
Delete	Delete an agent. See "Deleting an agent" on page 112.
Edit Policy	Edit an existing policy applied to an agent. See "Editing a policy applied to an agent or group" on page 109.
Apply Policy	Apply a policy to an agent. See "Applying a policy to an agent or policy group" on page 106.
Clear Policy	Clear a policy applied to an agent. See "Clearing a policy applied to an agent or group" on page 110.
Save Applied Policy	Save an applied policy as a workspace policy on an agent. See "Saving a policy applied to an agent or group" on page 109.
View Config	View the configuration applied to an agent. See "Viewing agent properties" on page 89.
Apply Config	Apply a configuration to an agent. See "Applying the Symantec policies to agents or groups" on page 42.
Clear Config	Clear a configuration applied to an agent. See "Clearing a configuration applied to an agent or group" on page 111.
Add To	Add an agent to a group. You can add an agent in a group when you are in the **Detection** view.

To search assets by attributes

1. In the management console, click **Assets**.
2. On top-right, in the search text box, type an agent name, a host name, or an IP address.

   You can also use wildcards in the search string.

   When you click the **Advanced Search** link, all of the search filters in the **Asset Search** window appear blank.
3. Click the search icon or press **Enter**.

4. In the **Asset search** window, specify the search filters.

5. Click **Search**.

   On the right-hand pane, the search result appears in the **Asset Search** table. You can select the required agent and perform the following actions in Table 3-2.

See “About asset search” on page 71.

About console views, agents, and groups

When an agent first registers with the management server, it tells the server whether it supports prevention features, detection features, or both. The agent is placed in a default group in each console view that it supports, unless a group was assigned during agent installation.

Each console view lets you create agent groups in different ways. Each view has its own rules about policy and configuration assignment to agents, and lets you perform specific actions.

Using the Network view

You use the Network view to monitor your entire agent deployment. You can do the following activities in the Network view:

- List all agents that are registered with the management server.
- View the overall status of each agent in your network.
- View a list of the policies and configurations that are applied to each agent.
- Organize agents in a hierarchy of groups.
- Register virtual agents that indirectly detect off-platform event data and associate the data with agents in the management console.
- Delete an agent's record from the management server database.

Note: You cannot change agent policy or configuration in the Network view.

Agent groups

In the Network view, you organize agents in a hierarchy of groups. You might use groups to reflect your organization's geographical or divisional structure. Every agent lives in exactly one Network view group. You can create as many groups as you need. You can nest agent groups within each other.

The default Master group is named Network. When an agent registers with the management server, it is automatically placed in the Network group.

Note: The Network view group hierarchy does not affect agent configuration.

Using the Prevention view

You use the Prevention view to apply policies and configurations to agents that support the prevention features of Symantec Critical System Protection.

You can do the following activities in the Prevention view:

- List all agents that support prevention features.
- List all virtual agents.
- View the overall status of each agent.
- View policy and agent configuration.
- Organize agents in a hierarchy of groups.
- Apply prevention policies to agents and policy groups.
- Apply prevention configurations to agents and configuration groups.

In the Prevention view, you can create the following types of agent groups:

- Policy groups
- Configuration groups

Prevention policy groups

You apply prevention policies to policy groups. Policy groups contain one or more agents that support prevention features. Policy groups are organized in a hierarchy of groups.

You might use prevention policy groups for the following reasons:

- The agents use the same policy. You can apply the policy once to the policy group.
- Your network consists of different operating systems. You can have separate policy groups for your Windows, Linux, and Solaris computers.

In the Prevention view, each agent resides in exactly one policy group. The default policy group is named Policy. When an agent that supports prevention features registers with the management server, it is automatically placed in the default Policy group unless a group was assigned during agent installation.

You can group agents in any logical manner that reflects the structure of your network. You can create as many policy groups as you need. You can nest policy groups within each other. When you need to update your agents, you can apply a single policy to the entire policy group, rather than individually to each agent.

How prevention policies are applied to agents

Symantec Critical System Protection applies prevention policies to agents based on the following rules:

- Upon initial Symantec Critical System Protection agent installation, the Null prevention policy is applied to an agent when it registers with the management server.
- An agent uses exactly one prevention policy. For example, if an agent has a prevention policy applied directly to it, and the agent's policy group has a prevention policy applied to it, only one of the prevention policies is used. The two prevention policies are not combined and then applied to the agent.
- An agent uses the closest policy as you move up the agent group tree. If an agent has a prevention policy applied directly to it, then the agent uses that policy, since the agent's policy is closer in the group tree than the agent's group policy.
- Policies that are incompatible with an agent are ignored. For example, consider when a Windows agent and a Solaris agent are in the same policy group. The policy group has a Solaris policy applied to it and the policy group's parent group has a Windows policy applied to it. The Solaris agent uses its group's policy since it is compatible. The Windows agent, however, skips its group's policy and uses the policy of its group's parent, which is compatible.
- Since a policy group can have multiple policies assigned to it, it is possible to have more than one policy that is compatible with an agent. In this case, Symantec Critical System Protection chooses the most compatible policy, based on the minimum agent version of the policy. The policy with the highest minimum agent version is used.

You apply a policy to an agent directly or through a policy group. When you apply or make changes to a policy from a policy group, the management server determines which agents in that group use the group's policy, and then flags those agents for pending policy updates.

Prevention configuration groups

You apply prevention configurations to configuration groups. Configuration groups contain one or more agents that support prevention features. Configuration groups are organized in a hierarchy of groups.

You might use prevention configuration groups for the following reasons:

- The agents have the same prevention configuration. You can configure the settings once on the group rather than individually for each agent.
- You can manage many configurations. You can organize the configurations in groups so that you can update your agents' configuration settings efficiently.

The default prevention configuration group is named Configuration. When an agent that supports prevention features registers with the management server, it is automatically placed in the default Configuration group unless a group was assigned during agent installation.

How prevention configurations are applied to agents

Symantec Critical System Protection applies prevention configurations to agents based on the following rules:

- Upon initial Symantec Critical System Protection agent installation, the default common parameters and default prevention parameters are applied to an agent when it registers with the management server.
- An agent that supports prevention features uses common parameters and prevention parameters.
- An agent can get its prevention configuration from itself or from a prevention configuration group.
- An agent resides in exactly one prevention configuration group.
- If you apply a prevention configuration to an agent that already has a prevention configuration, then the new prevention configuration replaces the old prevention configuration.

You can configure agents directly or through a prevention configuration group. When you configure agents through a group, the management server determines which agents in the group use the group's configuration, and then flags those agents for pending configuration updates.

Common configuration groups

The common configuration groups are available in the Prevention view.

Enabling or disabling the state of the prevention feature

The Symantec Critical System Protection agent installation kit includes an Enable Intrusion Prevention installation option. When this 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 installation 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.

If intrusion prevention was disabled during Symantec Critical System Protection agent installation, you should note the following:

- All agents that support the intrusion prevention feature appear in the Prevention view. On the **Assets** page, an icon indicates whether the feature is currently enabled.
- You can make policy and configuration changes to all agents, even those agents for which the prevention feature is disabled.
- Agents with the intrusion prevention feature disabled request and process prevention and common configuration changes, but not prevention policy changes. Any prevention policy updates remain pending until the prevention feature is enabled on the agents.

If intrusion prevention was disabled during agent installation and you want to enable it, you must log on to the agent computer, run the agent config tool, and then restart the agent computer. The -I switch in the agent config tool toggles the state of the intrusion prevention feature between enabled and disabled.

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

To enable or disable the state of the prevention feature

1. Log on to the agent computer.
2. Navigate to the agent config tool directory.
3. At a command prompt, type `sisipsconfig -I` (Windows)

   Or

   `sisipsconfig.sh -I` (UNIX), and then press **Enter**.

Using the Detection view

You use the Detection view to apply policies and configurations to agents that support the detection features of Symantec Critical System Protection.

You can do the following activities in the Detection view:

- List agents that support detection features
- View the overall status of each agent
- View policy and agent configuration
- Organize agents in policy domains and policy groups
- Organize agents in configuration groups
- Apply policies to agents and agent groups
- Apply configurations to agents and agent groups
- Delete agents from detection policy groups

In the Detection view, you can create the following types of agent groups:

- Policy groups
- Configuration groups

Detection policy domains

You organize agents and policy groups in a hierarchy of policy domains. The default policy domain is named Policy.

You might use policy domains to manage many customers. You can build a customer domain hierarchy, with one customer per domain and multiple policy groups under each domain.

When using domains, please note the following:

- You can create domains within domains. You cannot create domains within groups.
- You can nest domains. Domains can contain other domains, groups, or agents; any combination is permitted.
- Groups can only reside in domains.
- Every agent must reside in at least one group or domain in the detection policy tree. Agents can reside in multiple domains. Agents can reside in domains and groups simultaneously.
- You can delete an agent from a domain (or a group) as long as the domain (or group) is not the last instance of the agent in the tree. The last instance cannot be deleted.
- You cannot delete the default Policy domain.
- You can move agents between domains, between groups, and between domains and groups. You cannot move groups between domains. You cannot move domains between domains.

- You cannot apply policies to domains.

Detection policy groups

You apply detection policies to policy groups. Policy groups contain one or more agents that support detection features. Policy groups are organized in a hierarchy of domains and groups.

During server installation, the following default OS-specific policy groups are created in the default Policy domain:

- AIX
- HP-UX
- Linux
- Solaris
- Tru64 UNIX
- Windows

You might use policy groups for the following reasons:

- The agents use the same policy. You can apply the policy once to the policy group rather than individually to each agent.
- Your network may contain agents that are installed on different operating systems. You can have separate policy groups based on the operating system type.

When an agent that supports detection features registers with the management server, it is automatically placed in the default OS-specific policy group in the default Policy domain, unless a group was assigned during agent installation. If any detection policies are applied to any of the OS-specific policy groups, these policies are automatically applied to the agent when the agent registers.

How detection policies are applied to agents

Symantec Critical System Protection applies detection policies to agents based on the following rules:

- An agent can reside in multiple detection policy groups. If an agent resides in more than one policy group, it gets the combination of all detection policies applied to all the groups in which it resides.
- Every agent must reside in at least one group or domain in the detection policy tree.

- An agent can be deleted from a domain (or a group) as long as the domain (or group) is not the last instance of the agent in the tree. The last instance cannot be deleted.
- You can apply multiple policies to a policy group. If multiple policies are applied to a group, the agents in that group get the combination of all detection policies applied to the group.
- You cannot apply policies to domains.
- An agent can have none, one, or many detection policies applied to it. If an agent has no policies applied to it, the agent does not log any detection events.
- Upon initial Symantec Critical System Protection agent installation, any detection policies applied to the OS-specific policy groups are automatically applied to an agent.

Since you can apply multiple detection policies to an agent, you can apply conflicting policies to an agent. Symantec Critical System Protection resolves policy conflicts based on the following rules:

- If one policy enables a rule, and another policy disables the same rule, then the rule is enabled on the agent. For example, suppose a policy that is applied to a group explicitly enables the record successful logon rule, and another policy that is applied to the same group explicitly disables the same rule. If an agent is placed in both groups, then the record successful logon rule is enabled for the agent.
- If a parameter list has different contents in different policies, then the agent is sent the combined parameter list from the policies. For example, suppose a policy applied to a group lists File A and File B in the watch for file creation rule, and a policy applied to another group lists File 1 and File 2 in the same rule. If an agent is placed on both groups, then the agent receives a watch for file creation list of File A, File B, File 1, and File 2.

Detection configuration groups

You apply detection configurations to configuration groups. Configuration groups contain one or more agents that support detection features. Configuration groups are organized in a hierarchy of groups.

You might use configuration groups for the following reasons:

- The agents have the same configuration. You can configure these settings once on the group rather than individually for each agent.
- You manage many configurations. You can organize the configurations in groups so that you can update your agents' configuration settings efficiently.

The default detection configuration group is named Configuration. When an agent that supports detection features registers with the management server, it is automatically placed in the default Configuration group unless a group was assigned during agent installation.

How detection configurations are applied to agents

Symantec Critical System Protection applies detection configurations to agents based on the following rules:

- An agent that supports detection features uses common parameters and detection parameters.
- An agent can get its detection configuration from itself or from a detection configuration group.
- An agent resides in exactly one detection configuration group.
- If you apply a detection configuration to an agent that already has a detection configuration, then the new detection configuration replaces the old detection configuration.
- Upon initial Symantec Critical System Protection agent installation, the default common parameters and default detection parameters are applied to an agent when it registers with the management server.

Common configuration groups

The common configuration groups are available in the Detection view.

About common configuration groups

You apply common configurations to common configuration groups. Common configuration groups contain one or more agents that are registered with the management server.

Symantec Critical System Protection applies common configurations to agents based on the following rules:

- All agents uses common configurations.
- An agent can get its common configuration from itself or from a common configuration group.
- An agent resides in exactly one common configuration group.
- If you apply a common configuration to an agent that already has a common configuration, then the new common configuration replaces the old common configuration.

Common configuration groups are organized in a hierarchy of groups. The default common configuration group is named Common Configuration. When an agent registers with the management server, it is automatically placed in the default Common Configuration group unless a group was assigned during agent installation.

The common configuration groups are available in the Prevention view and Detection view. Changes made in one view are automatically reflected in the other view.

Viewing agents registered with the management server

You use the Network view to view all agents that are registered with the management server. You can determine how well your computer is protected by monitoring and analyzing this information.

Upon initial installation, the following occurs:

- All agents are assigned to the Network group, in the Network view.
- The SCSP Manager, which collects all server-related events, is assigned to the Virtual Agents folder.
  See "About the SCSP Manager virtual agent" on page 87.

To view all agents registered with the management server

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Network**.

3 On the Network page, in the **Network Assets** pane, click **Network** to list all agents that are registered with the management server.

4 (Optional) To expand or restrict the list of agents, select one of the following filters:

All Nodes	Filter that displays all the agents.
Windows Nodes	Filter that displays the agents that run a Windows operating system.
Solaris Nodes	Filter that displays the agents that run a Solaris operating system.
Linux Nodes	Filter that displays the agents that run a Linux operating system.
AIX Nodes	Filter that displays the agents that run an AIX operating system. Applies to agents that support detection features.
HP-UX Nodes	Filter that displays the agents that run an HP-UX operating system. Applies to agents that support detection features.
Tru64 Nodes	Filter that displays the agents that run Tru64 operating system. Applies to agents that support detection features.

About the management server health

In the management console menu bar, the overall health of the connection between the management server and the database is indicated by one of the following icons:

- A green circle icon indicates that the management server is running.
- A red circle icon indicates that a management server or database error occurred.

About the agent pane

The agent pane lists the agents in a policy or configuration group. The agent pane is located on the right side of the Assets page. The bottom half of the agent pane lists details about a selected agent.

The agent pane comprises columns of information about each agent.

Agent Health column

Agent Health is the first column in the agent pane. The Agent Health column indicates whether an agent is in contact with the management server. Place your mouse cursor over the Agent Health column to view a pop-up tool tip.

The Agent Health column displays one of the following icons:

- A green circle icon indicates that an agent is healthy.
- A yellow circle icon indicates that an agent is possibly offline and experiencing minor problems.
- A red circle icon indicates that an agent is offline and experiencing major problems.

See "Configuring agent health timeout settings" on page 94.

Feature State column

Feature State is the second column in the agent pane. The Feature State column appears in the Network view and Prevention view. Each prevention feature supported by the management console has a Feature State column. Place your mouse cursor over the Feature State column to view a pop-up tool tip.

The feature state can change from complete protection to limited or no protection if you do the following:

- Apply the Symantec Critical System Protection Null prevention policy to an agent.
  By default, the Null prevention policy is applied to an agent when it registers with the management server. The Null prevention policy provides no protection.
- Enable the global disable prevention policy option in a Symantec Critical System Protection prevention policy applied to an agent.
  The disable prevention policy option in the prevention policies disables policy prevention for an agent computer. The policy violations are logged by the agent, but are not enforced.
- Override an agent's prevention policy using the policy override tool.
  The policy override tool lets a user temporarily or permanently disable prevention policy enforcement on an agent computer. To use the policy override tool, the prevention policy applied to the agent computer must be configured to allow the user to override prevention policy enforcement. The policy override tool runs on Windows and UNIX operating systems.

The feature state icon shows one of the following states:

- Shield icon: An agent is protected
- Shield icon with red X: An agent has limited or no protection
- Shield icon with blue V: An agent is a virtual agent (Network view only)
- Blue triangle icon: Restart the agent computer

- If the blue triangle icon points up, the prevention feature is disabled, but is enabled after a restart. Restart the agent computer.
- If the blue triangle icon points down, the prevention feature is enabled, but is disabled after a restart. Restart the agent computer. The agent continues to enforce the most recent prevention policy until the restart. To stop enforcement before the restart, apply the Null policy before disabling the prevention feature.
- After installing an agent, if the blue triangle appears next to the agent, stop and then restart the intrusion prevention service (click Start > Settings > Control Panel > Administrative Tools > Services, and then select Symantec Critical System Protection Agent). The blue triangle changes to the shield icon.
- Black circle with diagonal line icon: Prevention feature is completely disabled

Name column

The Name column contains the name of the agent.

The lettering of the agent's name and the appearance of an icon indicate the following:

- Normal lettering: No pending changes or outstanding errors.
- Bold and italic: Pending changes to the agent's configuration or policy assignment that have yet to be received by the management server. When the changes are applied to the agent, the lettering reverts to normal.
- Bold: Pending changes to the agent that were received by the management server, but not applied to the agent. Check the agent's property Status tab for information about the failed action, and decide how to manually solve the problem.
- Flag icon: Changes to the agent's configuration or policy assignment are pending.
- Exclamation icon: An error has occurred.

You can change the name of the agent.

See “Modifying an agent name” on page 106.

IP Address column

The IP Address column contains the IP address of an agent computer.

Policy column

The Policy column contains the name of the prevention policy applied to an agent. You use the Policy column in the Prevention view.

A folder icon after the policy name indicates that an agent gets its policy from a group. To find the group name, move the cursor over the policy cell. You can also determine the group name from the Policy tab in the **Details** pane.

Version column

The Version column contains the version of Symantec Critical System Protection software that is installed on an agent computer.

OS column

The OS column contains the operating system of the computer on which the agent is installed.

Last Contact column

The Last Contact column contains the date and time that the agent last contacted the management server to request policy and configuration updates.

Details pane

The **Details** pane comprises the following tabs:

General tab	Provides a selected agent's host name, software version, operating system, IP address, creation, and modification dates, Deny Logs check box.
Policies tab	Lists the policies applied to a selected agent.
Configs tab	Lists the configurations applied to a selected agent.
Recent Events tab	Lists recent prevention or detection events for a selected agent.
History tab	Lists audit events for a selected agent.

About the SCSP Manager virtual agent

The SCSP Manager virtual agent represents the Symantec Critical System Protection entity (front-end servers and database as a single object). All server-related events (startup and shutdown of front-end servers, alert control events, cleanup, database storage errors, aggregate health change events, etc.) are assigned to the SCSP Manager virtual agent.

Every Symantec Critical System Protection management server has a SCSP Manager virtual agent that was created during installation. SCSP Manager is registered into the Virtual Agents folder in the Network group, in the Network view.

The SCSP Manager virtual agent is configured as follows:

Host name	SCSP Manager
Type	Virtual agent
Agent type	CSP Server Entity
Operating system	Windows
IP Address	127.0.0.1
Health timeouts	The SCSP Manager virtual agent is considered possibly offline (yellow icon) after 10000000 seconds. The SCSP Manager virtual agent is considered offline (red) after 20000000 seconds.
Health attribute	Last event determines the agent health.
Health events	No events are generated when the SCSP Manager virtual agent changes status.

To control user access to the SCSP Manager virtual agent, you can move the virtual agent into a subgroup.

You can use Search Events on the Monitors page to view all server-related events. Server-related events include event types Server Status and Agent Status. Search events using the source computer name (for example, SCSP Manager (Sales-GCPX1C)).

About the management server list

An agent's management server list comprises the primary management server and optional alternate management servers. Alternate management servers are used for 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.

Viewing the management server list

To view an agent's management server list, you use the -view command in the agent config tool.

To view the management server list

1. Log on to the agent computer.
2. Navigate to the agent config tool directory.
3. At a command prompt, type sisipsconfig `-view` (Windows) or `sisipsconfig.sh -view` (UNIX), and then press **Enter**.

Modifying the management server list

You can modify an agent's management server list using the following methods:

CSP_Agent_Diagnostics detection policy

An option in the CSP_Agent_Diagnostics detection policy lets you modify an agent's management server list.

See the *Symantec Critical System Protection Detection Policy Reference Guide* for details.

Agent config tool

On the agent computer, run the agent config tool using the -host command. The -host command sets the IP address or fully qualified host name of the primary management server and optional alternate management servers used by the agent.

In the command line, specify the primary management server, followed by the optional alternate management servers.

On Windows agents, the command is as follows:

```
sisipsconfig -host primary[,alternate1,alternate2,...]
```

On UNIX agents, the command is as follows:

```
sisipsconfig.sh -host primary[,alternate1,alternate2,..
```

Viewing and configuring agent and group properties

Agent and group properties provide an overview of how an agent or group is configured.

Viewing agent properties

Agent properties describe how an agent is configured.

In the management console, the agent properties dialog comprises several tabs of information: General, Details, Contact, Status, Policy, Config, Group, Recent Events, History, and Collector.

The following agent properties appear on the **General** tab, which provides general agent information:

Host Name

The name of the agent host computer.

This name appears in the management console.

Type

The type of host (agent, virtual agent).

Version

The Symantec Critical System Protection agent version.

Operating System

The operating system of the agent computer.

IP Address

The IP address of the agent computer.

Created

The date the agent was created.

Modified

The date the agent was last modified.

Last Contact

The date the agent last polled for configuration changes.

Last Event

The date the agent last sent an event.

Agent Health

The health of the agent, indicated by a colored icon.

Agent health is denoted by the green/yellow/red circle icon in the Agent Health column on the Assets page. A green icon indicates that an agent is healthy. A yellow icon indicates that an agent is possibly experiencing problems. A red icon indicates that an agent is experiencing problems.

See "Configuring agent health timeout settings" on page 94.

Deny Logs

Select the Deny Logs check box to temporarily stop an agent from sending events to the management server.

If an agent is experiencing problems, selecting this check box prevents the agent from flooding the management server database with events. After you resolve the agent problem, clear the Deny Logs check box to resume sending events to the management server.

The Deny Logs option overrides an agent's log rules.

Default: Off

Description

A full description of the agent.

The following agent properties appear on the **Details** tab, which tracks the agent's event file activities:

Service start time

The date the Symantec Critical System Protection communications service/daemon was last started.

If this service is not running, then no communications are possible with the agent.

Last collector update

The date the IDS service/daemon was last started.

If this service is not running, then no new events are produced for transmission to the server. This date is usually within a few seconds of the service start time. If it is not, then problems occurred on the agent that caused the service to restart abnormally.

Agent Uptime

A formatted display of the time difference since the service start time and the current time.

The agent uptime is shown as number of days, hours, minutes, seconds (DDDd HH:MM:SS).

Example: 28d 01:41:12

Agent Age

The age, in days, of the agent.

Timezone offset

The time, in minutes, that the agent local time is offset from Greenwich Mean Time (UTC).

This value can be negative (for agents to the west of GMT) or positive (for agents to the east of GMT). This may be useful to know when choosing a collector host for virtual agents. The collector host should have the same timezone offset as the virtual agent source system.

Note: All system date/time values are handled as Coordinated Universal Time (UTC). Some system date/time values that are shown in the management console are converted to the local time zone. Converted values are shown with the appropriate time zone values.

Character set

The character encoding format used by the agent.

UTF-8 indicates single byte environment. UTF-16 indicates double byte environment.

This may be useful to know when choosing a collector host for virtual agents. The collector host should have the same character encoding as the virtual agent source system.

Last event file

The name of the last bulk event file created on the agent.

Last file's event count

The number of total events stored in the last bulk event file created on the agent.

Total event files

The cumulative number of bulk event files produced on the agent.

Total event count	The cumulative number of events recorded to bulk event files on the agent.
Last uploaded file	The name of the last bulk event file uploaded to the management server.
Last upload's event count	The number of total events stored in the last bulk event file uploaded to the management server.
Total uploaded files	The cumulative number of bulk event files uploaded to the management server.
Total uploaded events	The cumulative number of events recorded to bulk event files that were uploaded to the management server. This figure represents the total number of events potentially available for forensic analysis.

The **Contact** tab provides contact information for the agent. You can modify the contact information.

The Contact tab contains the following information:

Agent priority	The priority (0-99) of the agent.
Contact name	The name of the person or organization responsible for the underlying system that the agent represents.
Telephone numbers	The telephone numbers associated with the contact name.
Email address	The email address for the contact name.
Location	The physical or logical address where the system resides.
Business Information	Additional business context information about the agent. This may include user-defined keywords or phrases for query and reference purposes. For example, the keywords may refer to business functions (such as Payroll, Sales, Development), regulatory issues (such as HIPAA, SOX, GLBA), or application usage (such as Database, Email, Web).

The following agent properties appear on the **Status** tab, which provides the status of pending policy and configuration updates for the agent:

Policy and configuration status for the agent	Provides the status of pending policy and configuration updates for an agent.
Error Messages	Error messages associated with the agent.

The following agent properties appear on the **Policy** tab, which lists the policies applied to the agent or policy group:

Prevention Policies	The prevention policies applied to the agent or policy group.
Detection Policies	The detection policies applied to the agent or policy group.

The following agent properties appear on the Config tab, which lists the configurations applied to the agent or configuration group:

Prevention Configs	The prevention configurations applied to the agent or configuration group.
Detection Configs	The detection configurations applied to the agent or configuration group.

The following agent properties appear on the **Group** tab, which lists the groups in which the agent resides:

Netwok Group	The Network view groups in which the agent resides.
Prevention Groups	The Prevention view groups in which the agent resides.
Detection Groups	The Detection view groups in which the agent resides.
Common Config Group	The common configuration group in which the agent resides.

The following agent properties appear on the **Recent Events** tab, which lists recent events for the agent:

Source Machine	The source machine that generated the event.
Date	The event date.
Event Type	The event type.
Severity	The event severity level.

Description	A description of the event.

The following agent properties appear on the **History** tab, which lists audit events for the agent:

Date	The event date.
User	The user that generated the event.
Operation	The operation that generated the event.
Description	A description of the event.
Source Machine	The source machine that generated the event.

The **Collector** tab lists the Symantec Critical System Protection agent that most recently collected a virtual event for a virtual agent.

See “About virtual agents” on page 98.

To view agent properties

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent, and then right-click **Properties**.
4. In the properties dialog box, view or edit the agent properties.
5. Click **OK**.

Configuring agent health timeout settings

Agent health timeout settings provide control over agent health conditions and change-of-status event generation.

Configured independently of the polling interval, agent health is denoted by the green, yellow, or red circle icon in the Agent Health column on the Assets page. A green icon indicates that an agent is online. A yellow icon indicates that an agent is possibly offline. A red icon indicates that an agent is offline. Separate yellow and red default values are provided for native and virtual agents.

The color of the agent health icon is determined using the following rules:

- Agent health is set to green when the last contact time or the last event time plus the yellow interval seconds is greater than the current time.
- Agent health is set to yellow when the last contact time or the last event time plus the yellow interval seconds is less than the current time and the last

contact time or the last event time plus the red interval seconds is greater than the current time.

- Agent health is set to red when the last contact time or the last event time plus the red interval seconds is less than the current time.

Status change events are optionally generated when the agent health icon changes color. These real-time events are available for viewing using real-time monitors or alerts.

The agent health timeout settings are as follows:

Agent is Possibly Offline after [n] seconds (min. 30)	The number of elapsed seconds before the agent health icon turns yellow. Default for native agents: 900 The default value for native agents is 2 times the normal polling interval of 5 minutes. This provides enough time for agents to check on a busy system or to accommodate temporary connectivity issues. If the agent health icon skips from green to red, set the yellow interval equal to the red interval. If the agent health icon is perpetually green, set a very large number for the yellow and red intervals. Default for virtual agents: 172800 The default value for virtual agents represents a 4-hour interval for a virtual agent to generate an expected event.
Agent is Offline after [n] seconds (larger than above)	The number of elapsed seconds when the agent health icon turns red. Default for native agents: 3000 The default value for native agents represents 30 minutes for an agent's health to turn red (offline). The minimum red interval must be equal to or greater than the yellow interval. Default for virtual agents: 604800 The default value for virtual agents represents 12 hours for an event to appear from a virtual agent before turning red.

Last Event or Last Contact	Select which attribute determines agent health: ■ Last Event: The last time the agent sent an event. ■ Last Contact: The last time the agent polled for configuration changes. Default: Last Contact Agent health is computed using Last Contact unless the agent is configured to use Last Event. Virtual agents use Last Event, since they do not poll for configuration changes.
Generate events when this agent becomes green	Select this check box to generate a status change event when the agent goes from offline status to online status. Default: Off (no event is generated)
Generate events when this agent becomes yellow	Select this check box to generate a status change event when the agent goes to possibly offline status. Default: Off (no event is generated)
Generate events when this agent becomes red	Select this check box to generate a status change event when the agent goes to offline status. Default: Off (no event is generated)

To prevent network flooding as agents go offline and then online, a system-wide flood-control option aggregates status change events into a single event.

See "About the Agent Health setting" on page 250.

You can configure agent health settings for a single agent or many agents. The changes are applied to all selected agents.

To configure agent health timeout settings for an agent

1. In the management console, click **Assets**.
2. On the Assets page, select an agent, and then right-click **Properties**.

   To configure many agents, press and hold the Shift or Ctrl key while selecting the agents, and then right-click **Properties**. Click the **Health** tab, and then continue with step 4.
3. In the agent properties dialog box, on the General tab, click **Configure Heath**.
4. In the **Agent Health Settings** dialog box, edit the agent health timeout settings.
5. Click **OK**.

Viewing group properties

Group properties describe how a group is configured. You can view group properties to determine which policies and configurations are applied to a group.

Group properties are as follows:

General tab	Provides group name, group tree path, date group was created, date group was last modified.
Policy tab	Lists the policies applied to a policy group.
Configuration tab	Lists the configurations applied to a configuration group.
Security tab	Lists the roles that have access to a group.
Recent Events tab	Lists recent events for a group.
History tab	Lists audit events for a group.

To view group properties

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**
3. On the Assets page, select a policy or configuration group, and then right-click **Properties**.
4. In the properties dialog box, view the group properties.
5. Click **Cancel**.

Creating a policy domain

You can create domains within domains. You cannot create domains within groups.

To create a policy domain

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Detection**.
3. On the Assets page, select the default Policy domain or another domain, and then right-click **New Domain**.

   A new domain is created with the name New Domain.

Creating an agent group

Create agent groups so that you can update your agents' policy and configuration settings efficiently. Name agent groups so that you can easily identify which agents to apply to the group.

To create an agent group

1. In the management console, click **Assets**.
2. If you are creating a detection policy group, select a domain,
3. On the Assets page, select the default group or another group, and then right-click **New**.

   A new agent group is created with the New Group.
4. Type the name of the agent group, and then press **Enter**.

About virtual agents

Symantec Critical System Protection virtual agents indirectly detect off-platform event data and associate the data with agents in the management console. Virtual agents provide the appearance of deployed agents reporting events from endpoint systems where Symantec Critical System Protection is not directly installed or managed.

Virtual agents greatly expand event collection beyond the traditional Symantec Critical System Protection endpoint systems.

Using virtual agents, you can do the following:

- Capture event data from legacy systems (such as Symantec Intruder Alert) and represent those agents and events in the management console
- Forward events from multiple Symantec Critical System Protection managers into a common manager and console that can display events from agents in your entire deployed environment
- Handle forwarded operating system event data (such as syslog and Windows event log) as individual source system events
- Capture event data from a variety of platforms (such as mainframe, Windows 98, AS 400, Mac OS) that Symantec Critical System Protection does not support with an agent kit

Symantec Critical System Protection recognizes and processes virtual agent event data that is derived from syslog and Windows event log.

Symantec Critical System Protection also recognizes and processes virtual agent event data via policy rules. Detection policies let you designate resulting events as originating from virtual agents. Similar to specifying a user-defined text string, you can identify a source system identification tag that indicates the events are from an agent other than the host machine that processed the events.

Virtual agents can be dynamically registered as part of the event flow and manually registered in the management console.

Virtual agents behave like native agents from an event visibility and object management standpoint.

Virtual agents do not accept policies or configurations.

There is no direct relationship between a virtual agent and the native agents that act as collection hosts. The virtual agent mapping is derived from the event data trail.

About agent properties and console behavior

With a few exceptions, you manipulate virtual agents in the Network view and throughout the console like native agents. You can move agents among groups, delete agents, display and edit agent properties, and view recent events and audit history events. All relevant console functions within the Home page, Assets page, Monitors page, Reports page, and Alerts page operate as if you were interacting with a native agent.

The following agent properties pertain specifically to virtual agents:

Agent health settings

A virtual agent's health is based on the last time the agent sent an event.

See General tab > Configure Health button > Health Attribute > Last Event.

You can use this information to configure when the agent health icons turn yellow and red. For example, if a virtual agent typically generates an event every four hours, then this may be an appropriate timeout value to use to cause an agent health status change when no event is received during that period.

See "Configuring agent health timeout settings" on page 94.

Collector tab

The Collector tab lists the Symantec Critical System Protection agent that most recently collected an event for a virtual agent.

The View button on the Collector tab lets you view agent properties for the collector agent. This is particularly useful when the virtual agent is offline and you want to determine if the collector agent is itself offline.

Deny Logs setting

Virtual agent properties include the Deny Logs setting. When enabled, this setting temporarily stops a virtual agent from sending events to the management server.

The following console behavior pertains specifically to virtual agents:

Home page

The Home page contains reporting statistics for virtual agent-related counts, including registered virtual agent count and offline virtual agent count.

Assets page

The feature state icon shows virtual agents with the Shield icon and a blue V.

Monitors page

The Event Details window includes additional attribute information for virtual events. These virtual events include a description of the source agent type (ITA forwarded, CSP forwarded, OS forwarded, external system/object) and details about the collection agent.

You can use the virtual agent type to configure filters for real-time monitors and event searches.

Reports page

A stock query displays all collection hosts for virtual agents based on the event trail.

You can use the virtual agent type to configure filters for queries.

Alerts page

You can use the virtual agent type to configure filters for alerts.

About virtual agent types

Every virtual agent is assigned a virtual agent type. The virtual agent type reflects the source environment that originally collected the event data.

See “About event sources” on page 174.

The predefined virtual agent types are as follows:

ITA

Agents whose source events were collected via Symantec Intruder Alert.

CSP Forwarded Agent

Agents whose source events were collected by a Symantec Critical System Protection agent that was controlled and managed by another Symantec Critical System Protection manager.

Derived

Agents whose sources events originated from a system other than the system on which the Symantec Critical System Protection agent resides.

Typical examples include OS forwarded syslog or Windows event logs.

External	Agents whose source events originated from a system or object completely external and unknown to Symantec Critical System Protection. These virtual agents may represent a system (such as a Mainframe), a device (such as a printer), an object (such as a database or user) or even abstract concepts (such as applications, rule names, categories, actions).
CSP Native	Native agents running Symantec Critical System Protection agent on the local machine. This is the default agent type that is used when a Symantec Critical System Protection agent registers with the management server.
CSP Server Entity	The virtual agent associated with every Symantec Critical System Protection management environment. See “About the SCSP Manager virtual agent” on page 87.

About collector hosts

Symantec Critical System Protection agents act as collector hosts for virtual agents. Collector hosts capture virtual events and represent those virtual agents and events in the management console.

The following information may be useful when choosing the Symantec Critical System Protection agents that act as collector hosts:

- The collector host should have the same timezone offset as the virtual agent source system being monitored.
  In the agent properties, the timezone offset is the time, in minutes, that the agent local time is offset from GMT (UTC). This value can be negative (for agents to the west of GMT) or positive (for agents to the east of GMT).
- The collector host should have the same character encoding as the virtual agent source system being monitored.
  The character set is the character encoding format used by the Symantec Critical System Protection agent. UTF-8 indicates single byte environment, UTF-16 indicates double byte environment.

You must configure the Symantec Critical System Protection agents that act as collector hosts to do the following:

- Transmit virtual events to the management server
  You must configure agent log rules to transmit virtual events to the management server.
  You can configure agent log rules based on the virtual tag. A virtual tag identifies the source system or abstract object where a virtual event originated.

It can be a text string (such as Mainframe01) or a variable (such as {VIRTUAL_TAG}).

- Bulk log virtual events
  If the virtual agent system-wide settings are configured to bulk log virtual events, you must enable bulk logging on the agent.
  See "Configuring Virtual Agent settings" on page 103.

About virtual agents and log rules

You can configure agent log rules based on the following event variables:

- System State
- Virtual Agent/Tag

For example, you can bulk log all virtual agent events for Mainframe01 using a wildcard character match on Virtual Agent/Tag.

You can transmit all virtual events as real-time console events by matching System State equal to V.

See "About the System State event flag" on page 178.

About virtual events and bulk logging

The bulk log transfer feature in Symantec Critical System Protection supports virtual agents. Virtual bulk log files are generated for every virtual agent represented by event data.

The main event file is separated into component host files, as follows:

- An event file is produced for the native collector host.
- An event file is produced for each virtual agent that is identified in the event stream.

For example, suppose an agent rotates its event logs daily, and the current event log file contains events for the local host and four virtual agents. Upon log rollover, the agent produces five bulk log files, each labeled according to the source system identifier. Bulk log processing occurs five times; each compressed log file is moved to the upload directory for transmission to the management server.

Virtual bulk files use the general bulk file naming convention, as follows:

YYYYMMDD_HHMMSS_QQQQ-FT_HOSTNAME

Virtual bulk files use file type V (virtual) and OS type O (other).

For example:

- 20070413_170421_001-VO_Mainframe01

- 20070407_131415_456-VO_192.168.12.25

Configuring Virtual Agent settings

The Virtual Agent settings on the Admin page control the storage of virtual events and the dynamic registration of virtual agents.

See "About the Virtual Agent settings" on page 249.

Virtual agents can be dynamically registered as part of the event flow and manually registered in the management console. Manual registration gives you complete control over the definition of a virtual agent. With manual registration, you explicitly set all the registration information for an agent, as well as place the agent into the desired Network view group.

Dynamic registration saves time when registering large numbers of agents. With dynamic registration, agents are automatically registered as part of the event flow and placed into the appropriate Master group and Manager subgroups.

Dynamically registered agents are placed into the following Master groups:

- Agents whose source events were collected via Symantec Intruder Alert or Symantec Critical System Protection appear in a Master group named ITA Forwarded and CSP Forwarded, respectively.
- Agents whose source events originated from a system other than the system on which the Symantec Critical System Protection agent resides (for example, forwarded syslog or Windows event logs) appear in the appropriate OS Forwarded Master group.
- Agents whose source events originated from an external system or object appear in the appropriate External group.

Manually registering a virtual agent

During manual registration, you explicitly set all of the registration information for an agent, and place the agent into the desired Network view group.

Make sure you configure the system-wide setting that controls virtual agent registration and virtual event storage.

See "Configuring Virtual Agent settings" on page 103.

Make sure you configure log rules for the Symantec Critical System Protection agents that act as collector hosts.

See "About collector hosts" on page 101.

To manually register a virtual agent

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Network**.
3. In **Network Assets** pane , select **Virtual Agents** folder, and then right-click **New Virtual Agent**.

4 In the **New Virtual Agent** dialog box, configure the agent properties, and then click **Next**.

Name

A name for the virtual agent.

The name appears in the management console. The name is intended but not required to be a unique name among all virtual agents.

Required.

Agent Type

Select or enter the virtual agent type.

The virtual agent type reflects the source environment that originally collected the event data.

See “About virtual agent types” on page 100.

Required

Host Name

The name of the source machine or system that originally processed the virtual events.

The host name is not considered unique.

Optional

IP Address

The address of the source machine or system that originally processed the virtual events.

This IP address is not considered unique.

Optional

Default: Local host IP address

Manager Name

A name for the aggregation or consolidation point for the virtual agent.

Example: For ITA or CSP forwarded environments, the manager name is the server name.

The manager name is not considered unique.

Note: For ITA forwarded events, the IP Address plus the Manager Name uniquely represent an agent within the ITA universe.

Optional

5 In the **New Virtual Agent** dialog box, configure the display properties, and then click **Finish**.

Operating System	The operating system of the source machine or system that originally processed the virtual events.
Description	A description of the virtual agent.

Modifying an agent name

When modifying the agent name, please note the following:

- An agent name must be between 1 and 128 characters in length.
- By default, the agent name is the host name of the agent computer. If you use the default agent name, and the host name changes, the agent name will also change.
- You can modify the agent name via the Name column on the Assets page (see the following procedure) or the **General** tab in agent properties.
  See "Viewing agent properties" on page 89.
- The agent name extends throughout the management console.
- Duplicate agent names (and host names) can occur.

To modify an agent name

1 In the management console, click **Assets**.

2 On the Assets page, select an agent, and then right-click **Rename**.

3 On the Assets page, in the Name column, type the new agent name, and then press **Enter**.

Applying a policy to an agent or policy group

You apply a policy to an agent directly or through a policy group. When you apply a policy to a policy group, the management server determines which agents in that group use the group's policy and then flags those agents for pending policy updates.

You should consider the following information before applying policies to agents:

- The **Set Policy Wizard** shows the policies that match the agent's operating system type and have a minimum agent version equal to or lower than the agent's version.

- The **Set Policy Wizard** also shows UNIX policies. You can apply UNIX policies to any non-Windows agent. When a UNIX prevention policy is applied to a group with an OS-specific policy, the agent uses the OS-specific policy unless the UNIX policy uses a higher minimum agent version.
- Review the policy option settings before applying a policy.
- Checking the Disable Prevention box in the Set Policy Wizard automatically checks the global Disable Prevention option in the policy option tree.
- When applying a new policy, apply it to a small set of agents and then verify that the agent computers are functioning properly with the applied policy.
- In the Detection view, you can apply multiple detection policies to agents and policy groups. If you apply detection policies to any of the default OS-specific policy groups, the policies are automatically applied to an agent when the agent registers with the management server.

To apply a policy to an agent or policy group

1. In the management console, click **Assets**.
2. Under the Assets tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent or policy group, and then right-click **Apply Policy**.
4. In the **Set Policy Wizard** dialog box, select the policy that you want to apply to the agent or policy group, and then click **Next**.

   Double-click the **Symantec** folder to list the Symantec policies.

   If applying a policy directly to an agent, the operating system is selected for you. If applying a policy to a group, select the operating system, and then select the policy.

   To select multiple detection policies, hold down the Shift or Ctrl key while selecting the policies.
5. If the agent or group already has a policy (other than the Null policy) applied to it, in the **Set Policy Wizard** dialog box, select the merge option, and then click **Next**.
6. (Optional) If you want to edit the policy options before applying the policy, in the **Set Policy Wizard** dialog box, click **Edit Policy**.
7. In the **Set Policy Wizard** dialog box, review the policy summary, and then click **Finish** to apply the policy to the agent or agent group that you selected.
8. In the management console, click **Refresh** to apply the agent updates.

About merging policy options

Symantec Critical System Protection prompts you to select a merge option if you are applying a policy to an agent or policy group that already has a policy, and the policies have the same agent version and operating system.

You are prompted to select a merge option in the following situations:

- When updating a workspace policy with a library policy
- When applying a library policy to an agent or policy group that already has a policy
- When applying a workspace policy to an agent or policy group that already has a policy
- When using the Copy Options command to merge the option settings from two workspace policies

In these situations, you must select one of the following merge options:

Retain current option settings	Keep the current policy's option settings. This option uses the current policy settings and ignores the new policy.
Merge the changed options	Merge all changes in the current policy with the option settings in the new policy. Preference is given to the new policy when an option in both policies has changed or neither option has changed. In most cases, you will select this option. It gives you the best of both policies. All changes from the base in the current policy are retained. All other option settings are taken from the new policy.
Merge the changed options (when using the Copy Options command)	Merge all changes in the current policy with the option settings in the new policy. Preference is given to the old policy when an option in both policies has changed or neither option has changed.
Take the new option settings	Discard the current policy's option settings and apply the new policy's option settings. This option ignores the current policy and uses the new policy settings.

Managing applied policies

You can edit, save, and clear policies that are applied to an agent or policy group.

Editing a policy applied to an agent or group

You can edit policies applied to agents or policy groups. When you edit policies applied to a policy group, the management server determines which agents in that group use the group's policy and then flags those agents for pending policy updates.

Your policy option changes affect only the selected agent or policy group. The changes do not affect the workspace policy.

See "Editing a workspace policy" on page 132.

To edit a policy applied to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent or policy group, and then right-click **Edit Policy**.

   If you are editing a policy that is applied to a group, select the policy, and then click **OK**.
4. In the policy dialog, configure the policy options.
5. Click **OK** to save your changes.
6. Click **View > Refresh** to apply the agent updates.

Saving a policy applied to an agent or group

You use the Save Applied Policy command to save an applied policy as a workspace policy. The workspace policy is saved in a user-specified workspace folder, using the same name and revision as the applied policy. If a policy with the same name already exists, a number is appended to the workspace policy name.

To save a policy applied to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**
3. On the Assets page, select an agent or policy group, and then right-click **Save Applied Policy**.
4. In the **Save Policy** dialog box, select a policy to save.
5. In the **Save Policy** dialog box, select a destination folder.
6. Click **OK**.

Clearing a policy applied to an agent or group

You can clear policies that are applied to agents and policy groups.

When clearing policies, you should note the following:

- When you clear a policy that is applied to a policy group, the policy is deleted from the group. The management server determines which agents in the group (or the group's descendents) use the group's policy and then flags those agents for pending policy updates.
- (Prevention policies) If any of the agents in a group cannot find a compatible policy, the clear policy request is denied.
- (Prevention policies) If a request to clear a policy is denied because a compatible policy cannot be found, replace the policy that you want to clear by applying another policy.
  See "Applying a policy to an agent or policy group" on page 106.

To clear a policy applied to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent or group, and then right-click **Clear Policy**.

   You can select one or more agents.
4. In the **Clear Policy** dialog box, select the policy that you want to clear, and then click **OK**.
5. Click **Refresh** to apply the agent updates.

Applying a configuration to an agent or configuration group

You apply a configuration to an agent directly or through a configuration group. When you apply a configuration to a group, the management server determines which agents in that group use the group's configuration and then flags those agents for pending configuration updates.

To apply a configuration to an agent or configuration group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent or group, and then right-click **Apply Config**.

4 In the **Apply Config Wizard** dialog box, select a configuration, and then click **Finish**.

Double-click the **Symantec** folder to list the Symantec configurations.

5 Click **Refresh** to apply the agent updates.

Managing applied configurations

You can view and clear configurations that are applied to agents and configuration groups.

Viewing a configuration applied to an agent or group

You can view details about the configurations that are applied to agents and configuration groups.

To view a configuration applied to an agent or group

1 In the management console, click **Assets**.

2 Under the **Assets** tab, click **Prevention** or **Detection**.

3 On the Assets page, select an agent or group, and then right-click **View Config**.

4 In the **View Config** dialog box, select a configuration, and then click **OK** to view the configuration.

5 In the configuration dialog box, click **OK**.

Clearing a configuration applied to an agent or group

You can clear configurations that are applied to agents and configuration groups.

When clearing a configuration, you should note the following:

- When you clear a configuration that is applied to a configuration group, the configuration is deleted from the group. The management server determines which agents in the group (or the group's descendents) use the group's configuration and then flags those agents for pending configuration updates.
- Each configuration type has its own group hierarchy. Each agent must be able to find a configuration object, either applied directly to it or from the group hierarchy.
- If a request to clear a configuration is denied because a compatible configuration of the same type cannot be found, replace the configuration that you want to clear by applying another configuration of the same type.

To clear a configuration applied to an agent or group

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Prevention** or **Detection**.
3. On the Assets page, select an agent or configuration group, and then right-click **Clear Config**.
4. Click **Refresh** to apply the agent updates.

Deleting an agent

You can delete agents in the Network view and the Detection view.

Deleting an agent in the Network view

When you delete an agent in the Network view, the agent's record in the management server database is deleted. Deleting an agent in the Network View automatically removes the agent from all hierarchies in the Prevention view and the Detection view.

If the agent software is not removed from the agent computer, the agent automatically re-registers with the management server during the agent's next polling interval. During re-registration, the policies that were applied to the agent before it was deleted are re-applied.

To delete an agent in the Network view

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Network**.
3. On the Assets page, select an agent, and then right-click **Delete**.
4. In the **Confirm Deletion** dialog box, click **Yes** to delete the agent.
5. Uninstall the agent software from the agent computer.
6. In the management console, click **Refresh** to apply the agent updates.

Deleting an agent in the Detection view

You can delete an agent from a detection policy group, as long as the agent resides in at least one other detection policy group.

You cannot delete an agent from a configuration group. Every agent resides in exactly one configuration group at all times.

To delete an agent in the Detection view

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Detection**.
3. On the Assets page, navigate to and select the agent, and then right-click **Delete**.
4. In the **Confirm Deletion** dialog box, click **Yes** to delete the agent.
5. Click **Refresh** to apply the agent updates.

Chapter 4

Managing policies

This chapter includes the following topics:

About policies

Symantec Critical System Protection uses the following types of policies:

Prevention policies	Prevention policies protect against inappropriate modification of, rather than inappropriate access to, system resources. The prevention policies confine each process on a computer to its normal behavior. Programs that are identified as critical to system operation are given specific behavior controls, while generic behavior controls provide compatibility for other services and applications. See the *Symantec Critical System Protection Prevention Policy Reference Guide* for descriptions of the Symantec Critical System Protection prevention policies.
Detection policies	Detection policies monitor events and syslogs, and report anomalous behavior. Features include sophisticated policy-based auditing and monitoring; log consolidation for easy search, archival, and retrieval; advanced event analysis and response capabilities; and file and registry protection and monitoring. See the *Symantec Critical System Protection Detection Policy Reference Guide* for descriptions of the Symantec Critical System Protection detection policies.

Policies have options that let you configure a policy for assignment to a target computer. Policy options comprise a simplified set of controls that you can use to enable or disable features in a policy. Some options have parameters, which let you customize the behavior of the option.

About the Symantec policy library

Symantec Critical System Protection is packaged with pre-configured prevention and detection policies, which are stored in the policy library, in the Symantec folder. The policies are read-only and cannot be modified or deleted.

The policy library may also contain custom policies that you authored, as well as policies from third-party policy developers.

About policy viewer

The policy viewer enables you to search policies through the management console. However, you cannot make changes to the policies in the policy viewer. Afer you search for policies, you can export the data in the **Policy Summary** section to a CSV, HTML or PDF file.

The policy viewer enables you to search for a policy based on **Policy ID**, **PolicyName**, and **GroupName**. You can arrive at a specific policy search result with the help of search filters. These search filters are **Os Type**, **Category**, **Instance**, **Status**, **Time Frame**, **Version**, and **Resource Type**. In addition, you can select the display attributes to control the display of search results in the **Policy Summary** section. These display attributes are **Data Detail**, **Content Display**, **Content Hidden**, **Symbol**, **Header**, **Footer**, and **Indent Style**.

The **Policy Summary** section displays the search results based on the search filters and the display attributes.

The **SQL** section displays the SQL stored procedure for all search attributes that you have selected.

Note: The policy viewer displays only primary policies. It does not display the custom policies that you have added.

See “Searching for policies in the policy viewer” on page 144.

See “Policy viewer search filters” on page 145.

See “Policy viewer display attributes” on page 148.

See “Policy Summary information” on page 149.

Viewing the Policies page

You use the Policies page in the management console to manage the policies that agents enforce on your computers.

You can do the following activities from the Policies page:

- Create and edit policies
- Apply and reapply policies to agents and policy groups
- View policy properties
- Create folders to organize your policies
- Reset policy options
- Rename, copy, and delete policies
- Apply revisions to the Symantec policies
- Updated policy, copy options, and custom controls
- Import and export policies

To obtain an overview of prevention policies or detection policies, view policies in the Prevention view or Detection view. To obtain an overview of all your policies, view policies in the Master view.

To view the Policies page

1. In the management console, click **Policies**.
2. On the Policies page, in the Policies tree, click the **Symantec** folder to list the Symantec Critical System Protection policies.
3. (Optional) To expand or restrict the list of policies, in the Filters tree pane, select one of the following filters:

All Policies	Filter that displays all prevention or detection policies.
Windows Policies	Filter that displays the Windows prevention or detection policies.
Solaris Policies	Filter that displays the Solaris prevention or detection policies.
Linux Policies	Filter that displays the Linux prevention or detection policies.
AIX Policies	Filter that displays the AIX detection policies.
HPUX Policies	Filter that displays the HP-UX detection policies.
Tru64 Policies	Filter that displays the Tru64 UNIX detection policies.
UNIX policies	Filter that displays the unified UNIX detection policies.

4. (Optional) To expand or collapse the panes in the Policies page, click the size arrows.

About the policy workspace

The policy workspace lists the policies that agents enforce on your computers. The policy workspace is located on the right side of the Policies page. Upon installation of Symantec Critical System Protection, the policy workspace is populated with the pre-configured Symantec Critical System Protection policies.

You can populate your policy workspace with the following policies:

- Policies that you created using existing workspace policies as a baseline
- Policies that you obtained from third-party policy developers

The policy workspace comprises the following information:

Name	The name of a workspace policy. Workspace policies that were changed from the baseline settings are marked with a blue asterisk (*).
Rev	The policy revision number used to track changes to a policy.
Min. Agent	The minimum agent version needed to support a policy. Every Symantec policy is assigned a version number and a revision number. The version number refers to the minimum agent version needed to support a policy. The policy can only be applied to agents of this version or higher. Symantec uses the revision number to track changes to a policy.
Operating System	The operating system of the target computer.
Type	The type of policy (prevention, detection).
Date Modified	The date that a policy was last modified.

Creating a workspace policy

You create a workspace policy by basing it on an existing policy. You can base a workspace policy on a Symantec Critical System Protection policy, a policy that you customized in the management console or a policy that you obtained from a third-party policy developer.

You create a policy using the New Policy Wizard. The New Policy Wizard walks you through a series of Wizard pages about the policy that you want to create. You can follow each prompt by clicking Next, or you can click a specific prompt to jump directly to that Wizard page. You can click Finish at any time.

All Wizard pages apply to prevention policies. Only the Select a Policy and Summary pages apply to detection policies.

The New Policy Wizard pages are as follows:

Select a Policy

(Prevention and detection)

To select a policy, do the following:

- In the Name box, type a name for the new policy.
- In the Operating System box, select the target operating system for the new policy. The policy list is refreshed to show the policies for the selected operating system.
- In the Policy Pack box, select the Symantec Critical System Protection policy pack that contains the policy to use as a baseline. Select All to list policies from all Symantec Critical System Protection policy packs.
- In the policy list, select the policy on which you want to base the new policy.

Click the Advanced button to browse the policy library; to open a policy folder, double-click it. The Advanced button toggles between the policy library and the policy list. Click Advanced once to browse the policy library. Click it again to return to the policy list.

Prevention Mode

(Prevention)

Click the prevention indicator to enable or disable prevention. The prevention indicator turns red (when prevention is disabled) and green (when prevetion is enabled).

Setting the disable prevention option is useful if you want to test the policy before enforcing it. Disabling prevention logs policy violations but does not enforce the violations. This lets you gather information about how a computer performs, without running the risk of preventing critical aspects of your computer operation.

Inbound Network Access

(Prevention)

Prevention policies contain options that let you control whether remote computers can make network connections. By default, all prevention policies have the global prevent inbound network connections option enabled. You can permit all remote computers to connect, block all remote computers from connecting, or allow only specific IP addresses or subnets to connect.

Add the addresses to the list of addresses that can make inbound network connections. Specify the addresses in CIDR format, such as 192.168.1.0/24.

Outbound Network Access

(Prevention)

By default, the Strict prevention policy prevents outbound network connections, except on ports 80 (HTTP), 135 (Location Service), 389 (LDAP), and 443 (HTTPS). You can specify a list of programs that are allowed to use the network freely, or disable this prevention completely.

Trusted Applications

(Prevention)

Some programs may require more than the default file and registry access to function properly. You can grant this access by giving these programs additional privileges within the policy.

Safe privileges allow a program to access core operating system resources, but not Symantec Critical System Protection resources or user-defined resource lists.

Full privileges are not subject to file or registry restrictions and allow a program to access all resources.

Trusted Users

(Prevention)

When an alternate privilege level is applied to a user, all interactive programs run by that user are run at the user's privilege level.

Safe privileges allow a user access to core operating system resources, but not to Symantec Critical System Protection resources or user-defined resource lists.

Full privileges allow a user access to all resources.

Trusted Groups

(Prevention)

When an alternate privilege level is applied to a user group, all interactive programs run by a group member run at the group's privilege level.

Safe privileges allow a group access to core operating system resources, but not to Symantec Critical System Protection resources or user-defined resource lists.

Full privileges allow a group access to all resources.

Policy Override

(Prevention)

The Symantec Critical System Protection agent includes the policy override tool, which allows a user logged onto an agent computer to override the policy applied to the agent. The policy override tool is available on computers that run supported Windows, Solaris, and Linux operating systems.

List the users and groups that are allowed to run the policy override tool.

Setting the policy override options in the New Policy Wizard sets the corresponding options in the policy.

Agent Tools

(Prevention)

The agent includes a command-line tool to reconfigure parameters that were set during installation, and parameters that are not accessible with the management console.

In the policy, list the users and groups that are allowed to run the agent command-line tool.

Note: Because the prevention policies include protection against processes that modify Symantec Critical System Protection resources, you cannot run the agent command-line tool with the default policy settings.

Agent Event Viewer (Prevention)	The Symantec Critical System Protection agent includes the agent event viewer, which allows a user logged onto an agent to display recent events reported by the agent. The agent event viewer is available on computers that run supported Windows and Windows NT Server operating systems. This option appears for Windows prevention policies that use agent versions 5.1.0 or higher. List the users and groups that are allowed to run the agent event viewer. Setting the agent event viewer options in the New Policy Wizard sets the corresponding options in the policy. See the *Symantec Critical System Protection Agent Guide* for instructions on how to use the agent event viewer.
Summary (Prevention and detection)	Review the policy options.

To create a workspace policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, in the Policies tree, select the folder in which you want to store the new policy, and then right-click **New Policy**.
4. In the **New Policy Wizard** dialog box, respond to each prompt, and then click **Next** after each response.

   You can follow each prompt by clicking **Next**, or you can click a specific prompt to jump directly to that Wizard page. You can also click **Finish** at any time.
5. In the **New Policy Wizard**, in the **Summary** pane, click **Finish**.

   Your new policy appears in the policy workspace pane, in the folder that you selected.

Creating default workspace policies from an installed policy pack

You can create default workspace policies from all the compiled policies in an installed Symantec Critical System Protection policy pack. The policies are created in a folder of your choice.

Before using these instructions, you must download the latest Symantec Critical System Protection policy packs.

See "About updating Symantec policy and report packs" on page 48.

To create default workspace policies from an installed policy pack

1. In the management console, click **Policies**.
2. Under the **Policies** tab, **Prevention** or **Detection**.
3. On the Policies page, select a folder in which to store the default workspace policies, and then right-click **Create Default**.
4. In the **Create Default Policies** dialog box, select an installed Symantec Critical System Protection policy pack.
5. Click **Create**.

Controlling custom programs in prevention policies

The prevention policy editor includes a feature called My Custom Programs. You use My Custom Programs to control interactive programs and services separately from the default interactive programs and services.

My Custom Programs creates the following set of options to control each custom program that is defined in the policy:

Table 4-1 My Custom Program options

Option	Description
Specify Interactive Programs (or Services) with Custom privileges	Defines the interactive programs (or services) that are controlled by the custom group.
Disable prevention - log but do not prevent policy violations	Disables prevention of policy violations by programs in the custom group.
Enable logging of trivial policy violations	Logs all policy violations by programs in the custom group.
Block modifications to executable files	Prevents programs in the custom group from modifying executables files on disk.
Block modifications to startup folders	Prevents programs in the custom group from modifying the contents of startup folders.
Block registration of COM and ActiveX controls	Prevents COM objects and ActiveX controls from registering as an in-process server for programs in the custom group.

Table 4-1 My Custom Program options *(continued)*

Option	Description
Enable buffer overflow detection	Enables buffer overflow detection for programs in the custom group.
Enable thread injection detection	Enables thread injection detection for programs in the custom group.
Resource lists	Defines file access for programs in the custom group.
Network controls	Controls network access for programs in the custom group.
SysCall options	Controls privileged system calls made by programs in the custom group.
Process logging options	Controls process logging by programs in the custom group.

To control custom programs in prevention policies

1. In the management console, click Policies.
2. Under the **Policies** tab, click **Prevention**.
3. On the Policies page, double-click a selected prevention policy.
4. In the policy editor dialog box, under **Policy Settings**, click **My Custom Programs**, and then click **Add a new Custom Control** icon.

5 In the **New Custom Control Wizard** dialog box, specify the following information.

Display Name	Type a descriptive name for the custom options. This text appears in the management console, in the policy editor dialog, under My Custom Programs.
Category	Select a program type.
Identifier	Type a name to identify the custom options. The identifier must not include spaces or special characters. The identifier is used to create the process set name, which uses the format cust_identifier_ps.
Group Tags	Type a Group Tag name. You can associate a single group tag or multiple group tags with custom programs. You can specify multiple group tags as comma separated values. For example, GRPTAG1, GRPTAG2, GRPTAG3 and so on.
Description	Type a full description of the program that is controlled by the custom options.

6 Click **Finish**.

7 In the policy editor dialog box, under My Custom Programs, click **Edit** icon next to the custom program to view the policy options.

8 In the policy editor dialog box, check or uncheck the required policy options under **General Settings**, **Network Controls**, **File Rule**s, and **Registry Rules**.

9 Click **OK** to save the policy changes,

About importing a large set of values for a parameter

The Symantec Critical System Protection Policy Editor lets you import a large set of values for a parameter in the Symantec Critical System Protection policy. For example, suppose that you want to create a network rule that blocks all incoming connections from a set of IP addresses. In this case, you can create a set of values for the IP address parameter in a comma-separated value (CSV) format. You can then import the file that contains the value set into the Symantec Critical System Protection policy. After you import the CSV file, the parameter values are populated at the top of existing list of parameter values.

To import a set of parameter values, use Microsoft Excel or any application that supports the CSV format to create a CSV file. When you import parameter values, you can either add new parameter values to the existing list of parameter values or you can replace the existing list.

By default, the Policy Editor ignores the duplicate parameter values. However, if you type a parameter value that already exists in the list, Symantec Critical System Protection displays an error message.

Also, you can export an existing list of parameter values in the Symantec Critical System Protection policy in the CSV file format.

About creating an input comma-separated value file

The input comma-separated value (CSV) file contains parameter values in a comma-separated format. Each parameter type has its own format that includes the data fields in the corresponding parameter type. The first line in the CSV file contains a comma-separated list of column headers.

Table 4-2 List of parameter types, column headers, and the parameter value format.

Parameter type	Column headers
String	String-value, rule-name, comment
stringlist	String-value, rule-name, comment
processlist	program, command-line, id, group-id, rule-name, comment
processnocmdlist	program, id, group-id, rule-name, comment
resourcelist	String-value , program, command-line, id, group-id, rule-name, comment
networklist	Action, protocol, local-port, remote-ip, remote-port, log, rule-name, comment
networkprocesslist	Action, protocol, local-port, remote-ip, remote-port, log, program, command-line, id, group-id, rule-name, comment
datetimevalue	date, time-zone, rule-name, comment
Datetimeduration	duration, rule-name, comment
datetimerepeat	Frequency, rule-name, comment

In the CSV file, each row should contain one value set of the parameter. Each row includes the components of the parameter, such as protocol, action, local port, remote port, remote IP address.

For example, if you import a CSV file that contains values for Network Rules parameter, the CSV file looks like:

action, protocol, Local-port, remote-ip, remote-port, log, rule-name, comment

net_action_choice_allow , net_protocol_choice_tcp , %iis_accept_tcp_list%,%iis_netaccept_addr_list%, ,net_log_choice_none,rul1,Symantec default

Importing an input CSV file

To import an input CSV file

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the **Policies** page, in the **Symantec** folder, edit any policy.
4. In the **Policy Editor** dialog box, under **Resource Lists**, click **Network Rules**.
5. Under **Kernel Driver Options [kernel_ps] > Inbound Network Rules**, beside **Process Set Inbound Rules**, click **Edit[+]**.
6. Click **Import**.
7. In the **Import** dialog box, select the CSV file to import and then click **Import**.

Exporting the parameter values into a CSV file

To export the parameter values into a CSV file

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention**.
3. On the **Policies** page, in the **Symantec** folder, edit any policy.
4. In the **Policy Editor** dialog box, under **Resource Lists**, click **Network Rules**.
5. Under **Kernel Driver Options [kernel_ps] > Inbound Network Rules**, beside **Process Set Inbound Rules**, click **Edit[+]**.
6. Select the rows that you want to export and click **Export**.
7. In the **Export To** dialog box, browse the destination folder, select an **Export Range**, type a name for the export file.
8. Click **Export**.

Adding group tags to custom programs

You can organize custom programs by grouping them in folders. To do so, in the **Policy Editor** dialog box, you can assign a group tag to each custom control. However, a custom program can have zero or more group tags associated with it. Also, you can select a single or multiple custom controls in the **Policy Editor** dialog box and group them in a single or multiple folders.

A custom program without a group tag is grouped under the **Default** folder. The **Group Tags** tab in the **Policy Editor** dialog box displays a list of all the custom programs that are grouped together by their group tags.

To add group tags to custom programs

1. Open the **Policy Editor** dialog box.
2. Click **My Custom Programs**.
3. Click **Add a new Custom Control**.
4. In the **New Custom Control Wizard** dialog box, perform the following actions:

   Display Name
   Type a descriptive name for the custom options.

   This text appears in the management console, in the **Policy Editor** dialog box, under **My Custom Programs**.

   Category
   Select a program type.

   Identifier
   Type a name to identify the custom options. The identifier cannot include spaces or special characters.

   The identifier is used to create the process set name, which uses the format cust_identifier_ps.

   Group Tags
   Type a Group Tag name. You can associate a single group tag or multiple group tags with custom programs.

   You can specify multiple group tags as comma-separated values. For example, you could use GRPTAG1, GRPTAG2, GRPTAG3 and so on.

   The **Group Tags** tab displays all the group tags with their associated custom programs.

   Description
   Type a full description of the program that is controlled by the custom options.

5. Click **Finish**.

Searching for custom programs by group tags

You can search for a custom program by its group tag.

To search for custom programs by group tags

1. Open the **Policy Editor** dialog box.
2. Click **My Custom Programs**.
3. In the top-right **search** box, type a group tag name and press **Enter**.

Modifying an existing group tag

You can modify an existing group tag in the **Group Tags** tab of the **Policy Editor** dialog box.

To modify an existing group tag

1. Open the **Policy Editor** dialog box.
2. In the **Policy Editor** dialog box, click **My Custom Programs**.
3. In the **My Customs Programs** dialog box, under **Group Tags** tab, check the box beside the custom program that you want to edit.
4. Click the **Add group tags to selected Custom Controls** icon.
5. In the **Add Group Tags** dialog box, type a new group tag name for the selected custom program.

Applying and reapplying workspace policies

You use the Apply Policy command to apply a workspace policy to agents and policy groups that do not currently enforce the policy.

You use the Reapply Policy command to reapply a workspace policy to agents and policy groups that currently enforce the policy. The Reapply Policy command is useful when you need to reapply a workspace policy that was modified.

After you apply or reapply a prevention policy to a target computer, you should verify the operation of the computer.

See “Verifying prevention policies” on page 141.

Applying a workspace policy to an agent or group

When applying a policy, you are prompted to select the agents and policy groups that will enforce the policy.

To apply a workspace policy to an agent or group

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, select a policy to apply, and then right-click **Apply Policy**.

   To select multiple policies, hold down the Shift or Ctrl key while selecting the policies.
4. In the **Apply Policy** dialog box, select the agents and policy groups, and then click **Apply**.

   To select multiple agents and agent groups, hold down the Ctrl key while making your selection.
5. In the management console, click **Refresh** to update the management console page.

   Refreshing the page lets you confirm that the agents successfully processed the policy changes.

Reapplying a workspace policy to an agent or group

When reapplying a policy, you are presented with a list of agents and policy groups that currently enforce the policy. You can reapply the policy to some or all of those agents and groups.

When reapplying a policy, you can choose to retain the old policy option settings, merge the old and new option settings, or take the new option settings.

See “About merging policy options” on page 108.

To reapply a workspace policy to an agent or group

1. In the management console, click **Policies**.
2. Under the Policies tab, **Prevention** or **Detection**.
3. On the Policies page, select a policy to reapply, and then right-click **Reapply Policy**.

   To select multiple policies, hold down the Shift or Ctrl key while selecting the policies.
4. In the **Reapply Policy Wizard** dialog box, select the agents and policy groups, and then click **Next**.

   To select multiple agents and agent groups, hold down the Ctrl key while making your selection.
5. In the **Reapply Policy Wizard** dialog box, select the merge option.

6 Click **Finish**.

7 In the management console, click **Refresh** to update the management console page.

Refreshing the page lets you confirm that the agents successfully processed the policy changes.

Viewing policy properties

Policy properties provide the following information about a workspace policy:

General tab	Provides policy name and description, tree path, revision number, and target operating system. You can modify the policy name, description, and revision number.
Applied To tab	Lists the agents and groups to which a policy is currently applied. From this tab, you can reapply a policy. Select the agents and policy groups, and then click Reapply. To select multiple agents and groups, hold down the Ctrl key while making your selection.
Recent Events tab	Lists recent events for a policy.
History tab	Lists audit events for a policy.

To view policy properties

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click**Prevention** or **Detection**.

3 On the Policies page, select a policy, and then right-click **Properties**.

4 In the properties dialog box, view and edit the policy information.

5 Click **OK**.

Creating a policy folder

You use folders to organize your policies. For example, you might use folders to reflect the structure of your network environment, or to group policies by operating system. There is no limit to the number of folders that you can create. You can create nested folders within other folders.

The default policy folder is named Workspace. It contains the Symantec folder, which contains the policies that are included with Symantec Critical System Protection.

Create policy folders so that you can edit policy options efficiently. Name policy folders so that you can easily identify which policies to assign to the folders.

To create a policy folder

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, in the Policies tree, select the default Workspace folder or another folder, and then right-click **New Folder**.

   A new policy folder is created with the name New Folder.
4. Rename the policy folder, and then press the **Enter**.

Moving a workspace policy to a folder

You move policies to folders using the following methods:

- Drag-and-drop operation
  You can move a policy from one folder to another folder in a drag-and-drop operation. In the Workspace pane, select a policy, and then drag it to the desired folder in the Policies tree.
- Move To command
  You can move a policy from one folder to another folder using the Move To command. In the Workspace pane, select a policy, and then right-click **Move To**. In the **Move Folder** dialog box, select the folder to receive the policy, and then click **Move To**.

Editing a workspace policy

You can edit a workspace policy to adjust the policy options.

You are prompted to complete a change request that describes the policy modifications.

Policy modifications are saved in your policy workspace. The modifications are not applied to the agents and policy groups that enforce the policy. You must manually reapply the policy to take advantage of the modifications.

To edit a workspace policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, select a policy, and then right-click **Edit Policy**.

4 In the policy dialog box, specify how you want to view the policy options by selecting one of the following:

General

Displays general policy and reference information, such as policy description, type, revision number, minimum agent version, target operating system, referenced policy pack, and policy pack status.

Settings

Displays the full policy option tree.

Options are check boxes that you set or clear. Parameters are lists of files, registry keys, programs, port numbers, etc.

Note: When you set an option that contains a parameter, also set the parameter. Agents reject policies that contain empty parameters.

Changes from Base

Displays the changes made to a base policy.

The options and parameter values that are changed from the default library settings are shown in bold. The Changes column indicates what kind of change was made to the option (enabled or disabled) or parameter (added or removed).

Summary

Displays a summary of the policy options in tree form. The tree includes only those options that are enabled and the parameters that have values. The parameter values are listed below the parameter names.

Parameters with comments are flagged with the following colored icons:

- Yellow icon indicates Symantec default comments.
- Blue icon indicates user-specified comments.
- Gray icon indicates comments auto-generated by the Event Wizard.
- Green icon indicates default comments.

IPress Ctrl+A to select the settings and then press Ctrl+C to copy the settings to the Windows clipboard. You can paste the contents of the clipboard into a text file.

My Custom Programs

Displays the custom programs that are defined in the policy.

My Custom Programs creates a set of options to control interactive programs and services separately from the default interactive programs and services.

See "Controlling custom programs in prevention policies" on page 123.

Show advanced options normally hidden in the policy	Select this check box to display hidden policy options.

5 In the policy dialog box, enable or disable the policy options as needed.

To view a pop-up tool tip, roll your mouse cursor over an option.

6 Click **OK**.

7 In the **Submit Changes** dialog box, complete the following change request information:

Write a policy change description	Type a description of the policy modification.
Update revision to	Select this check box to update the policy revision number. The revision number is automatically incremented by one. You may accept the incremented revision number or enter another revision number.

8 Click **Submit**.

How to determine a policy's policy pack reference

In the policy dialog, the general policy information identifies the Symantec Critical System Protection policy pack in which a policy is contained.

You see one of the following messages:

This policy references the latest policy pack	You see this message, along with a green circle icon, when the referenced policy pack is the latest version.
A newer policy pack exists; this policy should be updated	You see this message when the referenced policy pack is not the latest version. If the referenced policy pack is not the latest version, you should update the workspace policy with the latest policy pack. See "Updating a workspace policy" on page 139.

Copying policy options

The Copy Options command copies policy options from one workspace policy to another workspace policy. The Copy Options command assists in maintaining a consistent set of policies across platforms. For example, suppose you customized the options in Prevention_Windows_Policy_A and you want to reuse the options in Prevention_Windows_Policy_B. Without the Copy Options command, you would have to manually re-enter all the options into Prevention_Windows_Policy_B.

With the Copy Options command, you simply select the policy that contains the options you want to copy, select the target policy, and then indicate how you want to merge the policy options.

See "About merging policy options" on page 108.

When copying policy options, the workspace policies must be of the same type (prevention or detection). All policy options are copied to the target policy.

To copy policy options

1. In the management console, click **Policies**.
2. Under the Policies tab, click **Prevention** or **Detection**.
3. On the Policies page, in the workspace pane, select the policy that contains the options you want to copy, and then right-click **Copy Options**.
4. In the **Copy Policy Options Wizard** dialog box, select the target policy, and then click **Next**.
5. In the **Copy Policy Options Wizard** dialog box, select **Merge the changed options** or **Take the new option settings** (default).
6. Click **Finish**.

Resetting policy options

Resetting the options for a policy removes all changes to the option settings and restores the baseline settings.

You are prompted to complete a change request that describes the policy change.

To reset policy options

1. In the management console, click **Policies**.
2. Under the Policies tab, click **Prevention** or **Detection**.
3. On the Policies page, select a policy, and then right-click **Edit Policy**.
4. In the policy dialog box, click **Reset**.

5 Click **OK**.

6 In the **Submit Changes** dialog box, complete the following information:

Write a policy change description	Type a description of the policy change.
Update revision to	Select this check box to update the policy revision number. The policy revision number is automatically incremented by one. You may accept this revision number or enter another revision number.

7 Click **Submit**.

8 (Optional) Reapply the modified policy to agents and policy groups.

Renaming a workspace policy

You can rename workspace policies.

To rename a workspace policy

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention** or **Detection**.

3 On the Policies page, select a policy, and then right-click **Rename Policy**.

4 Type a new policy name, and then press **Enter**.

Copying a workspace policy

Copying a workspace policy creates a copy of the policy. The copy is saved in the same folder as the original policy. The copy name is prefixed with Copy_of followed by the original policy name. For example:

Copy_of_sym_win_protection_core

After copying a policy, you should move the copy to your own policy folder. Do not store the copy in the Symantec folder.

To copy a workspace policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, select a policy, and then right-click **Copy Policy**.

   To copy multiple policies, hold down the Shift or Ctrl key while selecting the policies.

Deleting a workspace policy

You can delete policies from the policy workspace.

To delete a workspace policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. On the Policies page, select the policy that you want to delete, and then right-click **Delete Policy**.
4. In the **Confirm Deletion** dialog box, click **Yes** to delete the selected policy.

Importing and exporting policies

You can import and export prevention and detection policies.

See "Installing the Windows NT policy" on page 138.

Importing policies

You can import the following policies from files:

- Library policies
  Symantec periodically releases policy packs that contain revisions to the Symantec Critical System Protection policies. Symantec releases the policy packs in zip files.
  See "About updating Symantec policy and report packs" on page 48.
  Once imported, library policies are visible when you create a new workspace policy. You can identify these policies by their revision numbers.
- Custom policies
  You can import custom policies that were previously exported. Once imported, custom policies are immediately visible in the policy workspace. You can update custom policies with the Symantec library policies.

The import process is the same for library policies and custom policies. The management console recognizes the policy pack type and imports the policies to the correct destination, which is the policy library or your policy workspace.

See “Installing the Windows NT policy” on page 138.

To import policies

1. In the management console, click **Policies**.
2. Under the Policies tab, click **Prevention** or **Detection**.
3. On the Policies page, in the Policies tree, navigate to and select the folder and then right-click **Import Policy**.
4. In the **Import** dialog box, browse to the policy pack that you want to import.
5. Click **Import** to import the policy into the policy library.

   In the **Import** dialog box, each successfully imported policy is marked with a green check mark.

Installing the Windows NT policy

The Windows NT prevention policy is not part of the Symantec Critical System Protection installation. You must install the policy separately.

You can obtain the Windows NT policy from the Symantec Critical System Protection installation CD, and then manually import the policy into the policy library.

Before installing the Windows NT prevention policy, please note the following:

- The Windows NT prevention policy is only for use with Windows NT agents.
- The Windows NT policy is stored on the installation CD, in the file sym_winnt_protection_sbp.zip.
- After importing the Windows NT policy into the policy library, you must create a new prevention policy that is based on the Windows NT policy. You should store this new policy in a separate policy folder (for example, name the policy folder Symantec NT policy). Storing the policy separately from the other Windows prevention policies will help ensure that the Windows NT policy is only applied to Windows NT agents.

To install the Windows NT policy

1. Insert and display the installation CD.
2. In the management console, click **Policies**.
3. Under the **Policies** tab, click **Prevention**.
4. On the Policies page, click **File > Import Policy**.

5 In the **Import** dialog box, browse the installation CD and select the policy file sym_winnt_protection_sbp.zip.

6 Click **Import** to import the Windows NT policy into the policy library.

7 In the Policies pane, create a folder for the Windows NT policy.

For example, name the policy folder Symantec NT policy.

8 In the Windows NT policy folder that you created, create a workspace policy that is based on the Windows NT policy.

Exporting policies

You can export your custom policies to files. Exporting policies is useful for sharing policies with other Symantec Critical System Protection administrators. You can export one or more policies. Exported policies are saved in .zip files.

To export policies

1 In the management console, click **Policies**.

2 Under the **Policies** tab, click **Prevention** or **Detection**.

3 On the Policies page, in the Policies tree, navigate to and select the folder that contains the policies that you want to export, and then right-click **Export Policy**.

To select multiple policies, hold down the Ctrl key while selecting the files.

4 In the **Export** dialog box, browse to the folder where you want to export the policies.

5 In the **Export** dialog box, in the File Name box, type a name for the export file, and then click **Export**.

The selected policies are exported to a .zip file, using the file name that you specified.

In the **Export** dialog box, each successfully exported policy is marked with a green check mark.

6 In the **Export** dialog box, click **Close**.

Updating a workspace policy

Symantec periodically releases policy packs that contain updates to the Symantec Critical System Protection policies. These policy packs contain internal improvements and additional policy option controls. To incorporate Symantec Critical System Protection policy updates with your workspace policies, you use the Update Policy command.

Before you update a workspace policy, you should note the following:

- You must obtain the Symantec Critical System Protection policy packs. The easiest way to get a policy pack is to use LiveUpdate.
  See "About updating Symantec policy and report packs" on page 48.
- Make a backup copy of the workspace policy that you want to update. This lets you revert to the pre-updated version in case any problems occur with the updated version.
- When updating a workspace policy that was applied to an agent, you must decide how you want to merge the option settings of the workspace policy with the baseline settings of the Symantec Critical System Protection policy.
- You can update a UNIX workspace policy with a new UNIX policy, but you cannot update a UNIX OS-specific (for example, Solaris) workspace policy with a new UNIX policy.
  You may attempt to retain the policy settings by creating a new UNIX workspace policy, and using the Copy Options command to copy the option settings from the Linux policy to the UNIX policy. The success of this approach depends on how many of the option and parameter names are consistent between the policies.
- You can update multiple workspace policies at once. When updating multiple policies, you prompted to select a currently-installed policy pack, and choose a merge strategy to apply to all selected policies. The selected pack is searched for a new compiled policy with the same name and OS type as the old compiled policy. If a matching compiled policy is found, the workspace policy is updated and merged. If a matching compiled policy is not found, the workspace policy is not updated or merged. You will not see a results screen that lists which policies were updated. As an informal measure, the names of the policies being updated appear briefly on-screen. You can determine if a policy was updated by checking the policy settings.

To update a workspace policy

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. In the Workspace pane, select a workspace policy, and then right-click **Update Policy**.

   To select multiple policies, press and hold the Shift or Ctrl key while selecting the policies.
4. In the **Update Policy Wizard** dialog box, select the Symantec Critical System Protection policy that you want to use to update your workspace policy, and then click **Next**.

5 In the **Update Policy Wizard** dialog box, select the policy merge option.

6 In the **Update Policy Wizard** dialog box, click **Finish** to save your changes.

7 In the management console, click **Refresh**.

8 (Optional) Reapply the updated policy to agents and policy groups.

Verifying prevention policies

Once you apply a prevention policy to a target computer, you can verify the operation of the computer using the Monitors page. The Monitors page displays event information reported to the management server from your entire agent deployment.

Using the Monitors page, search for events from the target computer.

Events that indicate unexpected activity or problems include the following:

- Events with a severity of warning indicate unexpected activity or problems that have already been handled by Symantec Critical System Protection. If the event has an event type of file access, network access, OS call, or buffer overflow, the warning severity indicates abnormal application behavior that was stopped. Since the behavior was stopped, no further action is required.
- Even if the policy is not enforcing prevention (that is, the disable prevention option is set), improper access to resources by a service or application generates events. With the disable prevention option set, the disposition property indicates allow instead of deny, and the severity property appears in blue instead of red.
- If the policy is enforcing prevention (the disable prevention option is not set), then warning events with an event type of file access, network access, or OS call indicate that a resource access which violated the policy was attempted and then stopped. A warning event with an event type of buffer overflow indicates that a buffer overflow which violated the policy was attempted and then stopped. These warning events might indicate that a service or application on the target computer is functioning improperly with the applied policy.

After investigating the policy violations, you can configure the policy and allow the service or application access to the specific resources if necessary.

You can use the following methods to configure a policy to allow the computer to function properly:

- If there are multiple warning entries from a service or interactive program, and that program has individual behavior controls written for it, you can tailor the policy specifically for that program.

- If there are no individual behavior controls written for the program, the program falls into either the Default Services or Default Interactive Programs group. In this case, you can configure the policy using the Default Service Options or the Default Interactive Program Options.
- You can also configure the policy using the Global Policy Options. The settings apply to the entire computer.
- To adjust the policy, look at the warning severity-type events, with an event type of file access, network access, or OS call, that are being generated on the computer. The process set shown on the Monitors page corresponds to an option group in the policy option tree.

The following rules apply to the Windows Strict prevention policy:

If the process set in the event is svc_stdpriv_ps or int_stdpriv_ps

Configure the process using one of the following:

- Default Service Options [svc_stdpriv_ps]
- Default Interactive Program Options [int_stdpriv_ps]

If the process set in the event is svc_safepriv_ps or int_safepriv_ps

The process has been granted safe privilege. Modify either the group level options for interactive programs or services, or the global options:

- General Service Options
- General Interactive Program Options
- Global Policy Options

If the process set in the event is svc_fullpriv_ps or int_fullpriv_ps

The process has been granted full privilege. Modify either the group level options for interactive programs or services, or the global options:

- General Service Options
- General Interactive Program Options
- Global Policy Options

Full privilege programs and services are not restricted from accessing any files or registry keys on the computer. However, they are restricted in terms of the networking they can perform. These processes obey the Network Remote Access restrictions, and the Network Resource Lists.

Other process sets

All other process sets can be found in one of the following option groups:

- Application Service Options
- Core OS Service Options
- Specific Interactive Program Options

Opening the policy viewer

If you have created policies and want to view these policies, you can open the policy viewer.

To open the policy viewer

1. In the management console, click **Policies**.
2. Under the **Policies** tab, click **Prevention** or **Detection**.
3. In the Workspace pane, select a policy and right-click **Edit Policy**.
4. In the policy editor dialog box, under **Policy Changes and Summary**, click **Policy Viewer**.

Searching policies

You can search for policies in the policy viewer. The ability to search policies lets you find a specific policy that you want to view. You must have full administration rights to search policies.

Table 4-3 provides the tasks you can perform to search for policies.

Table 4-3 Tasks to search policies

Step	Task	Description
1	Open the policy viewer	See "Opening the policy viewer" on page 143.
2 (Optional)	Enter the **Policy ID: (number)**	Use this search filter to search for a policy with a specific **Policy ID**. This filter cannot be used with any other filter since it is intended to find a specific policy to process. However, you can use the **Resource Type** filter with **Policy ID**.
3 (Optional)	Enter the **PolicyName**, **FolderName**, or **date**	Optionally, use any of these search filters to search for a policy with the **PolicyName**, **FolderName**, or **date**. Enter the date using the format DD-MON-YYYY. For example: 29-JAN-2011

Table 4-3 Tasks to search policies *(continued)*

Step	Task	Description
4 (Optional)	Enter the **GroupName**, **AgentName** or **date**	Optionally, use any of these search filters to search for a policy with the **GroupName**, **AgentName**, or **date**. Enter the date using the format DD-MON-YYYY. For example: 29-JAN-2011
5	Select the appropriate search filters.	You can filter the policy search results with the search filter values. See "Policy viewer search filters" on page 145.
6	Select the appropriate display attributes.	You can determine the policy display in the **Policy Summary** section by selecting the appropriate display attributes. See "Policy viewer display attributes" on page 148.
7	Click **Search**.	The search displays the policies in the **Policy Summary** section. It also shows the SQL stored procedures for the search result in the **SQL** section. See "Policy Summary information" on page 149.

See "About policy viewer" on page 117.

Searching for policies in the policy viewer

You can use the policy viewer to search and view policies in the Symantec Critical Systems Protection environment.

Note: The policy viewer displays only primary policies. It does not display the custom policies that you have added.

To search for policies in the policy viewer

1 Open the policy viewer.

2 Optionally, type the **policy ID: (number)** that you want to search.

3 Optionally, type the **PolicyName**, **FolderName**, or **date** of the policy that you want to search.

4 Optionally, type the **GroupName**, **AgentName**, or **date** of the policy that you want to search.

5 Select the appropriate search filters.

6 Select the appropriate display attributes.

7 Click **Search**.

See “About policy viewer” on page 117.

See “Policy viewer search filters” on page 145.

See “Policy viewer display attributes” on page 148.

See “Policy Summary information” on page 149.

Policy viewer search filters

When you open the policy viewer, the **Policy Summary** section is empty. You can use the default settings to search and populate the summary. You can filter the search results with the search filter values.

Table 4-4 provides the description for the search filters in the policy viewer.

Table 4-4 Policy viewer search filters

Search filter	Description
Os Type	Use this search filter to search for policies that are applied on operating sytems. Following operating system options are available: ■ **allOS** Use this search filter to select policies for all the operating systems. ■ **windows** ■ **unix** ■ **solaris** ■ **linux** ■ **hpux** ■ **tru64** ■ **aix**
Category	Use this search filter to search for policies with the following policy categories: ■ **allcategories** Use this category to search for **detection** and **prevention** policies. ■ **detection** ■ **prevention**
Instance	Use this search filter to search for policies that are applied on instances. Following instance options are available: ■ **workspace** ■ **applied** ■ **allinstance** Use this category to search for **workspace** and **applied** policy instances.
Status	Use this search filter to search for policies that are applied with the following status: ■ **active** ■ **archived** ■ **allstatus** Use this category to search for policies with **active** and **archived** status.

Table 4-4 Policy viewer search filters *(continued)*

Search filter	Description
Time Frame	Use this search filter to search for policies that are applied with the following time frame: ■ **alltime** Use this category to search for policies with **day**, **week**, **week**, and **month** time frames. ■ **day** ■ **week** ■ **month**
Version	Use this search filter to search for policies that are applied for the following versions: ■ **allversions** Use this category to search for policies with **V5.1** and **V5.2** versions. ■ **V5.1** ■ **V5.2**
Resource Type	Use this search filter to search for policies that are applied for the following resource types: ■ **file** ■ **registry** ■ **network** ■ **memory** ■ **process** ■ **user** ■ **group** ■ **disabled** ■ **logging** ■ **login** ■ **logMon** ■ **allresources** Use this category to search for policies with all resource types.

See "About policy viewer" on page 117.

Policy viewer display attributes

Once you have decided on the policies you want to search, you can determine how the display of results through the display attributes.

Table 4-5 shows the available display attributes with the description.

Table 4-5 Policy viewer display attributes

Attribute	Description
Data Detail	Enables you to view the policies either with details or without details. Following are the data detail options: ■ **nodetail** ■ **detail**
Content Display	Following are the content display options: ■ **current** ■ **allviews** ■ **baseline** ■ **summary** ■ **wschanges** ■ **allchanges**
Content Hidden	Following are the content hidden options: ■ **nohidden** ■ **hidden**
Symbol	Following are the symbol options: ■ **symbols1** ■ **nosymbols**
Header	Following are the header options: ■ **header** ■ **noheader**
Footer	Following are the footer options: ■ **nofooter** ■ **footer**

Table 4-5 Policy viewer display attributes *(continued)*

<table>
<tr><th>Attribute</th><th>Description</th></tr>
<tr><td><b>Indent Style</b></td><td>Following are the indent style options:
■ |---|---|
■ <b>periods</b>
■ <b>spaces</b>
■ <b>underscores</b>
■ <b>noindent</b></td></tr>
</table>

Note: By placing multiple items that conflict each other from the same category such as **baseline** and **summary**, or **hidden** and **nohidden** may produce unwanted results.

See "About policy viewer" on page 117.

Policy Summary information

The **Policy Summary** section in the policy viewer displays the results of your search.

Table 4-6 shows the summary information that is displayed.

Table 4-6 Summary information

Summary	Description
Policy ID	This number identifies the policy uniquely.
Item Status	For policies, the value is either Start or End. For an option, it is either On or Off. Blank items are lists, with values.
Item Description	For a policy or an option, the text that is displayed in the Console. For lists, each value in the list has its own line.
Bread Crumbs	The path on the option tree where the item or policy was found.

See "About policy viewer" on page 117.

Advanced settings for SQL stored procedure

The policy viewer uses an SQL stored procedure. You can use the viewer to determine the argument parameters that you need to extract policy information. Once you have the parameters you want, you can copy and paste the SQL statement. You can use the statement to extract information instead of the policy viewer user interface. You can also use the information to modify the SQL string to add columns or to do additional filtering or sorting.

Table 4-7 shows the table structure that is used in the SQL procedure. You can use this information to modify the SQL string to add columns or to do additional filter operation or sort operation.

Table 4-7 Advanced settings table structure

Column name	Datatype
PolicyID	int
RID	int
SEQ	int
ELEMENTRID	int
LEVEL	int
BASETYPE	varchar(16)
SETID	char(1)
OPTNAME	nvarchar(128)
OPTTYPE	varchar(63)
STATE	bit default 1
READONLY	bit default 0
HIDDEN	bit default 0
OPTVAL	nvarchar(1024)
OPTPROCESS	nvarchar(260)
OPTARGUMENTS	nvarchar(1024)
OPTUSERNAME	nvarchar(128)
OPTGROUPNAME	nvarchar(128)

Table 4-7 Advanced settings table structure *(continued)*

Column name	Datatype
OPTTIMEZONE	nvarchar(10)
OPTRULE	nvarchar(64)
OPTINFO	nvarchar(128)
OPTDESC	nvarchar(2048)
DELETED	bit default 0
BASESTATE	bit default 1
TypeID	nvarchar(128)
ControlID	int
OptLocalPort	nvarchar(128)
OptRemotePor	nvarchar(128)
OptRemoteIp	nvarchar(128)
OptGenVal1	nvarchar(256)
OptProtocol	nvarchar(128)
OptAction	nvarchar(128)
OptIdx	Int
OptLog	nvarchar(128)
PolicyTime	datetime
AppliedTime	datetime
AppliedPath	nvarchar(512)
WsPolicyName	nvarchar(128)
WSPath	nvarchar(512)
WSCreateTime	datetime
WSModTime	datetime
WSRevision	varchar(16)
WSRID	int

Table 4-7 Advanced settings table structure *(continued)*

Column name	Datatype
OSTYPE	nvarchar(64)
AgentVersion	varchar(16)
PolicyType	nvarchar(64)
ElementType	varchar(16)
CompiledPolicyName	nvarchar(128)
CompiledPath	nvarchar(512)
CompiledCreatetime	datetime
CompiledRevision	varchar(16)
BaseLineView	varchar(3)
SettingsView	varchar(3)
SummaryView	varchar(3)
WSChangesView	null
ChangesView	varchar(3)
TreePath	varchar(128)
BreadCrumbs	nvarchar(2048)
ParentNode	int

See “About policy viewer” on page 117.

Chapter 5

Managing configurations

This chapter includes the following topics:

About configurations

Configurations specify how agents operate. Symantec Critical System Protection uses common, prevention, and detection configurations.

About common configurations

Common configurations control how agents communicate with the management server.

Common configurations comprise the following parameters:

- Communication parameters
  - Polling interval

  - Enable real-time notification
  - Connection timeout
- Logging parameters
  - Enable log consolidation
  - Enable log rotation
  - Enable bulk log transfer
  - Delete log files after processing
  - Stop and restart logging at disk usage (%)
  - Reader and writer limits

Polling interval

The polling interval is the frequency at which an agent polls the management server for configuration changes. Polling is the most reliable method for agents to obtain configuration changes.

An agent learns of changes to its configuration in the following ways:

- During system startup, the agent queries the management server for configuration changes. This ensures that the agent immediately applies any changes made while the agent was shut down or disconnected from the network.
- The agent uses the polling interval to periodically poll the management server for configuration changes. In extremely large deployments (over 100,000 computers), you might need to increase the polling interval.

  The polling interval also controls how often an agent updates its policy state information (indicated by the shield icon) and how often an agent performs disk space monitoring.

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. The agent uses a port that you specify to communicate with the management server.

By default, real-time notification is enabled. 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.

Connection timeout

The connection timeout is the TCP/IP connection timeout for connections initiated by the agent to the management server. While the agent is waiting for a connection to time-out, it suspends some activities, including responding to policy override requests, which are made using the policy override tool. Increasing the connection timeout may improve agent connectivity with the management server on slow or congested networks. However, it can also cause the policy override tool to time-out while waiting for the agent to respond to the override request.

See the *Symantec Critical System Protection Agent Guide for* instructions on how to use the policy override tool.

Enable log consolidation

Log consolidation controls when an agent consolidates similar log events into a summary event that is sent to the management server. Similar log events that occur consecutively, within a user-specified summary delay period (for example, one minute), are consolidated into a summary event. The summary event includes a count of the number of similar log event occurrences.

Log consolidation only occurs for prevention events.

For similar log events to be consolidated, the following fields in each event must match:

- Severity code
- Event type
- Process ID
- Process name
- Disposition

Enable log rotation

Log rotation determines how and when agents rotate event log files.

When an agent rotates a log file, the current log file is closed and nothing more is written to it. A new log file is opened with the same base file name, but with the next highest sequence number added to the file name. Once a log file is rotated, the old file might still be in use by the agent. Although no new records are written to the log file, the agent might still have to process events and send them to the management server.

Log files are compressed into .zip files when processing is finished.

The frequency at which agents rotate log files is based on one of the following parameters:

- File size
  Agents can rotate log files based on log file size (in MB). When a log file reaches the size that you specify, a new log file is started.
- Time interval
  You can rotate log files based on the following time intervals:

Monthly

The numerical day of the month to rotate log files.

Examples: 1, 2, 3, 4, etc.

Weekly

The day of the week to rotate log files.

Examples: Sunday, Monday, Tuesday, etc.

Daily

The time of day (on the hour) to rotate log files.

Examples: Midnight, 1:00 A.M., 2:00 A.M., 3:00 A.M., etc.

Hourly

The hour intervals to rotate log files are as follows:

- On the hour
- 15 minutes past the hour
- 30 minutes past the hour
- 45 minutes past the hour

Enable bulk log transfer

Bulk log transfer collects events of long-term interest, without burdening the network or flooding the Symantec Critical System Protection database with events that have no immediate reporting or actionable purpose. Events of long term interest are generally used for audit or forensic analysis needs.

Table 5-1 lists the high-level steps for configuring bulk log transfer.

Table 5-1 Bulk log transfer steps

Step	Action	Description
1	Enable bulk log transfer in the agent's common configuration	Enable the Enable Bulk Log Transfer option in the agent's common configuration, on the Configs page. When full, the agent's log file is transmitted to the management server, where it is stored.

Table 5-1 Bulk log transfer steps *(continued)*

Step	Action	Description
2	Enable or disable deleting the transmitted bulk log files	If you disable the Delete Log Files After Processing option in the agent's common configuration, then the agent log files that were successfully transmitted to the management server for bulk log storage are copied to the following archive folder: C:\Program Files\Symantec\Critical System Protection\Agent\scsplog\archive If you enable the Delete Log Files After Processing option, then the agent log files that were successfully transmitted to the management server for bulk log storage are deleted. See "Delete log files after processing" on page 158.
3	Configure the agent's log rules for bulk logging	When configuring the agent's log rules, set the Transmit Action to Bulk Log Only. You access the agent's log rules from the Configs page. The agent has prevention log rules and detection log rules, which you configure separately. See "About prevention configurations" on page 159. See "About detection configurations" on page 160.
4	Verify bulk logging	Verify that the agent log files are being transmitted to the management server for storage. Search the Monitors page. Look for events of type Agent Status, with the operation Bulk Log Transfer. The name of the compressed log file appears in the event message.
5	Load the bulk log events	To view bulk log events in the management console, you must load the events into the Symantec Critical System Protection database. To load the events, you run the Bulk Loader utility. You do not need to load bulk log events until you are ready to view them. See "Loading bulk log events into the management server database" on page 260.

When an agent is configured for bulk log transfer, the following processing occurs:

- The event log files that are waiting to be uploaded for bulk logging are copied to the upload folder in C:\Program Files\Symantec\Critical System Protection\Agent\scsplog\upload.
- The bulk file name format is YYYYMMDD_HHMMSS_QQQQ-FT_HOSTNAME. QQQQ is a sequence number, F is a file type, T is the OS type, and Hostname is the agent name, host name, or IP address.
- To verify that the upload for bulk logging occurred, search the Monitors page in the management console. Look for events of type Agent Status, with operation Bulk Log Transfer. The name of the compressed log file appears in the event message.
- If the delete flag is set to false, files that were successfully uploaded for bulk logging are copied to the archive folder in C:\Program Files\Symantec\Critical System Protection\Agent\scsplog\archive.
- You must run the bulk loader utility to load bulk log events into management server database.
- Bulk file transmission does not block ongoing agent activities such as filtering, real-time event transmission, or update processing.
- By default, bulk log transfer is disabled for an agent.

Delete log files after processing

Delete log files after processing deletes an event log file after Symantec Critical System Protection reads the events in the file. If an agent is configured to transfer event logs to the management server, the deletion occurs after the transfer is successful.

By default, delete log files after processing is disabled.

Stop/restart logging at disk usage

The agent monitors the used disk space on the disk that contains the logs, to avoid filling the disk completely. The agent checks the percentage of used disk space at each polling interval. If the percentage of used disk space exceeds the configured stop-logging threshold, the agent stops logging events to the log files. Logging remains off until the percentage of used disk space drops below the configured start-logging threshold. At that point, the agent restarts logging events to the log files. When stopping or restarting logging, the agent generates a log message that appears on the Monitors page.

The stop-logging threshold must be at least five percent greater than the restart-logging threshold.

You can change the stop-logging and restart-logging thresholds using the agent config tool (sisipsconfig.exe).

Reader/writer limits

The reader limit and writer limit control how the agent processes events that are sent to the Monitors page.

The reader limit is the maximum number of events processed before the agent pauses. By pausing after a specified number of events, the agent avoids consuming too many system resources. Increasing the reader limit lets the agent consume more resources, but gets events to the Monitors page more quickly. Decreasing the reader limit reduces the resources that the agent consumes, but gets events to the Monitors page more slowly.

The writer limit is the maximum number of events that the agent can send in a single TCP/IP connection. Creating a TCP/IP connection is overhead, and sending multiple events in a single connection reduces the average overhead per event.

About prevention configurations

Prevention configurations comprise log rules. You use log rules to configure the transmission of events that agents send to the management server.

Log rules comprise the following:

- Filter rules
- Transmit action

You use the log rule editor to specify filter rules and a transmit action.

About filter rules

Each filter rule comprises <field, operator, value>. You can configure multiple filter rules for each log rule. Events must match all filter rules.

Please note the following when configuring filter rules:

- Examples of valid fields include event type, event severity, event date, disposition, event priority, process, user name, remote IP.
- Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.

- Not all operators are valid for all fields. For example, greater than and less than only make sense for numeric fields.
- The equals/not equals operator supports the wildcard character asterisk (*) for zero or more characters, and the wildcard character question mark (?) for a single character.
- The in/not in operator allows multi-select for fields with drop-down lists of possible values. For fields that have free-form text entry, the operator accepts a comma-separated list (no wildcard character support).
- Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.
- You can use Event Value1 through Event Value26 to specify additional fields in an event.
- Ordering is significant in log rules. Events are matched against log rules from top to bottom. The agent uses the transmit action of the first log rule that matches the event. If the transmit action is transmit in real-time, the agent sends the event to the management server. If the transmit action is bulk log only, the agent does not send the event. If the event does not match any of the log rules, the event is ignored.
- There is an implicit bulk-log-only default rule. A prevention configuration with zero log rules implies that all events are transmitted in bulk log only.

About transmit actions

The transmit actions are as follows:

Transmit in real-time	Real-time events are actionable events that are transmitted to the management server for storage in the Symantec Critical System Protection database.
Bulk log only	Bulk log events are events of long-term interest that have no immediate reporting or actionable purpose. Bulk log events are recorded in log files on the agent computer. When full, the log files are compressed and transferred to the management server for storage. Bulk log events are loaded into the management server database using the bulk loader utility. The events are loaded into the analysis event table (the default) or the real-time event table.

About detection configurations

Detection configurations comprise the following parameters:

- Parameters that control how the detection features of an agent operate. These parameters include the following:
    - File collector
    - Event log collector
    - Audit collector
    - Registry collector
    - Syslog collector
    - WTMP collector
    - BTMP collector
    - C2 collector
- Log rules

Parameters that control how detection features operate

Symantec Critical System Protection includes collectors that watch for changes to files, registry keys, event logs, and audit logs.

File collector

The file collector determines how agents monitor files. Intruders often attempt to replace critical system files with Trojan horse versions, or alter system files to create a back door for future intrusions. The file collector detects changes to these system critical files.

The file collector is valid for agents that are installed on supported Windows and UNIX operating systems. By default, the file collector is enabled.

On Windows operating systems, the file collector is a real-time collector.

On Windows, the file collector monitors the following file attributes:

- Create date
- Modified date
- Read-only
- Hidden
- System
- Size
- Compression

- Encryption
- Temporary
- Index service

On UNIX operating systems, file monitoring is implemented as polling. When you add a file to the filewatch list, you can specify a priority level of Normal or High. Files with Normal priority are polled for changes on the long poll interval. Files with the High priority are polled for changes on the short poll interval.

On UNIX operating systems, the file collector monitors the following attributes:

- Size
- Owner ID
- Group ID
- Permissions
- Number of hard links
- Access time
- Modified time

On UNIX operating systems, if a filewatch entry corresponds to a symbolic link or contains a wildcard character that expands to include a symbolic link, the file to which the link points is monitored.

You can monitor additional files by adding the files to a filewatch list. When the file tampering policy is applied to an agent, the filewatch list detects and reports when an agent computer file is added, deleted, modified, or renamed.

See the *Symantec Critical System Protection Detection Policy Reference Guide* for information on the file tampering policy.

Agents can determine if a file in the filewatch list was changed while the agent was shut down. At agent shutdown, all associated attributes of all watched files are written to a file on the agent computer. When the agent restarts, the attributes' state is compared to the attributes in this file. If a modified attribute is detected, an event is recorded.

Agents use the following settings to determine how to monitor files:

Monitor Last Access Time

The file collector monitors a file's last access time in addition to the file attributes.

A file's last access time is checked at agent startup to determine whether the file was modified since Symantec Critical System Protection was last shut down.

This parameter monitors the following:

- Access time changes (indicating that a file was read)
- Non-content related bit settings on Windows: Archive, Offline, Read-only, Reparse-point, Sparse File, Temporary, Indexed

Changes to this parameter require agents to be restarted.

Monitor File Checksums

The file collector computes checksums to determine whether a file has changed.

Changes to this parameter require agents to be restarted.

Search Depth

If you use a wildcard character at the end of a path in the file collector list, the recursion level determines how many directory levels are watched.

Select one of the following recursion levels:

- Recursion level 1 causes the collector to monitor all files in a specified directory.
- Recursion level 2 causes the collector to monitor all files in a specified directory and in the sub-directories of that directory.
- Recursion levels 3, 4, and 5 add additional levels of sub-directory monitoring.

Symantec Critical System Protection does not watch all levels below a specified directory to avoid severe impact on system performance.

Changes to this parameter require agents to be restarted.

High Priority Polling Interval

The high-priority polling interval, in seconds.

Files with the high priority are polled for changes on the short poll interval.

Normal Priority Polling Interval

The normal-priority polling interval, in minutes.

Files with normal priority are polled for changes on the long poll interval.

Event log collector

The event log collector looks for matches in the Windows event log. By default, the event log collector is enabled.

Audit collector

The audit collector monitors events from Windows standard system audit logs.

The system audit log sources in Windows are as follows:

- Security
- Application
- System

By default, the audit collector is enabled.

Registry collector

The registry collector watches for changes made to registry keys on the Windows operating system. By default, the registry collector is enabled.

Syslog collector

The syslog collector watches for syslog daemon tampering on UNIX-based operating systems. By default, the syslog collector is enabled.

WTMP collector

The WTMP collector monitors the WTMP logging system on UNIX-based operating systems. By default, the WTMP collector is enabled.

BTMP collector

The BTMP collector monitors the BTMP logging system on UNIX-based operating systems. By default, the BTMP collector is enabled.

C2 collector

The C2 collector monitors the C2 audit logging system on Solaris, Linux, HP-UX, and AIX operating systems. By default, the C2 collector is disabled. When the C2 collector is enabled, the agent automatically transmits C2 log events to the management server.

Log rules

You use log rules to configure and control the transmission of events that an agent sends to the management server.

You configure detection log rules in the same way that you configure prevention log rules.

See “About prevention configurations” on page 159.

Viewing the Configs page

You use the Configs page in the management console to manage the configurations that you apply to agents and configuration groups.

You can do the following activities from the Configs page:

- Create and edit common, prevention, and detection configurations
- Organize configurations in folders
- Apply and reapply configurations to agents and configuration groups
- Copy, rename, and delete configurations
- Import and export configurations

To view the Configs page

1. In the management console, click **Configs**.
2. Under the **Configs** tab, select any view.
3. On the Configs page, in the Configs pane, click the **Symantec** folder to list the Symantec default configurations.
4. (Optional) To restrict or expand the configuration list, in the Filters tree pane, select one of the following filters:

All Configs	Filter that displays all configurations.
Common Parameters	Filter that displays common configurations.
Prevention Parameters	Filter that displays prevention configurations.
Detection Parameters	Filter that displays detection configurations.

5. (Optional) To expand or collapse the panes, click the size arrows.

Setting up your configuration workspace

Your configuration workspace is where you store the configurations that you apply to agents and configuration groups.

Upon initial installation of Symantec Critical System Protection, your configuration workspace is automatically populated with the Symantec default configurations.

You can also populate your configuration workspace with the following configurations:

- Configurations that you created based on modifications to the Symantec default configurations
- Configurations that you obtained from other Symantec Critical System Protection administrators

Creating a common configuration

All agents use common configurations.

See "About common configurations" on page 153.

To create a common configuration

1. In the management console, click **Configs**.
2. Under the Configs tab, click **Prevention** or **Detection**.
3. On the Configs page, in the Configs tree, select the folder where you want to store the new configuration, and then right-click **New Config**.
4. In the **New Config Wizard** dialog box, click the **Common Parameters** icon.
5. In the **New Config Wizard** dialog box, in the Name box, type a name for the new configuration, and then click **Finish**.
6. (Optional) Change the default settings for the common configuration.

Creating a prevention configuration

Agents that support prevention features use prevention configurations.

See "About prevention configurations" on page 159.

To create a prevention configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention**.
3. On the Configs page, in the Configs tree, select the folder where you want to store the new configuration, and then right-click **New Config**.
4. In the **New Config Wizard** dialog box, click the **Prevention Parameters** icon.
5. In the **Name** box, type a name for the new configuration, and then click **Finish**.
6. (Optional) Change the default settings for the prevention configuration.

Creating a detection configuration

Agents that support detection features use detection configurations.

See “About detection configurations” on page 160.

To create a detection configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Detection**.
3. On the Configs page, in the Configs tree, select the folder where you want to store the new configuration, and then right-click **New Config**.
4. In the **New Config Wizard** dialog box, click the **Detection Parameters** icon.
5. In the **Name** box, type a name for the new configuration.
6. Click **Finish**.
7. (Optional) Change the default settings for the detection configuration.

Editing a workspace configuration

Modifications to common, prevention, and detection configurations are saved in your configuration workspace. The modifications are not automatically applied to the agents and configuration groups that use the configuration. You must manually reapply the configuration to the agents and configuration groups to take advantage of the modifications.

To edit a workspace configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, select a configuration, and then right-click **Properties**.
4. In the properties dialog box, edit or view the settings for a common, prevention, or detection configuration.
5. Click **OK** to save your changes.
6. (Optional) Reapply the modified configuration to agents and groups.

See “About common configurations” on page 153.

See “About prevention configurations” on page 159.

See “About detection configurations” on page 160.

Renaming a workspace configuration

You can rename workspace configurations.

To rename a configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, in the Configs workspace pane, select a configuration, and then right-click **Rename Config**.
4. Type a new name for the configuration, and then press Enter.

Copying a workspace configuration

Copying a configuration creates a copy of the configuration. The copy is saved in the same configuration folder as the original configuration. The copy name is prefixed with Copy_of followed by the original configuration name (for example, Copy_of_Common_Parameters).

To copy a workspace configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, navigate to and select the configuration that you want to copy, and then right-click **Copy Config**.

Deleting a workspace configuration

You can delete workspace configurations.

To delete a workspace configuration

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, navigate to and select the configuration that you want to delete, and then right-click **Delete Config**.
4. In the **Confirm Deletion** dialog box, click **Yes**.

Creating a configuration folder

You use folders to organize the configurations that you apply to agents. You might use configuration folders to store configurations of like types (for example, a folder for common configurations, another folder for prevention configurations).

There is no limit to the number of configuration folders that you can create. You can create nested configuration folders within other folders.

Create configuration folders so that you can edit the configurations efficiently. Name configuration folders so that you can easily identify which configurations to assign to the folders.

To create a configuration folder

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, in the Configs tree, select the default Configs folder or another folder, and then right-click **New Folder**.

   A new configuration folder is created with the name New Folder.
4. Rename the configuration folder, and then press the **Enter** key.

Moving a workspace configuration to a folder

You move configurations to folders using the following methods:

- Drag-and-drop operation
  You can move a configuration from one folder to another folder in a drag-and-drop operation. In the Workspace pane, select a configuration, and then drag it to the desired folder in the Configs tree.
- Move To command
  You can move a configuration from one folder to another folder using the Move To command. In the Workspace pane, select a configuration, and then right-click **Move To**. In the Move Folder dialog, select the folder to receive the configuration, and then click **Move To**.

Applying and reapplying workspace configurations

You use the Apply Config command to apply a workspace configuration to agents and configuration groups that do not currently use the configuration.

You use the Reapply Config command to reapply a workspace configuration to agents and configuration groups that currently use the configuration. The Reapply Configuration command is useful when you need to reapply a workspace configuration that was modified.

Applying a workspace configuration to an agent or group

When applying a configuration, you are prompted to select the agents and configuration groups that will use the configuration.

To apply a configuration to an agent or group

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, select the configuration that you want to apply, and then right-click **Apply Config**.
4. In the **Apply Configuration** dialog box, select the agents and configuration groups to which you want to apply the selected configuration, and then click **Apply.**

   To select multiple agents and groups, hold down the Ctrl key while making your selection.
5. In the management console, click **Refresh** to update the management console page.

   Refreshing the page lets you confirm that the agents successfully processed the configuration changes.

Reapplying a workspace configuration to an agent or group

When reapplying a configuration, you are presented with a list of agents and configuration groups that currently use the configuration. You can reapply the configuration to some or all of those agents and groups.

To reapply a configuration to an agent or group

1. In the management console, click **Configs**.
2. Under the **Configs** tab, click **Prevention** or **Detection**.
3. On the Configs page, select the configuration that you want to reapply, and then right-click **Reapply Config**.

4 In the **Reapply Configuration** dialog box, select the agents and configuration groups to which you want to reapply the selected configuration, and then click **Reapply.**

To select multiple agents and groups, hold down the Ctrl key while making your selection.

5 In the management console, click **Refresh** to update the management console page.

Refreshing the page lets you confirm that the agents successfully processed the configuration changes.

Importing configurations

You can import configurations that you or another Symantec Critical System Protection administrator exported.

To import configurations

1 In the management console, click **Configs**.

2 Under the **Configs** tab, click **Prevention** or **Detection**.

3 On the Configs page, in the Configs tree, select the folder to which you want to import the configurations, and then right-click **Import Config**.

4 In the **Import** dialog box, browse to the configuration .zip file, and then click **Import**.

In the **Import** dialog box, each successfully imported configuration is marked with a green check mark.

5 In the **Import** dialog box, click **Close**.

Exporting configurations

You can export configurations to .zip files. Exporting configurations is useful for sharing your configurations with other Symantec Critical System Protection administrators.

To export configurations

1 In the management console, click **Configs**.

2 Under the **Configs** tab, click **Prevention** or **Detection**.

3 On the Configs page, navigate to and select the configurations that you want to export, and then right-click **Export Config**.

To select multiple configurations, hold down the Ctrl key while selecting the configurations.

4 In the **Export** dialog box, browse to the folder where you want to export the configurations.

5 In the **Export** dialog box, in the File Name box, type a name for the export .zip file, and then click **Export**.

The selected configurations are exported to the .zip file, using the file name that you specified. In the Export dialog, each successfully exported configuration is marked with a green check mark.

6 In the **Export** dialog box, click **Close**.

Chapter 6

Viewing events

This chapter includes the following topics:

About events

Events are informative, notable, and critical activities that concern the Symantec Critical System Protection agent and management server. The agent logs events to the management server, and the management console lets you view summaries and details of those events.

An agent's log rules determine which events are sent to the management server.

You can use the Home page in the management console to obtain an overview of events that are being generated in your network.

You can use the Symantec Critical System Protection agent event viewer to display recent events that were reported by a Symantec Critical System Protection agent.

See the *Symantec Critical System Protection Agent Guide*.

About event sources

Symantec Critical System Protection events originate from the following sources:

Agent

The agent transmits events to the management server. Agent-transmitted events are loaded into the CSPEVENT table by default. Agent-transmitted events include events reported by Symantec Critical System Protection native agents and virtual agents.

Bulk loader utility

The bulk loader utility loads events into the ANALYSIS_EVENT table by default. No other mechanism exists to load events into this table.

Management server

Server operations generate server-related events. Server-related events are only loaded into the CSPEVENT table.

About event categories

The Monitors page groups events by the following categories:

All Events

All prevention and detection events.

Prevention

An agent's prevention policy generates prevention events when applications access computer and network resources that violate the policy's behavior control.

Detection

An agent's detection policy generates detection events when monitored files or registry keys change, or when system or application logs generate events that match the policy's criteria.

Management

An agent records management events that are related to the agent's configuration and communication status.

Profile

An agent's prevention policy generates profile events when a process is profiled.

File Catalog

An agent records file catalog events that acknowledge the following activities:

- Successful event log rollover
- Successful storage of log files in the agent repository in the management server during bulk log transfer

Analysis	Analysis events comprise the events that were transferred to the management server using bulk log transfer and then loaded into the database. Analysis events are of long-term interest, generally for audit or forensic analysis needs.
Audit	The management server records audit events whenever changes to the system configuration are made. Optionally, the management server can record audit events whenever searches, queries, or reports are executed. See "About the Audit settings" on page 248.

About event types

Symantec Critical System Protection groups events by types.

Prevention event types

Prevention event types are as follows:

Buffer Overflow	Contains information about applications that execute code that was inserted using buffer overflows. Buffer overflow events apply to agent computers that run Windows operating system.
File Access	Contains information about applications that access files and directories.
Mount	Contains information about applications that mount or unmount file systems.
Network Access	Contains information about applications that access the TCP/IP network.
OS Call	Contains information about applications that make selected operating system calls that are often exploited by attackers.
Process Access	Contains information about the process modification or process access.
Process Set	Contains information about the assignment of a process to a process set.
Process Create	Contains information about the creation of a process.
Process Destroy	Contains information about the termination of a process.
Registry Access	Contains information about applications that access registry keys.

Detection event types

Detection event types are as follows:

Audit Watch

Contains information about audit watch events.

Event categories: detection

Filewatch

Contains information about filewatch events for Windows and UNIX operating systems.

Event categories: detection

Generic Log

Contains information about generic log events.

Event categories: detection

NT Event Log

Contains information about NT event log events.

Prevention Watch

Contains information about prevention watch events.

Registry Watch

Contains information about registry watch events.

Syslog

Contains information about syslog events.

UNIX C2 Log

Contains information about C2 events.

UNIX Activity Log

Contains information about WTMP events.

Management event types

Management event types are as follows:

Agent Status

Status messages from the IPS Service/daemon.

Communications

Contains information about communications between the agent and the management server.

Configuration

Contains information about agent configuration status.

IDS Error

Contains information about detection errors.

IDS Status

Contains information about detection status.

Event File Create

Contains information about a single event file from an agent.

Event File Receive

Contains information about files transferred to the bulk file repository on the Symantec Critical System Protection management server.

Event Storage Error

Contains information about database storage errors.

Policy Override	Contains information about users overriding policies on agents.
IPS Status	Status messages from the IPS Driver.

Profile event types

Profile event types are as follows:

Buffer Overflow	Contains information about applications that execute code that is inserted using buffer overflows.
File Access	Contains information about applications that access files and directories.
Mount	Contains information about applications that mount or unmount file systems. By default, these events do not appear on the Monitors page.
Network Access	Contains information about applications that access the TCP/IP network.
OS Call	Contains information about applications that make selected operating system calls that are often exploited by attackers.
Process Set	Contains information about the assignment of a process to a process set.
Process Create	Contains information about the creation of a process.
Process Destroy	Contains information about the termination of a process.
Registry Access	Contains information about applications that access registry keys.

File catalog event types

File Catalog events contain information about bulk log files that are stored in the management server repository.

Analysis event types

Analysis events comprise the events that were transferred to the management server using bulk log transfer and then loaded into the server database. Analysis events are of long-term interest, generally for audit or forensic analysis needs.

Audit event types

Audit events contain system audit information.

About event severity levels

Symantec Critical System Protection assigns a severity level to each event.

The event severity levels are as follows:

Info

Events with a severity of Info contain information about normal system operation.

Notice

Events with a severity of Notice contain information about normal system operation.

Warning

Events with a severity of Warning indicate unexpected activity or problems that have already been handled by Symantec Critical System Protection.

These Warning messages might indicate that a service or application on a target computer is functioning improperly with the applied policy. After investigating the policy violations, you can configure the policy and allow the service or application to access to the specific resources if necessary.

Major

Events with a severity of Major imply more impact than Warning and less impact than Critical.

Critical

Events with a severity of Critical indicate activity or problems that might require administrator intervention to correct.

About the System State event flag

The System State event flag indicates the state of processing characteristics when the event occurred. For example, the System State flag can indicate the prevention override/disabled state and whether the event was selected for real-time transmission. The System State flag can indicate the kind of event injection and the kind of source agent type.

The System State event flag contains a concatenated list of flags that are appropriate for a given event.

The System State event flags are as follows:

Event Processing States

- R: real-time event
- V: virtual event
- I: injected event

Prevention Policy States	■ P: prevention policy overridden completely ■ X: prevention policy overridden except for self-protection ■ G: policy globally disabled
Event Source States	■ T: ITA forwarded ■ C: CSP forwarded ■ D: collector derived ■ L: logwatch policy generated ■ F: Config tool generated ■ S: IPS Service generated
Other Event Attributes	■ Z: Solaris non-global zone event ■ M: SCSP Manager virtual agent (this flag only exists in the database, not the CSV file)

Note: Not all virtual events are injected events. Not all injected events are virtual events. All virtual and injected events must also specify an event source. The Solaris Zone flag indicates that the event processed came from a non-global zone.

Examples of System State flags are as follows:

- PR: real-time event, prevention policy overridden
- IS: injected IPS Service event
- VT: virtual ITA event
- D: derived event
- RZ: Solaris zone event
- RVDZ: virtual derived event from a Solaris non-global zone
- VIM: virtual injected event for the SCSP Manager.
  These events are injected by the server (such as service startup/shutdown, event purging, aggregated health events, etc.) and do not appear in any source CSV since there is no agent to collect them.

Viewing the Monitors page

You use the Monitors page in the management console to view events that are sent to the management server. The Monitors page displays event information reported to the management server from your entire agent deployment.

You can do the following activities from the Monitors page:

- View all events or categories of events.
- Use the Event Details command to view detailed information that pertains to a selected event.
  See “Using the Event Details command” on page 183.
- Create and display real-time monitors, for viewing events in real time.
  See “About real-time monitors” on page 189.
- Use the Event Wizard to resolve events.
  See “Using the Event Wizard command” on page 184.
- Export events to comma-separated value (.csv) files.
  See “Exporting events” on page 193.

Symantec Critical System Protection preserves the Monitors page view for the current session of the management console. This feature lets you traverse between pages while maintaining the view settings for each page, which is useful when troubleshooting events. The next time that you log on to a new session of the management console, the Monitors page view is reset to its default settings.

To determine the number and age of the events that are displayed on the Monitors page and in real-time monitors, you set the Monitors preferences.

See “Setting the Monitors preferences” on page 181.

Note: All system date/time values are handled as Coordinated Universal Time (UTC). Some system date/time values that are shown in the management console are converted to the local time zone. Converted values are shown with the appropriate time zone values.

To view the Monitors page

1. In the management console, click **Monitors**.
2. On the Monitors page, in the **Monitors Types** pane, select an event category for viewing events.
3. To expand or restrict the list of events, in the **Filters** pane, select one of the following filters:

All Events	Filter that displays all the events.
The last 500 events	Filter that displays a subset of the last 500 events for a selected monitor type. For example, if you select the last 500 events and also select the Prevention monitor type, the Monitors page displays the subset of the last 500 events that are prevention events.
The last n hours	Filter that displays events that occurred in the last n hours. The number of hours is defined in the console preferences (View > Preferences). By default, this value is set to 2 days.
Within the last hour	Filter that displays the events that occurred in the last hour.
Past Day	Filter that displays the events that occurred during the past day.
Within the last week	Filter that displays the events that occurred with the last week.
Past Month	Filter that displays the events that occurred in the past month.
Within the past year	Filter that displays the events that occurred within the past year.

Setting the Monitors preferences

You use the Monitors preferences to set the number and age of events that are shown on the Monitors page.

See “Setting console preferences” on page 29.

Verifying the operation of an agent computer

You can verify the operation of an agent computer by viewing the events that were sent to the management server.

To verify the operation of an agent computer, search the Monitors page for event messages from the agent computer. Messages with a severity of Warning indicate unexpected activity or problems that were already handled by Symantec Critical System Protection. If a message has an event type of file access, network access, OS call, or buffer overflow, then a severity of Warning indicates abnormal application behavior that was stopped.

Even if the prevention policy is not enforcing prevention (that is, the disable prevention option is set), improper access to resources by a service or application will generate log messages. With the disable prevention option set, the disposition field in a log message will indicate allow instead of deny, and the event severity will appear on the Monitors page in blue instead of red.

After investigating these warning messages, you may find that Symantec Critical System Protection prevented an attempt to attack the agent computer or that the events do not reflect a risk condition on the system. In the latter case, you may want to further configure the policy so that it does not produce these events in the future.

Resolving events

You might need to adjust the Symantec Critical System Protection policies to resolve events that you see on the Monitors page.

The process of resolving events involves the following:

- You must decide whether to allow an event (in the case of prevention policies) or not log an event (in the case of detection policies).
- You must decide which policy modification strategy to use with an event (for example, add to a resource list, make a program privileged).
- You must decide which policy modification actions to perform (for example, enable or disable a policy option, add a value to a parameter list).
- You must decide which policies to modify.

To help you resolve events, Symantec Critical System Protection provides the following console features:

- Event Details
- Event Agent
- Event Policy
- Event Wizard

Using the Event Details command

You use the Event Details command to view detailed information that pertains to a selected event. The Event Details command displays a separate, resizable window that lets you quickly step through events, one event at a time, as the events are being sent to the management server. The Event Details window is tied to a selected event, so that when the Monitors page changes, the Event Details window also changes.

Please note the following about the Event Details command:

- You can display multiple Event Details windows. For example, you can display one Event Details window to monitor prevention events, and a second Event Details window to monitor detection events.
- You can display Event Details windows alongside other management console windows.
- You can invoke the Event Details command from the Monitors page (including real-time monitors), the Recent Events tab, and the History tab.
- You can copy events from the Event Details window to the Windows clipboard.
- You can invoke the Event Wizard command from the Event Details window.

To use the Event Details command

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, select an event, and then right-click **Event Details**.
4. In the Event Details window, click the **Next Event** and **Previous Event** icons to scroll events.
5. In the Event Details window, click the blue computer icon to show the agent that reported the selected event.
6. In the Event Details window, click the **Copy To Clipboard** icon to copy the details of the event that is currently displayed to the Windows clipboard.

Using the Event Agent command

You use the Event Agent command to show the agent that reported a selected event. The Event Agent command displays the properties of the agent that reported the event.

To use the Event Agent command

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.

3. On the Monitors page, select an event, and then right-click **Event Agent** to display the properties of the agent that reported the selected event.

   You can also invoke the Event Agent command by clicking the blue computer icon.

4. Click **OK**.

Using the Event Policy command

You use the Event Policy command to display a read-only version of the policy that caused a selected event. The Event Policy command displays the policy's current settings, changes made to the base policy, and changes made to the workspace policy.

You can invoke the Event Policy command from the Monitors page and the Recent Events tab.

The Event Policy command is not available for every type of event.

To use the Event Policy command

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, select an event, and then right-click **Event Policy** to display a read-only version of the policy settings.
4. Click **OK**.

Using the Event Wizard command

The Event Wizard offers a guided, interactive dialog that walks you through the policy adjustment process, from choosing a policy modification strategy to modifying a policy.

The Event Wizard walks you through the following choices:

- Which policy modification strategy to use with an event (for example, add to a resource list, make a program privileged)
- Which policy modification actions to perform
  The Event Wizard recommends actions to perform. You can disable any or all of the actions.

  The actions include the following:

  - Enable a policy option
  - Disable a policy option

- Add a value to a parameter list
  If a recommended action includes adding values to a parameter list (for example, a file path or network IP address), the Event Wizard lets you edit the values. You can convert an IP address into a subnet, or add wildcard characters to a file path.

- Which policies to modify
  You must browse your policy workspace and select the policies that you want to modify. The Event Wizard modifies workspace policies. It does not modify policies that are applied to agents and groups.

Examples of the options and parameters that the Event Wizard uses to configure policies for an agent computer are as follows:

Resource lists

You use resource lists to tailor the control of specific resources and define how they can be accessed by a service or interactive program. You can list file paths, registry paths, network ports, or IP addresses. The resource lists are provided at the global, group, and individual process set levels.

Applies to prevention policies

Alternate privilege lists

You use alternate privilege lists to change the privileges given to processes on an agent computer. You can apply alternate privilege lists to a service, interactive program, user, or user group. There are several reasons why you might change the privilege level of a user or program. For example, to give a user or group access to all resources on an agent computer, you would assign full privileges to the user or group. If a program is being denied access to multiple resources, you would increase the privilege level for the program.

Applies to prevention policies

Basic options

Basic options are provided at the individual level. These options are specific to the individual service or interactive program for which they are offered. Basic options provide configuration features specific to a service or interactive program. The prevention policies do not provide basic options for every individual program; they are only present when unique controls are necessary for a program.

Applies to prevention policies

Rule enable/disable

Each rule in a detection policy is controlled by its own option. If the option is enabled, the rule is enforced. If the option is disabled, the rule is not enforced.

Applies to detection policies

Exception lists	Some detection policies monitor a large set of files or registry settings. These files or registry settings often have associated exception (ignore) lists, so that you can easily configure monitoring an entire directory, while not monitoring one file in the directory that is noisy. Applies to detection policies

The Event Wizard walks you through a series of wizard pages. You follow each page by clicking Next or Back.

The Event Wizard remembers which workspace policy was last modified; it uses that policy as the default policy in subsequent invocations of the Event Wizard. If you modify multiple policies, the Event Wizard remembers the policies and selects them by default in subsequent invocations. This policy memory is retained for the current management console login session.

When using the Event Wizard, please note the following:

- You must manually apply the modified policies to agents and groups.
- If the modified policies do not work as intended, you can invoke the Event Wizard again and select another policy modification strategy.
- If you want to revert the policy modifications made by the Event Wizard, you must manually edit the policies.
- The Event Wizard is not available for use with every event. Use of the Event Wizard depends on the information contained in an event.
- You can launch the Event Wizard from the Monitors page (including real-time monitors), Event Details window, and the Recent Events tab.
- You can use the Event Policy command to view the policy that caused a selected event.

To use the Event Wizard command

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. In the events pane, select an event, and then right-click **Event Wizard**.

   You are presented with a list of policy modification strategies.
4. Click **Event Wizard** to display descriptions of the policy modification strategies.

5 In the **Event Wizard** dialog box, select a policy modification strategy, and then click **Next**.

You are presented with a list of actions to perform. The actions are prioritized, based on Symantec's recommendations, with the preferred actions presented first.

6 In the **Event Wizard** dialog box, disable the actions that you do not want to perform, and then click **Next**.

The Event Wizard automatically enables all actions. When an action is enabled, the Perform This Action check box is checked.

If an enabled action includes adding a value to a parameter list, type the value in the Value box.

To disable an action, clear the **Perform This Action** check box.

7 In the **Event Wizard** dialog box, select the workspace policies that you want to modify, and then click **Next**.

8 In the **Event Wizard** dialog box, click **Update** to modify the policies.

The Event Wizard shows progress and final status information about the actions that you applied. For policies that are updated successfully, you may enter comments and change the policy revision numbers.

Displaying text instructions for suppressing event transmission

The Event Wizard provides on-screen, step-by-step text instructions that explain how to suppress event transmission.

To display text instructions for suppressing event transmission

1 In the management console, click **Monitors**.

2 Under the **Monitors** tab, click **Events**.

3 In the events pane, select an event, right-click **Event Wizard**, and then select **How to suppress event transmission**.

To copy the on-screen text instructions to the Windows clipboard, select all the text in the Action Details pane, and then press Ctrl+C. You can paste the contents of the clipboard into a text document.

Searching events

The Monitors page includes a search function that you can use to search a broad or restricted range of events.

When using the search function, you can specify the following options:

Source Machine	The name and IP address of the agent that generated the event.
OS Type	The operating system of the agent computer that generated the event.
Event Category	The event category.
Event Type	The type of event.
Event Severity	The severity of the event.
Event ID	The event id.
A word or phrase in the Description	A word or phrase that is part of the summary information about the event. You can use an asterisk (*) as a wildcard character for this option.
When did the event occur?	The time frame in which the events occurred. The default setting is Don't remember.
Advanced options	You can use the advanced options to further expand or restrict the event search. Select one or more of the advanced options.
Save Query button	Click Save Query to save the search criteria as a tabular query that you can later run on the Reports page.

You can launch the Event Wizard from search results.

To search events

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, in the **Event Tasks** pane, click **Search Events**.
4. In the **Event Search** dialog box, specify the search criteria.

   The search criteria that you specify must match the events exactly. The only exceptions are resource (advanced options) and a word or phrase in the description. For these options, you can use an asterisk (*) as a wildcard character in the text string.
5. (Optional) To save the search criteria as a query, click **Save Query.**

   The **New Query Wizard** dialog box appears. Create a query using the search criteria that you specified.
6. In the **Event Search** dialog box, click **Search**.

   Events that match your search criteria are displayed in the **Event Search** dialog box, in the event pane.

About real-time monitors

You use real-time monitors to view events as they are sent in real time to the management server. Real-time monitors are useful for viewing recent events that you might have missed, and to aid in troubleshooting.

When using real-time monitors, please note the following:

- Newest events are listed first.
- You can create and view multiple real-time monitors. Shown as a separate, resizable window, each real-time monitor has its own filter rules and preferences. The All Events monitor, which displays all events, is the default real-time monitor.
- You can adjust policies for events in real-time monitors.
- You can use the Event Details command with real-time monitors.
- The following commands are available for use with real-time monitors:
  - Open Monitor
  - New Monitor
  - Copy Monitor
  - Import Monitor
  - Export Monitor
  - Refresh
  - Delete Monitor
  - Rename Monitor
  - Properties
- The real-time monitors that you create can be accessed by you and other users who share your management console login account (for example, the default symadmin account). If you do not want other users to access your real-time monitors, then log on to the management console using an account that you use exclusively, and create your real-time monitors.

Viewing a real-time monitor

You can open multiple real-time monitors simultaneously.

To view a real-time monitor

1. In the management console, click **Monitors**.
2. Under the **Mointors** tab, click **Events**.
3. On the Monitors page, in the **Real-Time Monitors** pane, select a monitor, and then right-click **Open Monitor**.

Creating a real-time monitor

You can create multiple real-time monitors. Each real-time monitor has its own filter rules and preferences.

To create a real-time monitor

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, in the **Real-Time Monitors** pane, click **New Monitor**.
4. In the New Real-Time Monitor dialog, on the **General** tab, type a name and description for the monitor.
5. Select **Include** or **Exclude** as the default action.
6. Click **OK**.

Adding a filter rule

A filter comprises rules that describe event criteria. When the filter rules match an event in a real-time monitor, the event is either included in or excluded from the real-time monitor. The rules in a filter are processed in the order in which they appear. Events must match all filter rules.

Each filter rule comprises <field, operator, value>.

When configuring filter rules, please note the following:

- Examples of valid fields include event type, event severity, event date, disposition, event priority, process, user name, remote IP.
- Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.
- Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.

To add a filter rule

1. On the Monitors page, select a real-time monitor, and then right-click **Properties**.
2. In the monitor properties dialog box, on the Filter Rules tab, click the **Add Rule** icon.
3. In the **Filter Rule Editor** dialog box, select **Include** or **Exclude**.
4. In the **Filter Rule Editor** dialog box, select <field, operator, value>, and then click **Add**.

   Repeat this step to add additional filter rules.
5. To edit an existing filter rule, edit <field, operator, value>, and then click **Update**.
6. Click **OK**.
7. In the monitor properties dialog box, select the **Default Action for Unmatched Events** (Include or Exclude).
8. Click **OK**.

Marking an event as read or unread

Event messages that appear in bold text are marked as unread; messages that appear in plain text are marked as read. You can use this feature to track recent events that you have not seen. You can use the feature to aid in troubleshooting; as you investigate and resolve problems, you can mark the corresponding events as read.

By default, new events are marked as unread.

To mark an event as read or unread

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, select a real-time monitor, and then right-click **Open Monitor**.
4. To mark an event as read, in the **Real-Time Event Monitor** dialog box, select the event, and then right-click **Mark as Read**.
5. To mark an event as unread, in the Real-Time Event Monitor, select the event, and then right-click **Mark as Unread**.

Searching events

You search events in real-time monitors just as you would search events on the Monitors page.

To search events

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, select a real-time monitor, and then right-click **Open Monitor**.
4. In the **Real-Time Event Monitor** dialog box, click the **Search Events** icon.

Removing an event from a real-time monitor

Events that you remove from real-time monitors are still visible on the Monitors page.

To remove an event from a real-time monitor

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, select a real-time monitor, and then right-click **Open Monitor**.
4. In the **Real-Time Event Monitor** dialog box, select an event, and then right-click **Remove**.

Importing a real-time monitor

You can import real-time monitors that you or another Symantec Critical System Protection administrator exported. Imported real-time monitors are owned by the user who imported them.

To import a real-time monitor

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Events**.
3. On the Monitors page, in the Real-Time Monitors pane, right-click **Import Monitor**.

   Right-click in the white space.

4 In the **Import** dialog box, browse to the real-time monitor .zip file that you want to import.

5 In the **Import** dialog box, click **Import**.

Exporting a real-time monitor

You can export real-time monitors that you own. The monitors are exported to .zip files.

To export a real-time monitor

1 In the management console, click **Monitors**.

2 Under the **Monitors** tab, click **Events**.

3 On the Monitors page, in the Real-Time Monitors pane, select a monitor, and then right-click **Export Monitor**.

4 In the **Export To** dialog box, specify the following information:

Look In	Select the location where you want to store the exported file.
File Name	Accept the default file name or type a new file name. By default, a real-time monitor is exported to a .zip file named [monitor_name].zip, where [monitor_name] is the name of the real-time monitor being exported.
Files of Type	Select Zip files.

5 In the **Export To** dialog box, click **Export**.

Exporting events

Symantec Critical System Protection offers the option to export events to a CSV file. You can view the comma-separated value (CSV) file by using a text editor or a spreadsheet program.

To export events

1 In the management console, click **Monitors**.

2 Under **Monitors** tab, click **Events**.

3 On the Monitors page, in the event pane, select the events that you want to export, and then click the **Export Events** icon.

To export multiple events, hold down the Shift or Ctrl key while you select the events. To export the current page or all pages, you need not select the events.

4 In the **Export To** dialog box, specify the following information:

Look In	Select the location where you want to store the .csv file.
Export range	Select one of the following options: ■ **All pages** – Export all events. Note that you must re-run the event search for each page that you want to export. If you export many events, you may get better performance by exporting the current page, even if the page contains many events. ■ **Current page** – Export the current page. ■ **Selected events** – Export the selected events.
File Name	Type the name of the .csv file.
Files of Type	Select CSV files.

5 Click **Export**.

Purging events

You can specify how long to retain real-time, profile, and analysis events in the Symantec Critical System Protection database.

See “About the Event Management settings” on page 248.

Managing queries and reports

This chapter includes the following topics:

Viewing the Reports page

You use the Reports page in the management console to create and run Symantec Critical System Protection queries and reports.

You can do the following activities from the Reports page:

- Run the Symantec predefined queries and reports
- Create and run custom queries and reports
- Publish the results from queries and reports
- Import and export queries and reports
- Organize queries and reports in folders
- Run LiveUpdate to download revisions to the Symantec queries and reports
  See "About updating Symantec policy and report packs" on page 48.

To view the Reports page

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports**.
3. On the Reports page, in the Reports pane, click the **Symantec** folder to list the Symantec reports.
4. (Optional) On the Reports page, click the size arrows to expand or collapse the panes on the Reports page.

To view the Queries page

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Queries**.
3. On the Queries page, in the Queries pane, click the **Symantec** folder to list the Symantec queries.

About the Symantec queries and reports

Symantec Critical System Protection includes over 75 predefined queries and reports that provide an overall view of your deployed environment, and prevention, detection, and management activity.

About the Symantec queries

The Symantec queries can help you identify groups with policies that provide no protection or only partial protection. The queries can help you identify agents that are disconnected from the network for a period of time or that are experiencing network connectivity issues.

The Symantec queries are grouped by the following categories:

Agent

Agent queries provide information about the following:

- Agent details, such as host name, IP address, agent version, asset network path, and OS version
- Agent counts based on OS type and version
- Offline agents that are not communicating with the management server
- Agents with no prevention policies or with overridden policies
- Counts of registered agents for each network path
- Duplicate agents

Event

Event queries provide information about agent, prevention, detection, and management events, including information about the following:

- Agent event counts for all agents
- Agent event counts by day, week, month
- Event counts grouped by disposition, event type, OS network
- Event severities
- Event types

Home Page

Home page queries provide information about agent and event statistics for the console views, including information about the following:

- Agents with errors
- Agents that are offline
- Agents with configurations pending
- Agents with policies pending

Policy

Policy queries provide information about policy attributes. Policy queries include a glossary of all process sets and operating systems.

Security

Security queries provide information about the following:

- Audit detail records by date/time
- Audit detail records for failed logins
- Users, roles, last login dates

Status

Status queries provide information about the following:

- Event statistics
- Symantec Critical System Protection objects by name and type
- System statistics

The Symantec queries are stored in the Symantec folder. The folder name includes the date that Symantec released the queries. To check for and download new releases, run LiveUpdate.

See "About updating Symantec policy and report packs" on page 48.

You can use the Symantec queries as the basis for custom query development.

To view a description of a Symantec query, select the query, and then right-click Properties.

About the Symantec reports

The Symantec reports include the following samples, which illustrate how the report feature works:

- The Last Week Event Charts report displays statistics about the previous week's events. The report uses the following Symantec event queries:
  - Event Counts By Day (weekly)
  - Top 10 Processes (weekly)
  - Top 10 Event Types (weekly)
  - Event Severities (weekly)
- The Recent Event Summary is a two-page report that summarizes the number of events and corresponding event types. Page one shows the data for the last month; page two shows the data for the last week.
  The report uses the following Symantec event queries:
  - Event Counts by Day (weekly, monthly)
  - Top 10 Event Types (weekly, monthly)

The Symantec reports are stored in the Symantec folder. The folder name includes the date that Symantec released the reports. To check for and download new releases, run LiveUpdate.

See "About updating Symantec policy and report packs" on page 48.

To view a description of a Symantec report, select the report, and then right-click Properties.

Managing queries

A query is a request for information from the Symantec Critical System Protection management server database.

Running a query

The results from running a query appear in a tab in the Report Results pane. Each time you run a query, another tab appears.

To run a query

1. In the management console, click **Reports**.
2. Under the **Report** tab, click **Queries**.
3. On the Queries page, in the Queries pane, select a query, and then right-click **Run Query**.
4. If the query prompts for input parameters, specify the parameter values, and then click **Run query**.
5. (Optional) Publish the results from running the query.

   See "Publishing a query or report" on page 212.
6. When you no longer need the query results, in the Report Results pane, click the query tab, and then click the green **X** icon to close the query results.

   To recover the query results, rerun the query.

Exporting query results to multiple file formats

You can export query results to a CSV, HTML, or PDF file.

To export query results to multiple file formats

1. Run the query.
2. In the **Report Results** pane, click the **query results** tab to make it the active tab.
3. Click the **Export Results** icon.
4. In the **Export To** dialog box, specify the following information:

Look In	Select the location where you want to store the file.
Export range	Select the export range. ■ For tabular queries, specify the export range (**All pages**, **Current page**, **Selected rows**). ■ For queries with images, specify the export range (**All pages**, **Current page**).
File Name	Type the name of the file you want to export.
Files of Type	Select the file format such as CSV, HTML, or PDF. **Note:** You can export the query output with images to a JPEG, HTML, or PDF file.

5. Click **Export**.

6. For the HTML and PDF file formats, type **Export Title** in the **Export** dialog box.

   The export title appears on the top-left corner of the query file that you export.

7. Click **OK**.

Creating a query

You create a query using the New Query Wizard.

The New Query Wizard prompts you to specify the following:

- Query chart type, query name, and data source
- Output columns
- Optional filters
- Optional input parameters

You follow each wizard page by clicking Next. To change a query selection, click Back to return to a previous wizard page.

To create a query

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Queries**.
3. On the Queries page, in the Queries pane, select the folder in which you want to store the query, and then right-click **New Query**.
4. In the **New Query Wizard** dialog box, specify the chart type, query name, and data source, and then click **Next**.

   See “Selecting the general query parameters” on page 201.

5. In the **New Query Wizard** dialog box, select the output columns that you want to appear in the query, and then click **Next**.

   See “Selecting the query output columns” on page 202.

6. (Optional) In the **New Query Wizard** dialog box, add filters to expand or restrict the data source, and then click **Next**.

   See “Selecting the query filters” on page 203.

7. (Optional) In the **New Query Wizard** dialog box, create the query input parameters.

   See “Creating query input parameters” on page 204.

8. In the **New Query Wizard** dialog box, preview the results of the query, and then click **Finish** to save the query.

   The query is saved in the folder that you selected. The icon next to the query name indicates the chart type that the query uses to display the query results.

9. Run the query to verify that the query works as needed.

Selecting the general query parameters

General query parameters include the following:

Chart type

Select from the following query chart types:

- Table
- Line graph
- Area graph
- Stacked area graph
- Horizontal bar
- Vertical bar
- Horizontal stacked bar
- Vertical stacked bar
- Pie

The Preview feature illustrates each chart type.

Query Name

Type a name for the query.

Data Source

Select a data source.

When you run a query, the results are based on one of the following data sources:

- Assets (agents)
- Policies
- All real-time events
- Profile events
- Analysis events
- Console audit events
- Catalog files
- Assets and objects

Advanced Query

Select this check box if you prefer to build the query SQL statement yourself. The next page in the wizard prompts you to enter the SQL statement.

Only users who are assigned the Administrators role may select the Advanced Query box.

Fast Query Mode

Select this check box to build the query so that it runs in fast (no-lock) mode.

Fast mode does not guarantee consistent results.

Selecting the query output columns

You select the output columns that you want to appear in your query.

The query output columns are as follows:

Only get the top [100] results

This check box limits the total number of rows (records) that appear in a query. Select the check box, and then enter the number of rows.

For example, suppose you create a query that displays all the events generated by an agent. The query could potentially yield thousands of events, but you only want to show the first 500 events. You would select the Only get the top [100] results check box, and then enter 500.

Distinct results

Select this check box to eliminate duplicate output rows.

Show [1000] results per page

Type the number of output rows that you want to display per page.

Applies to queries that use the table chart type.

Column

Select a column that you want to appear in the query results.

Aggregate Function

Select the aggregate function. The aggregate function performs a calculation on a set of values and returns a single value shown as a column in the query results.

Select one of the following options:

- Count–Returns the number of items in a group.
- Count Distinct–Returns the number of distinct items in a group.
- Sum–Returns the sum of all the values (or only the distinct values).
- Min–Returns the minimum value.
- Max–Returns the maximum value.
- Average–Returns the average of the values in a group.

Display Name

Type the column heading text.By default, Display Name uses the Column name.

Display Width

Type the column width.

Move Up

Move Down

Remove

To order a selected column, click Move Up and Move Down until the column is in the desired order.

To remove a selected column, click Remove.

Add

Update

Add All

To add a column to the query results, specify the column options, and then click Add to add the column to the column list.

To save changes to a selected column, click Update.

To include all columns in the query results, click Add All.

Column list

This pane lists all the columns that appear in the query results.

Selecting the query filters

You use query filters to expand or restrict the data source. Each filter rule comprises <field, operator, value>.

For each filter rule, you specify the following:

Field

Select the field.

Examples of valid fields include event type, event date, event severity, event disposition, OS type, agent version, host name.

Required

Operator

Select the operator for the field.

Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.

Required

Value

Specify the default value for the input parameter.

Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.

Optional

Group By

Select this check box to group the output columns.

Optional

Order By

Select this check box to sort an output column in ascending order or descending order.

Optional

To select the query filters

1. In the **New Query Wizard** dialog box, on the Configure the Filters page, select <field, operator, value>.
2. (Optional) Select the **Group By** check box to group the output columns.
3. (Optional) Select the **Order By** check box to sort an output column in ascending order or descending order.
4. Click **Add**.
5. Repeat steps 1-4 to add additional filter rules.
6. To edit an existing filter rule, edit <field, operator, value>, and then click **Update**.

Creating query input parameters

You can build a basic query with input parameters. When run, the query prompts for the parameter values.

For each input parameter, you specify the following:

Column	Select the input parameter. Required
Operator	Select the operator for the input parameter. The Between and Not Between operators are not available for input parameters. To allow a range specification, create separate parameters for the lower and upper bounds. Required
Default Value	Specify the default value for the input parameter. Optional
Require a non-empty value at runtime	Select this check box to force the query user to specify a value for the input parameter. Optional
Display Name	Specify a custom display name for the input parameter.The display name appears when the query is run. Optional

Description	Specify a description of the input parameter. The description appears when the query is run. The description helps the user understand how to use the input parameter. Optional

When building queries with input parameters, please note the following:

- Each input parameter comprises <column, operator> or <column, operator, default value>.
- Query users can save a specific instance of a query, which they can run repeatedly. If a query is refreshed (re-run) without being closed, the query uses the same input values.
- Query users can save a query with or without input parameters. When saving a query without input parameters, users must set fixed values for the input parameters.
- Queries with input parameters can be included in reports, and imported and exported.
- When a query with input parameters is published, the query user is prompted for values when the query is run. The query user is not prompted for the values when the published results are used.

The following instructions demonstrate how to create an input parameter to prompt for operating system. The default value is Windows, and users must select a value from a defined list. A non-empty value is required.

To create query input parameters

1. In the **New Query Wizard** dialog box, on the Configure the Parameters page, in the Column box, select OS Type.
2. In the **New Query Wizard** dialog box, on the Configure the Parameters page, in the Operator box, select Equals.
3. In the **New Query Wizard** dialog box, on the Configure the Parameters page, in the Default Value box, select Windows.
4. Select the check box to require a non-empty value at runtime.
5. In the Display Name box, type Operating System. .
6. Click **Add**.
7. In the **New Query Wizard** dialog box, on the Configure the Parameters page, in the Column box, select OS Type.
8. In the **New Query Wizard** dialog box, on the Configure the Parameters page, in the Operator box, select In.

9 Select the check box to require a non-empty value at runtime.

10 In the **Display Name** box, type Operating System.

11 Click **Add**.

Creating a query to count the number of event types

The following query is provided as a tutorial in creating a query. The query counts the number events types. The query results are shown in a pie chart.

To create a query to count the number of event types

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries**.

3 On the Queries page, in the Queries pane, select the folder in which you want to store the query, and then right-click **New Query**.

4 In the **New Query Wizard** dialog box, select **Pie** as the chart type, type Event types for the query name, select **All Events** as the data source, and then click **Next**.

5 In the **New Query Wizard** dialog box, specify the query output for the event types, and then click **Add**.

Column	Select Event Type.
Aggregate Function	Select Max.
Display Name	Type Event Type.
Display Width	Type 10.

6 In the **New Query Wizard** dialog box, specify the query output for the event type counts, and then click **Add**.

Column	Select Event Type.
Aggregate Function	Select Count.
Display Name	Type Event Counts.
Display Width	Type 10.

7 Click **Next**.

8 In the **New Query Wizard** dialog box, group the event types, and then click **Add**.

Column	Select Event Type.
Group By	Select the Group By check box.

9 Click **Next**.

10 Preview the query, and then click **Finish** to save the query.

Creating a query to display event types and event severities

The following query is provided as a tutorial in creating a query. The query lists event types and event severities. The query results are shown in a table.

To create a query to display event types and event severities

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries**.

3 On the Queries page, in the Queries pane, select the folder in which to store the query, and then right-click **New Query**.

4 In the **New Query Wizard** dialog box , select **Table** as the chart type, type Event types and severity for the query name, select All Events as the data source, and then click **Next**.

5 Set up the event type column, and then click **Add**.

Distinct results	Select the Distinct results check box to eliminate duplicate output rows.
Column	Select Event Type.
Display Name	Type Event Type.
Display Width	Type 20.

6 Set up the event severity column, and then click **Add**.

Column	Select Event Severity.
Display Name	Type Event Severity.
Display Width	Type 20.

7 Click **Next**.

8 Click **Next**, to skip the filter.

9 Preview the query, and then click **Finish** to save the query.

Editing a query

After you create a query using the New Query Wizard, you can go back and edit the query using the same wizard.

To edit a query

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries**.

3 On the Reports page, in the Queries pane, select a query, and then right-click **Edit Query**.

4 In the **New Query Wizard** dialog box, modify the query using the New Query Wizard.

5 On the Reports page, in the Queries pane, select the query, and then right-click **Properties**.

6 In the query properties dialog, revise the revision number and query description, and then click **OK** to save your changes.

Editing the Symantec queries

You can use the Symantec queries as the basis for custom query development.

When editing a Symantec query, you should do the following:

- Make a copy of the Symantec query.
- Save the copy in your own folder.
- Edit the copy.
  Some Symantec queries are edited using the New Query Wizard. Other Symantec queries can only be edited by modifying the SQL statement.

Managing reports

A report comprises one or more queries that are configured as a group and viewed in a single display.

Running a report

The results from running a report appear in a tab in the Report Results pane. Each time you run a report, another tab appears.

You use the report tool bar to save and print reports, adjust your view of a report, navigate the pages in a report, and add and delete report pages.

To run a report

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports**.
3. On the Reports page, in the Reports pane, select a report, and then right-click **Run Report**.

   The report results are shown in the Report Results pane.
4. When you no longer need the report results, in the **Report Results** pane, click the report tab, and then click the green **X** icon to close the report results.

   To recover the report results, rerun the report.

Creating a report

You create a report using the New Report Wizard. The New Report Wizard prompts you to select the report layout, report name, and page size. A preview feature shows a sample report using the layout and page size that you selected.

You can customize a report's appearance by including a title, header and footer, and your company's logo.

Reports support a maximum graphic size of 150x100 pixels.

To create a report

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports**.
3. On the Reports page, in the **Reports** pane, select the folder in which you want to store the report, and then right-click **New Report**.
4. In the **New Report Wizard** dialog box, specify the report layout, name, and page size.

Report Layout	Select one of the following report layouts: ■ One Query–Each report page shows one query centered on the page. ■ Two Horizontal Queries–Each report page shows two queries placed side by side. ■ Two Vertical Queries–Each report page shows two queries placed one on top of the other. ■ Four Queries–Each report page shows two vertical columns, with two queries in each column.
Report Name	The name of the report.
Page Size	Select a page size: ■ Portrait–The report is created using a vertical page orientation. ■ Landscape–The report is created using a horizontal page orientation.

5. Click **Finish**.
6. Edit the report to insert queries and customize the report appearance.

Editing a report

You can edit a report by doing the following:

- Insert queries in the report
- Change the report title
- Change the report's header and footer text
- Insert your company's logo
- Add and delete pages

To edit a report

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports**.

3. In the **Reports** pane, select a report, and then right-click **Edit Report**.

   The report is shown in the Report Results pane.

   Use the following tool bar icons to adjust the report view and size, add and delete pages, save, and print:

Actual Size, Fit Page, Fit Width, Zoom In, Zoom Out, Zoom Ratio	Use the icons to adjust your view of the report.
First Page, Previous Page, Next Page, Last Page, Go To Page	Use these icons to navigate the report.
Add a page to the report	Use these icons to add and delete report pages.
Delete current page from the report	
Save to Disk	Use the Save to Disk icon to save the report changes.
Print	Use the Print icon to print the report.

4. To insert a query in the report, click **Click here to insert a query**, select **Insert Query**, select a query, and then click **Add**.
5. To customize the report title and header/footer text, select the placeholder for the title, header, or footer text, type the text that you want to insert, and then click **OK**.
6. To add your company's logo to the report, click the colored logo placeholder, browse to the directory that contains the logo, select the logo file, and then click **Open**.
7. To add a page to the report, click the **Add a page to the report** icon.
8. To delete a page from the report, click the **Delete current page from the report** (red **X**) icon.
9. To save the report changes, click the **Save to Disk** icon.
10. Run the report to verify the contents and appearance.

Publishing a query or report

Publishing a query or report saves a snapshot of the graphic and/or tabular results from running a query or report.

When publishing a query or report, you should note the following:

- A published query or report is saved in a user-selected folder in the Published Results pane.
- The date and time that a query or report was published is included in the file name. For example:
  Agent Details (published 09-Jan-2006 14.20.10 EST)
- You can view the published results for a query or report.
- You cannot change the contents of a published query or report. If you need to change the contents of a published query or report, you must edit the query or report, rerun it, and then publish the new results.
- Publishing a tabular query saves the first 10,000 rows of data.
- You can export published queries and reports to .zip files.
- You can export published reports as .pdf files and .html files.

To publish a query or report

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports** or **Queries**.
3. On the Reports or Queries page, select a query or report, and then right-click **Publish Query** or **Publish Report**.
4. In the **Publish Query Wizard** dialog box or **Publish Report Wizard** dialog box, select a folder in which to store the published query or report, and then click **Finish**.

   The published query or report is saved in the Published Results pane, in the folder that you selected.
5. To view a published query, select the query in the Published Results under **Reports** tab, and then right-click **Run** Query.
6. To view a published report, select the report in the Published Results under **Reports** tab, and then right-click **View** Published Report.

Exporting a published report as PDF

Exporting a published report as PDF creates a .pdf file that contains a snapshot of the graphic and/or tabular results from a report. The published date and time is included in the .pdf file name. For example:

Summary_Report (published 09-Jan-2006 14.20.10 EST).pdf

To export a published report as PDF

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Published Results**.
3. On the Reports page, in the **Published Results** pane, select a published report, and then right-click **Export as PDF**.
4. In the **Export** dialog box, in the **Look In** box, browse to the location where you want to store the .pdf file.
5. In the **Export** dialog box, in the **File Name** box, type a file name for the .pdf file.
6. Click **Export**.

Exporting a published report as HTML

Exporting a published report as HTML creates a .html file that contains a snapshot of the graphic and/or tabular results from a report.

When exporting a published report as HTML, you should note the following:

- The published date and time is included in the .html file name. For example:
  Summary_Report (published 09-Jan-2006 14.20.10 EST).html
- A folder that contains the graphic images for the .html file is created in the same folder with the .html file.
  The folder name uses the name of the .html file and the text .html_files. For example:
  Summary_Report (published 09-Jan-2006 14.20.10 EST).html_files

To export a published report as HTML

1. In the management console, click a console view tab.
2. In the management console, click **Reports**.
3. Under the **Reports** tab, click **Published Results**.
4. On the Reports page, in the **Published Results** pane, select a published report, and then right-click **Export as HTML**.

5 In the **Export** dialog box, in the **Look In** box, browse to the location where you want to store the .html file.

6 In the **Export** dialog box, in the **File Name** box, type a file name for the .html file.

7 Click **Export**.

About the command-line query tool

The management console supports command-shell execution of previously defined Symantec Critical System Protection queries and reports.

The following features are supported:

- Execution of basic and advanced queries
- Support for queries with input parameters
- Support for output in PDF, HTML, CSV, and JPEG format
- Support for publishing (to a Published Results folder for later use in the management console) or exporting (to a file on disk)

When using the command-line query tool, you must specify your Symantec Critical System Protection login credentials. The command-line query tool authenticates your login credentials, and sets the operational context to obey all defined role-based access controls.

Your Symantec Critical System Protection account must belong to the Query Tool Users role.

See “Creating a user account” on page 236.

Running the command-line query tool

The command for running the command-line query tool is as follows:

```
cspquery.bat -u <username> -p <password> -q <inifile> -s <server name>
```

where:

<username>	Your Symantec Critical System Protection username. Required
<password>	Your Symantec Critical System Protection password. Required

<inifile>

The name of the query configuration .ini file.

You pass arguments to the command-line query tool using a query configuration .ini file. The configuration .ini file defines the query or report to run, the action to be taken (publish or export), and the runtime input parameters.

The following sample file contains instructions for setting up a query configuration .ini file:

C:\Program Files\Symantec\Critical System Protection\Console\query_template.ini

Required

<server name>

The server name.

Use this argument to set the server name if multiple servers were defined. The server name is displayed in the Server box on the Symantec Critical System Protection management console login screen.

Optional

To run the command-line query tool

1. Log on to the computer that runs the management console.
2. At a command prompt, navigate to the following directory:

   ```
   C:\Program Files\Symantec\Critical System Protection\Console
   ```

3. At a command prompt, type and run the following (required arguments are shown):

   ```
   cspquery.bat -u <username> -p <password> -q <inifile>
   ```

Distributing query and report output

You can implement your own scheduling and report distribution capability. You can construct command scripts that are scheduled for periodic execution using the Windows Task scheduler, and distribute query and report output to interested parties using operating system tools or third-party packages.

Using folders

You use folders to organize your queries and reports. For example, you might use one folder to store your custom queries and another folder to store your published reports.

The default query folder is named Queries. The default report folder is named Reports.

Creating a folder

There is no limit to the number of folders that you can create. You can create nested folders within other folders.

Create folders so that you can organize your queries and reports efficiently. Name folders so that you can easily identify which queries and reports to assign to the folders.

To create a folder

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Queries** or **Reports**.
3. In the **Queries** pane or the **Reports** pane, navigate to the folder under which you want to create the new folder.
4. Select the folder, and then right-click **New Folder**.

   A new folder is created with the name New Folder.
5. Rename the folder, and then press the **Enter**.

Moving a query or report to a folder

You can move queries among the folders in the Queries pane. You can move reports among the folders in the Reports pane.

To move a query or report to a folder

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Queries** or **Reports**.
3. In the **Queries** pane or the **Reports** pane, select the query or report that you want to move, and then right-click **Move To**.

   You can also move a query folder to another query folder.

   You can also move a report folder to another report folder.

4 In the **Move Query** dialog box, select the folder where you want to move the query or report.

To browse the folders in the Queries or Reports tree, double-click a folder.

5 Click **Move To** to move the query or report to the selected folder.

Deleting a query or report folder

You can delete a query folder or a report folder. The folder that you want to delete must be empty.

To delete a query or report folder

1 In the management console, click **Reports**.

2 To delete a query folder: Under Queries, In the Queries pane, select a folder, and then right-click **Delete**.

3 To delete a report folder: Under Reports, In the Reports pane, select a folder, and then right-click **Delete**.

Copying a query or report

You can make a copy of a query or report. You can save the copy as a backup copy, or customize the copy to create a new query or report. The copy is named Copy_of followed by the name of the original query or report (for example, Copy_Policy Detail).

To copy a query or report

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries** or **Reports**.

3 In the **Queries** pane or the **Reports** pane, select the query or report that you want to copy, and then right-click **Copy Query** or **Copy Report**.

4 Rename the copy, and then press **Enter**.

Renaming a query or report

You can rename a query or report.

To rename a query or report

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries** or **Reports**.

3 In the **Queries** pane or the **Reports** pane, select the query or report that you want to rename, and then right-click **Rename Query** or **Rename Report**.

4 Enter a new name, and then press **Enter**.

Exporting queries and reports

Symantec Critical System Protection exports queries and reports to .zip files. You can share the exported queries and reports with other Symantec Critical System Protection administrators.

Exporting a query

You can export a query or a query folder. Queries can be exported from the Queries pane or the Published Results pane.

To export a query

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Queries**.

3 On the Reports page, navigate to and select a query or query folder.

4 To export a query, in the **Queries** pane, right-click **Export Query**.

5 To export a published query, in the **Published Results** pane, right-click **Export Published Results**.

6 In the **Export** dialog box, in the **Look In** box, browse to the location where you want to store the .zip file.

7 In the **Export** dialog box, in the **File Name** box, type a file name for the .zip file.

Click **Export**.

The selected query or query folder is exported to a .zip file using the file name that you specified. In the Exporting dialog box, each successfully exported query is marked with a green check mark.

8 Click **Close**.

Exporting a report

You can export a report or a report folder. Reports can be exported from the Reports pane or the Published Results pane.

To export a report

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Reports**.
3. On the Reports page, navigate to and select a report or report folder.
4. To export a report, in the **Reports** pane, right-click **Export Report**.
5. To export a published report, in the **Published Results** pane, right-click **Export Published Results**.
6. In the **Export** dialog box, in the **Look In** box, browse to the location where you want to save the .zip file.
7. In the **Export** dialog box, in the **File Name** box, type a file name for the .zip file.
8. Click **Export**.

   The selected report or report folder is exported to a .zip file using the file name that you specified. In the Exporting dialog box, each successfully exported report is marked with a green check mark.
9. Click **Close**.

Importing queries and reports

Symantec Critical System Protection imports queries and reports from .zip files. You can import queries and reports that you obtained from other Symantec Critical System Protection administrators.

Importing a query

The management console extracts the query from the .zip file. Queries can be imported to the Queries pane or the Published Results pane.

The imported queries are available in the selected folder in the Queries pane.

To import a query

1. In the management console, click **Reports**.
2. Under the **Reports** tab, click **Queries**.
3. On the Reports page, navigate to and select a folder to receive the imported queries.
4. To import a query, in the **Queries** pane, right-click **Import Query**.

5 To import a published query, in the **Published Results** pane, right-click **Import Published Results**.

6 In the **Import** dialog box, in the **Look In** box, browse to the directory where the .zip file is located, and then select the file.

7 Click **Import**.

In the Importing dialog box, each successfully imported query is marked with a green check mark.

8 Click **Close.**

Importing a report

The management console extracts the report from the .zip file for you. Reports can be imported to the Reports pane or the Published Results pane.

The imported reports are available in the selected folder in the Reports pane.

To import a report

1 In the management console, click **Reports**.

2 Under the **Reports** tab, click **Reports**.

3 On the Reports page, navigate to and select a folder to receive the imported reports.

4 To import a report, in the **Reports** pane, right-click **Import Report**.

5 To import a published report, in the **Published Results** pane, right-click **Import Published Results**.

6 In the **Import** dialog box, in the **Look In** box, browse to the directory where the .zip file is located, and then select the file.

7 Click **Import**.

In the Importing dialog box, each successfully imported report is marked with a green check mark.

8 Click **Close.**

Deleting a query or report

You can delete queries and reports that you no longer need.

To delete a query or report

1. In the management console, click **Reports**.
2. To delete a query: Under Queries, In the **Queries** pane, select a query, and then right-click **Delete Query**.
3. To delete a report: Under Reports, In the **Reports** pane, select a report, and then right-click **Delete Report**.
4. In the Confirm Deletion dialog, click **Yes** to delete the query or report.

Chapter 8

Managing alerts

This chapter includes the following topics:

About alerts

You use alerts to send events of interest to email messages, SNMP traps, and text files.

The Alert module polls the Symantec Critical System Protection database for events that match an alert filter. When a match is found, the Alert module generates and sends email messages, SNMP traps, and text files that are associated with the alert.

About email aggregation

Email aggregation combines all email messages that are sent to an email address, over a specified aggregation time interval, into a single email message.

There are two criteria for aggregation: time interval and maximum email message size. Email aggregation prevents flooding email addresses with too many messages or with messages that exceed size limitations. (Some email accounts may reject email messages based on message size.)

The aggregation time interval starts when the Alert module is first started or immediately after sending emails for alerts from the last time interval. Once the specified number of minutes has elapsed, an email message is sent to the email address with all the alerts over that time interval.

Email alerts aggregation uses the following rules:

- First-level aggregation
  Combine similar repetitive alerts, over a specified time interval, into a single alert that includes aggregation start time, aggregation end time, and the number of events aggregated along with event information.
- Second-level aggregation
  Aggregation occurs at the end of an aggregation time interval where multiple aggregated alerts and individual alerts are combined into a single email message.
  Alerts are written into the body of the email message, sorted by time of occurrence. The first alert that occurs is written at the top of email message body. The last alert to occur is written at the bottom of the email message body. For aggregated alerts, time of occurrence is the time of occurrence of the first event.

In any given aggregation time interval, only one email message is sent to one email address, unless the size of the email body exceeds the maximum specified size. In this case, the data is split into multiple email messages.

About SNMP traps

The Alert module polls the management server database for new events at every user-specified event polling interval. An SNMP trap is generated and dispatched over the network for each event that matches a user-specified alert filter. The Alert module generates one trap for each alert.

The Alert module sends the following types of SNMP traps:

None	No SNMP trap is sent.
Basic	A basic trap contains the alert name, policy name, rule name, agent computer name and IP address, and event type.

General	A general trap contains the alert name, policy name, rule name, event date, agent computer name and IP address, user name, event severity, event priority, event disposition, event type, event count, event operation, OS type, process name, local IP address, local port number, remote IP address, remote port number, product version, target information, and description.

About alert text files

An alert text file contains events of interest; the alert text file can contain text strings and event fields. The alert text file is created when an alert captures an event of interest; subsequent events are appended to the file.

The Symantec Critical System Protection detection policy Global_Watch_Policy monitors alert text files. When an event in an alert text file matches the criteria specified in the policy, the policy sends the event to the management console.

About troubleshooting alert problems

A separate log file is used to record any problems that occur when sending SNMP traps and email alerts. You can use this file to help debug alert problems.

By default, the alert log file is stored in the following directory:

C:\Program Files\Symantec\Symantec Critical System Protection\Server\Tomcat\logs\sis-alert.?.log

The question mark (?) in the log file name is the sequence number. When the management server rotates the log file, the current log file is closed and nothing more is written to it. A new log file is opened with the same base file name, but with the next highest sequence number added to the file name. The active log file uses sequence number 0 (for example, sis-alert.0.log). Inactive (rotated) log files use sequence numbers 1 through n.

Viewing the Alerts page

You use the Alerts page in the management console to create and store the alerts that you send to users when specific events are observed by Symantec Critical System Protection.

You can do the following activities from the Alerts page:

- Configure alert settings.
- Create, edit, and delete alerts.
- Specify alert filters, email addresses, SNMP traps, and alert text files.

- Enable and disable alerts.

To view the Alerts page

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Alerts**.
3. On the Alerts page, in the **Alerts Configurations** pane, double-click an alert to view your settings for polling intervals, SMTP server and port, aggregation interval, and email message size.
4. (Optional) To expand or collapse the panes in the Alerts page, click the size arrows.

Configuring alert settings

The Alert Module uses alert settings to get polling intervals and email settings.

To configure alert settings

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Settings**.
3. On the Admin page, in the **System Settings** pane, click **Alert Settings**.

4 In the **Alert Settings** pane, specify the following alert settings:

Polling Settings: Configuration Polling Interval	The frequency, in minutes, at which the Alert module polls for changes to the alert settings. Default: 5 minutes
Polling Settings: Event Polling Interval	The frequency, in minutes, at which the Alert module polls the management server database for events. Default: 5 minutes
Email Settings: SMTP Server	The SMTP server address for sending email messages.
Email Settings: SMTP Port	The SMTP port number for sending email messages. Default: 25
Email Settings: Email From	The email address from which alert emails originate. Default: Alert@SCSP_Server
Email Settings: Enable Email Aggregation	Select this check box to enable email aggregation, and then specify the Aggregation Interval.
Email Settings: Aggregation Interval	The event polling intervals, in minutes. If email aggregation is enabled, aggregate emails are sent based on the frequency that you specify. Default: 10 minutes
Email Settings: Maximum Email Size	The maximum email message size, in KB. Default: 1024

5 Click **Save** (save the current setting changes) or **Revert** (revert to the last settings that were saved).

6 Click **Refresh** to apply the alert updates.

Creating an alert

Alerts notify users when specific events are observed by Symantec Critical System Protection.

Alerts comprise the following components:

- Alert filters

- Email address templates
- SNMP traps
- Alert text files

To create an alert

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Alerts**.
3. On the Alerts page, in the toolbar, click **Create a new Alert** icon.
4. In the **New Alert** dialog box, on the **General** tab, specify the following alert information:

Alert name	The name of the alert.
Enabled	Select this check box to enable the alert. The alert is enabled by default. You can enable and disable an alert after you create it.
Description	A description of the alert.

5. Click **OK**.
6. Edit the alert to specify filters, email address templates, SNMP traps, and text file.

Creating an alert filter

You use alert filters to specify which events you want Symantec Critical System Protection to observe.

When configuring alert filters, please note the following:

- Each filter rule comprises <field, operator, value>.
- Examples of valid fields include event type, event severity, event disposition, OS type, local IP address, remote IP address, host name.
- Examples of valid operators include equals, not equals, in, not in, contains, not contains, greater than, less than. Some operators support the use of wildcard characters in a value. Valid wildcard characters are asterisk (*), which represents zero or more consecutive characters, and question mark (?), which represents exactly one character.
- Valid values vary, depending on the field. Some fields are limited to a pre-defined list, while other fields allow free-form typing.

- The Preview Events button on the Filters tab lets you preview recent events that match the alert filters.

To create an alert filter

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Alerts**.
3. In the **Alert Configurations** pane, select an alert, and then right-click **Edit Alert**.
4. In the alert dialog box, on the **Filters** tab, select <field, operator, value>, and then click **Add**.
5. Repeat step 4 to add additional rules.
6. To edit an existing filter rule, edit <field, operator, value>, and then click **Update**.
7. To preview filtered events, click **Preview Events**.
8. Click **OK**.

Specifying an email address template

An email address template contains the email addresses that you want to receive the alert.

When including event date fields in the subject and body of an email message, you can select UTC or local agent date/time.

To specify an email address template

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Alerts**.
3. In the **Alert Configurations** pane, select the alert, and then right-click **Edit Alert**.
4. In the alert dialog box, on the **Email** tab, click **Add**.
5. In the **Email Template** dialog box, specify the following information:

To	In a comma-separated list, type the email addresses that you want to receive the alert.

Subject	Specify the subject of the email: ■ Type the text that you want to include in the subject line of the email. ■ Select the event fields that you want to include in the subject line.
Body	Specify the email message: ■ Type the message that you want to include in the email body. ■ Select the event fields that you want to include. Select Insert All to insert all of the available event fields, with each field shown on a separate line.

6. Click **Save**.
7. In the alert dialog box, on the **Email** tab, in the Enabled column, click the check box to enable the email address template.

   All email addresses contained in the template will receive the alert.If you do not want to send the alert at this time, uncheck **Enabled**.
8. Click **OK**.

Specifying an SNMP trap

You configure the following when specifying an SNMP trap:

- Type of SNMP trap to send
- Server to which the SNMP trap is sent
- Port numbers used by the SNMP server

To specify an SNMP trap

1. In the management console, click **Monitors**.
2. Under the **Monitors** tab, click **Alerts**.
3. In the **Alert Configurations** pane, select the alert, and then right-click **Edit Alert**.
4. In the alert dialog box, on the SNMP tab, specify the following information:

Server	Type the SNMP server address.
Server Port	Type the server port number used by the Symantec Critical System Protection server when it connects to your SNMP server. Default: 162

Local Port

Type the local port number used by the Symantec Critical System Protection server when it connects to your SNMP server. Optional.

Default: 161

Community

Type the SNMP community name used when sending SNMP traps.

Default: Public

Trap level

Select the type of SNMP trap that you want to generate when an alert is triggered.

Select one of the following SNMP trap types:

- None
- Basic
- General

See “About SNMP traps” on page 224.

5 Click **OK**.

Specifying an alert text file

You can set up an alert text file to save events of interest. The alert text file can contain text strings and event fields. The file is created when the alert captures an event; subsequent records are appended to the file.

An alert text file is stored on the Symantec Critical System Protection management server computer. The default alerts directory is as follows:

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

The Symantec Critical System Protection detection policy Global_Watch_Policy monitors alert text files. When an event in an alert text file matches the criteria specified in the policy, the policy sends the event to the management console.

See the *Symantec Critical System Protection Detection Policy Reference Guide* for details on how to configure the Global_Watch_Policy.

To specify an alert text file

1 In the management console, click **Monitors**.

2 Under the **Monitors** tab, click **Alerts**.

3 In the **Alert Configurations** pane, select the alert, and then right-click **Edit Alert**.

4 In the alert dialog box, on the **File** tab, specify the following information:

File Name	Type the name of the alert text file. The file name may not contain any backward slashes.
Text To Append	Type the text to save in the alert text file. The text can include event fields, selected form the menu.

5 Click **OK**.

Enabling or disabling an alert

Enabled alerts send email messages and SNMP traps. Disabled alerts do not send email messages and SNMP traps.

To enable or disable an alert

1 In the management console, click **Monitors**.

2 Under the **Monitors** tab, click **Alerts**.

3 In the **Alert Configurations** pane, enable or disable an alert.

To enable an alert, check **Enabled**.

To disable an alert, uncheck **Enabled**.

About copying alerts

Symantec Critical System Protection Copy Alerts function lets you create copies of alerts. For example, if there are existing alerts with complex filters and you want to create another alert with similar filters and some additional filters, you can copy an existing alert and add the required filter to it instead of creating an alert from the start.

The copied alert appears in the format **Copy of_ Alert name**. For example, a copied alert for an existing alert named ALERT1 would appear as Copy of_ALERT1.

Creating copies of alert

To create copies of alert

1 Log on to the management console.

2 Click the **Monitors** tab.

3 Click **Alerts**.

4 In the **Alerts Configuration** pane, right-click an alert and select **Copy Alert**.

Deleting an alert

You can delete alerts that you no longer need.

To delete an alert

1 In the management console, click **Monitors**.

2 Under the **Monitors** tab, click **Alerts**.

3 In the **Alert Configurations** pane, select an alert, and then right-click **Delete Alert**.

4 In the **Confirm Deletion** dialog box, click **Yes** to delete the alert.

Chapter 9

Using the Admin page

This chapter includes the following topics:

Viewing the Admin page

You use the Admin page in the management console to perform the following administrative tasks:

- Manage user accounts for the Symantec Critical System Protection management console.
- View system settings for management server health.
- View and edit audit settings, event management settings, and virtual agent settings.
- Manage the Tomcat server and Web applications.
- Change the management server's host name, server name, console port, and admin port.

Note: To perform these administrative functions, you must log on to the management console as a user who is assigned to the built-in Administrators role.

To view the Admin page

◆ In the management console, click **Admin**.

Creating a user account

User accounts provide secure access to the Symantec Critical System Protection management console.

You can create a user account that can be authenticated locally or by using Active Directory.

When you create a user account, you must assign one or more roles to the account. The roles that you assign determine what functions the user can perform in the management console.

The Symantec Critical System Protection built-in roles are as follows:

Administrators

Users with the Administrators role can log on to the management console and have complete, unrestricted access to all available features and tasks. Administrators can add users and make other system-wide changes. Administrators can access all agent groups on the Assets page, and all queries and reports on the Reports page.

The default account (symadmin) that was created during Symantec Critical System Protection installation is assigned the Administrators role.

Authors

Users with the Authors role can log on to the authoring environment and author policies.

Guests

Users with the Guests role can log on to the management console but cannot make any policy changes. Guests can access all agent groups on the Assets page.

You can create custom guest roles, each with its own name and folder permissions on the Assets page.

Managers

Users with the Managers role can log on to the management console and make changes to agents and policies, such as modifying agent and group policy and configuration settings, and creating and modifying policies. Managers may optionally access queries and reports on the Reports page. Managers cannot perform any security-related activities, except for changing their account password. Managers can access all agent groups on the Assets page.

Query Tool Users

Users with the Query Tool Users role can run the command-line query tool.

The account must have access to the queries, reports, and results folders. This access can come from the Query Tool Users role or an additional Managers/Guests role.

The Query Tool Users role gives users permission to run the command-line query tool. It does not give users permission to log on to the management console.

In addition to the Symantec Critical System Protection built-in roles, you can assign custom roles to a user.

See "Creating a custom role" on page 240.

To create a user account

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Users**.
3. In the toolbar, click **Create a new User** icon.

4. In the **New User** dialog box, on the **General** tab, specify the following information:

   User name

   The account user name.

   The user name is used to log on to the management console.

   Description

   A description of the user or the purpose of the account.

   Password

   The account password.

   The password is used to log on to the management console.

   The password must be at least eight characters, and contain a mix of letters and at least two numbers or special characters.

   Confirm Password

   Type the password again to confirm it.

5. In the **New User** dialog box, on the **Member Of** tab, click **Add**.
6. In the **Add Roles** dialog box, select a role, and then click **Add**.

   To select multiple roles, hold down the Ctrl key while selecting the roles.
7. In the **New User** dialog box , click **OK**.

   The user account is created with the user name, password, and roles that you specified.

Editing account information

You should provide contact name, addresses, and phone numbers for each account.

To edit account information

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Users**.
3. On the **Users** page, select a user account, and then right-click **Properties**.

4 In the user account dialog box, on the **Contact** tab, specify the following information:

Contact name	The name of the contact person for the user. The contact person can be a department administrator, the user's supervisor, etc.
Telephone number(s)	The user's office and cell phone numbers.
Email address	The user's email address.
Alert email address	The email address of contacts who should receive an email alert when an event occurs.
Address	The user's office mailing address.
Manager name	The name of the user's immediate supervisor.
Business	The company name or organization.
Preferred language	The user's preferred language.

5 Click **OK**.

Assigning roles to a user account

You can assign roles to an existing user account.

To assign roles to a user account

1 In the management console, click **Admin**.

2 Under the **Admin** tab, click **Users**.

3 On the **Users** page, select a user account, and then right-click **Properties**.

4 In the user account dialog box, on the **Member Of** tab, click **Add**.

5 In the **Add Roles** dialog box, select the roles, and then click **Add**.

To select multiple roles, hold down the Ctrl key while selecting the roles.

6 Click **OK**.

Removing roles assigned to a user account

You can remove roles that were assigned to a user account.

To remove roles assigned to a user account

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Users**.
3. On the **Users** page, select a user account, and then right-click **Properties**.
4. In the user account dialog box, on the **Member Of** tab, select the roles that you want to remove, and then click **Remove**.

   To select multiple roles, hold down the Ctrl key while selecting the roles.
5. Click **OK**.

Creating a custom role

You can create custom roles that have access to the following objects:

- Agent groups
- Policy groups
- Configuration groups
- Queries/reports

For each role you create, you must specify the following:

- Name and description of the role
- User accounts that are assigned to the role
- Objects that the role is allowed to access

You can also create custom guest roles, each with its own role name and permissions. Users with custom guest roles can log on to the management console, but cannot make any policy changes.

See "Examples of creating custom roles" on page 241.

To create a custom role

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.
3. On the **Roles** page, click **New Role** icon.
4. In the **New Role** dialog box, type a name and description of the new role.
5. If you are creating a custom guest role, check **Guest role**.

6. In the **New Role** dialog box, click **Add**.
7. In the **Add Users** dialog box, select the user accounts, and then click **Add**.

   To select multiple user accounts, hold down the Ctrl key while selecting the accounts.
8. Click **OK**.
9. In the management console, click **Assets**, and then edit the Security tab for each agent group that the role is allowed to access.

   Assign access to the default group, then assign access to specific groups in the tree.
10. In the management console, click **Reports**, and then edit the Security tab for each query/report folder that the role is allowed to access.

    You can assign access to all folders or specific folders in a tree.

Examples of creating custom roles

The following examples illustrate how to create custom roles.

Create a Prevention Manager role

You want to create a new role called Prevention Manager. The Prevention Manager will oversee all agents that support prevention features. You want to allow the Prevention Manager to access all agent groups in the Prevention view. You do not want to allow the Prevention Manager to access any agent groups in the Master View or the Detection view.

See Table 9-1 describes your current agent group structure.

Table 9-1 Create Role Example: Agent group structure

View	Default agent group	Sub-groups
Master	Network	You have not created any groups in the Network group tree.
Prevention	Policy	You have two groups in the Policy group tree: ■ East Coast Agents ■ West Coast Agents

Table 9-1 Create Role Example: Agent group structure *(continued)*

View	Default agent group	Sub-groups
	Configuration	You have two groups in the Configuration group tree: ■ East Coast Agents ■ West Coast Agents
Detection	Policy	You have two groups in the Policy group tree: ■ Division A Agents ■ Division B Agents
	Configuration	You have two groups in the Configuration group tree: ■ Division A Agents ■ division B Agents

In the Prevention view, the default Policy group has two groups in its tree: East Coast Agents and West Coast Agents. You want to allow the Prevention Manager to access the default Policy group and all the groups in its tree.

To create the Prevention Manager role

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.
3. On the **Roles** page, click **New Role** icon.
4. In the **New Role** dialog box, type **Prevention Manager** for the role name and **Oversees all prevention agents** for the description.
5. Assign user accounts to the Prevention Manager role.
6. Click **OK** to save the Prevention Manager role.
7. In the management console, click **Assets**.
8. Allow the Prevention Manager role to access the default Policy group.

   In the Asset Policies pane, select the default Policy group, and then right-click **Properties**. On the Security tab, select Prevention Manager, and then click **OK**.

9 Allow the Prevention Manager role to access the East Coast Agents group.

In the Asset Policies pane, select the East Coast Agents group, and then right-click **Properties**. On the Security tab, select Prevention Manager, and then click **OK**.

10 Allow the Prevention Manager role to access the West Coast Agents group.

In the Asset Policies pane, select the West Coast Agents group, and then right-click **Properties**. On the Security tab, select Prevention Manager, and then click **OK**.

Create an Assistant Manager role

You want to create a new role called Assistant Manager. The Assistant Manager will monitor all agents that have registered with the management server. You want to allow the Assistant Manager to access all agent groups in the Master view. You do not want to allow the Assistant Manager to access any agent groups in the Prevention View or the Detection view.

In the Master view, all agents reside in the default Network group.

To create the Assistant Manager role

1 In the management console, click **Admin**.

2 Under the **Admin** tab, click **Roles**.

3 On the **Roles** page, click **New Role** icon.

4 In the **New Role** dialog box, type **Assistant Manager** for the role name and **Monitors all agents that have registered with the management server** for the description.

5 Assign user accounts to the Assistant Manager role.

6 Click **OK** to save the Assistant Manager role.

7 In the management console, click **Assets**.

8 Allow the Assistant Manager role to access all agent groups in the Master view.

In the Network Assets pane, select the Network group, and then right-click **Properties**. On the Security tab, select Assistant Manager, and then click **OK**.

Assigning user accounts to a role

You can assign user accounts to an existing role.

To assign user accounts to a role

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.
3. On the **Roles** page, select a role, and then right-click **Properties**.
4. In the **Role** dialog box, on the **General** tab, click **Add**.
5. In the **Add User(s)** dialog box, select the user accounts for the role, and then click **Add**.

   To select multiple user accounts, hold down the Ctrl key while selecting the accounts.
6. Click **OK**.

Removing user accounts assigned to a role

You can remove user accounts that were assigned to a role.

To remove user accounts assigned to a role

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.
3. On the **Roles** page, select a role, and then right-click **Properties**.
4. In the **Role** dialog box, on the **General** tab, select the user accounts that you want to remove, and then click **Remove**.

   To select multiple user accounts, hold down the Ctrl key while selecting the accounts.
5. Click **OK**.

Assigning access permissions to roles

You can allow roles to access to the following management console objects:

- Agent groups
- Policy groups
- Configuration groups
- Queries/reports

Note: By default, the built-in Administrators role has complete, unrestricted access to all available Symantec Critical System Protection features and tasks, including access to all agent groups. Because you need at least one role with unrestricted access, it is recommended that you do not modify the built-in Administrators role.

To assign access permissions to roles

1. In the management console, click **Assets**.
2. Under the **Assets** tab, click **Detection**.
3. In the **Asset Policies** pane, select the agent group to which you want to allow access, and then right-click **Properties**.
4. In the properties dialog box, on the **Security** tab, select the **Allowed** check box for each role that can access the agent group.
5. Click **OK** to save your changes.
6. Repeat steps 3-5 to assign access for another agent group.
7. On the Reports page, select the query or report folder to which you want to allow access, and then right-click **Properties**.
8. In the properties dialog, on the Security tab, select the **Allowed** check box for each role that can access the query or report folder.
9. Click **OK**.
10. Repeat steps 7-9 to assign access for another query or report folder.

Allowing a role to edit the Security tab

By default, the built-in Administrators role is allowed to edit the Security tab for each Symantec Critical System Protection agent group. You can extend this privilege to other non-guest roles.

To allow a role to edit the Security tab

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.
3. On the **Roles** page, select a role, and then right-click **Properties**.
4. In the **Role** dialog box, on the Security tab, click **Allow this role to edit the** Security tab on its group.
5. Click **OK**.

Resetting a password

You can reset the password for a user account. The new password is effective immediately.

To reset a password

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Users**.
3. On the **Users** page, select a user account, and then right-click **Set Password**.
4. In the Set Password dialog, type the new password, then type it again to confirm.
5. Click **Set**.

Deleting a user account

If you no longer want a user to have access to the management console, you can delete the user's account.

Note: You cannot delete the built-in symadmin user account.

To delete a user account

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Users**.
3. On the **Users** page, select the user account, and then right-click **Delete User**.
4. In the **Confirm Deletion** dialog box, click **Yes** to delete the user account.

Deleting a role

You can delete roles that you no longer use.

Before you delete a role, make sure the role is not assigned to a user account.

Note: You cannot delete the built-in Administrators role.

To delete a role

1. In the management console, click **Admin**.
2. Under the **Admin** tab, click **Roles**.

3. On the **Roles** page, select the role, and then right-click **Delete Role**.
4. In the **Confirm Deletion** dialog box, click **Yes** to delete the role.

Viewing or modifying system settings

System settings comprise the following:

- Management server health
- **General settings** tab
  - **Audit settings**
  - **Event Management** settings
  - **Login Notice** setting
- **Agent setting**s tab
  - **Virtual Agent** settings
  - **Agent Health** setting
  - **Duplicate Agent Registration**

To view or modify system settings

1. In the management console, click **Admin**.
2. Under **Admin** tab, click **Settings**.
3. In the left-hand pane, click **System Settings**.
4. View or modify the system settings.
5. Click **Save**.

About the management server health

The health of the connection between the Symantec Critical System Protection management server and the database is indicated by the following:

- A green circle icon indicating that the management server is running, or a red circle icon indicating that a management server or database error occurred.
- The management server version
- The date and time the connection between the management server and the database was last checked

About the Audit settings

The Symantec Critical System Protection management server records audit events whenever changes to the system configuration are made.

By default, the management server records audit events for the following user activity:

- Creating data
- Saving data
- Deleting data
- Logging on to the management console
- Logging off the management console

Optionally, you can instruct the management server to record audit events for the following additional user activity:

- Execution of queries or reports
- Execution of searches from the Monitors page

The execution of searches, queries, and reports is disabled by default.

You can view all audit events from the Monitors page.

About the Login Notice setting

You can specify a message to display whenever a user logs on to the management console. The user must acknowledge the message by clicking OK (continue logging on) or Cancel (exit the management console).

About the Event Management settings

Event Management settings specify how long to retain the following types of events:

Real-time events	Events that are transmitted to the management server, based on an agent's log rules.
Profile events	Events that are generated when an agent profiles a program or service.
Analysis events	Events that are transmitted to the management server using bulk log transfer, and then loaded into the Symantec Critical System Protection database using the bulk loader utility. Analysis events are of long-term interest, generally for audit or forensic analysis needs.

Events older than the age that you specify are purged from the Symantec Critical System Protection database.

By default, event management settings are configured not to purge any events.

The event management settings are as follows:

Purge Real-Time Events older than [n] days	Select this check box to purge real-time events, and then type the age of the events, in days. When this check box is selected, the default event age is 365 days.
Purge Profile Events older than [n] days	Select this check box to purge old profile events, and then type the age of the events, in days. When this check box is selected, the default event age is 60 days.
Purge Analysis Events older than [n] days	Select this check box to purge old analysis events, and then type the age of the events, in days. When this check box is selected, the default event age is 60 days.

About the Virtual Agent settings

Virtual Agent settings control the storage of virtual events and the dynamic registration of virtual agents.

If your Symantec Critical System Protection agent deployment indirectly detects off-platform event data and associates the data with agents in the management console, you will need to configure Virtual Agent settings.

The Virtual Agent settings are as follows:

Allow virtual agents to register automatically	When selected, this setting allows both dynamic and manual registration of virtual agents. When the setting is not selected, only manual registration is allowed. Default: On
Allow virtual events to be stored in real time	When selected, this setting allows virtual events to be stored in real time with regular Symantec Critical System Protection events. Log rules for the agents that collect virtual events must be configured for virtual events. When this setting is not selected, virtual events are bulk-logged. Bulk logging must be enabled on the agents that collect virtual events. The agent log rules must be configured for virtual events. Default: On

About the Agent Health setting

To prevent network flooding as agents go offline and online, a system-wide flood-control option aggregates status change events into a single event.

The Agent Health setting is as follows:

Aggregate agent health events when more than [n] change at once	The threshold value for the number of agent status change events that cause a single aggregated status change event to be generated instead of a flood of individual agent events. This setting helps limit the number of meaningless events (and any related alerts) resulting from a network outage that affects a large number of agents at once. Default: 25

You can configure agent health settings for specific agents.

See “Configuring agent health timeout settings” on page 94.

About the duplicate agent registration settings

You can disable the registration of duplicate agents with the management server. By default, Symantec Critical System Protection lets you register duplicate agents based on some common attributes such as IP address, agent name, and so on. When Symantec Critical System Protection recognizes a duplicate agent, it updates the existing agent record in the database with the new agent data and flags the agent for policies and configs.

Symantec Critical System Protection evaluates the uniqueness of each agent based on the following attributes:

- Primary attributes
  - Agent name
  - Host name
  - IP address
- Secondary attributes
  - Domain name
  - Operating system type

See “Disabling duplicate agent registration” on page 251.

Disabling duplicate agent registration

Symantec Critical System Protection enables you to prevent registration of duplicate agents.

To disable duplicate agent registration

1. In the management console, click **Prevention View** or **Detection View**.
2. Click **Admin**.
3. Click **System Settings**.
4. Click **Agent settings**.
5. Check **Detect Duplicate Agent Registration**.
6. Check attributes under **Primary Agent Attributes for Duplicate Agent Identification** and **Secondary Agent Attributes for Duplicate Agent Identification.**

   You must select at least one primary attribute.
7. Click **Save**.

See "About the duplicate agent registration settings" on page 250.

Adding Active Directory servers

You must log on to Symantec Critical System Protection console as an administrator to define the Active Directory server information in the server configuration settings. You can define multiple Active Directory servers.

To add Active Directory servers

1. In the management console, click **Admin**.
2. Click **Settings**.
3. In the left pane, under **System Settings**, click **Directory Servers**.
4. In the toolbar, click the **Create a new Active Directory server** icon.
5. In the **New Active Directory Server Configuration** dialog box, type the Active Directory server name.
6. In the **Host** box, type the IP address or host name of the server.

   Or

   In the **Domain** box, type the fully qualified domain name of your Active Directory Servers.

7 To use Secure Sockets Layer (SSL) X.509 certificate-based channel encryption, check **Use encrypted communications** and then click **Test**.

Note: The Directory server must be configured to support SSL.

8 In the **Credentials of any user on the Active Directory** dialog box, type the **Username** and **Password** to validate the users account on the specified Active Directory server. This validates the communication between Symantec Critical System Protection Server and Directory Server.

9 Click **OK**.

See "Creating users with Active Directory credentials" on page 252.

Creating users with Active Directory credentials

If you choose Active Directory authentication for user accounts, you must specify the Active Directory server from the list of configured Active Directory servers and the domain name. When an Active Directory user logs on to the Symantec Critical System Protection console, the user must enter the user name in domain\user name format. You can assign an Active Directory user any role including the administrator role.

See "Assigning user accounts to a role" on page 243.

To create users with Active Directory credentials

1 In the management console, click **Admin**.

2 Click **Users**.

3 In the toolbar, click the **Create a new User** icon.

4 In the **New User** dialog box, on the **General** tab, specify the following information:

User name	Active Directory user name in Domain\User name format.
Description	A description of the user or the purpose of the account.
Active Directory User	Check **Active Directory User** to enable the **Active Directory Server** list box.
Active Directory Server	Select the Active Directory server name.

5 Click **OK**.

See "Adding Active Directory servers" on page 251.

See "Creating a user account" on page 236.

Viewing and exporting server configuration data

You must log on to Symantec Critical System Protection console as an administrator to view the management server settings in the console. The management server configuration data appears only for the management server that is connected to the console.

To view server configuration data

1. In the management console, click **Admin**.
2. Under **Admin**, click **Settings**.
3. In the left-hand pane, under **Server**, click **View Configuration**.
4. In the **Server Configuration Data** page, click any of the following tabs to view the server configuration data:

Tomcat	Displays the Tomcat configuration settings.
SCSP	Displays the SCSP Server properties.
JVM	Displays a snapshot of the server's Java Virtual Machine. Check **Auto-Refresh in 30 seconds** to receive latest Java Virtual Machine runtime statistics information.
Database	Displays the database runtime status.

You can export the server configuration data to a comma-separated value (CSV) file.

To export the server configuration data

1. In the toolbar, click the **Export Settings** icon.
2. In the **Export To** dialog box, select the file path in **Look In** box, and then click **Export**.

Managing the Tomcat server and Web applications

You use the Admin page in the management console to perform the following Apache Tomcat server and Web application tasks:

- Access the Tomcat Web Server Administration tool to administer the Tomcat server.

- Access the Tomcat Web Application Manager to manage Web applications
- Access the Server Status link to view the Tomcat Server Status.

To manage the Tomcat server and Web applications, you must log on to the selected Web page with the user name and password of a user who is assigned the Administrators role.

The Administration, Management, and Status tasks for the Tomcat server and Web applications are as follows:

Administration

Starts the Tomcat Web Server Administration tool, which provides a user interface for managing the Tomcat server. You must log in to the Tomcat Web server with a Symantec Critical System Protection user account that is assigned to the Administrators role.

From this option, you can configure the Tomcat, agent, and console services; data source, mail session, environment entry, and user database resources; and user, group, and role definitions.

Tomcat 5.5 documentation is available on the following Web site: http://jakarta.apache.org

Management

Starts the Tomcat Web Application Manager. The Tomcat Servlet/JSP Container Manager App provides a Web-based interface to the Web Application Manager that allows you to manage Web applications without having to shut down and restart the Tomcat server. You must log in to the Tomcat Web Server with a Symantec Critical System Protection user account that is assigned to the Administrators role.

Use this option to perform the following actions:

- Start, stop, reload, and undeploy Web applications.
- Deploy .war files without having to shut down and restart the Tomcat server.
- Request that an existing application reload itself, even if it is not declared reloadable in your Tomcat server configuration file.

Management also provide links to Tomcat documentation for the Tomcat Web Application Manager and the Manager App, as well as Tomcat Server Status information.

Status

Directly opens the same Tomcat Server Status information as the Server Status link on the Management page.

You must log on to the Tomcat Web Server with a Symantec Critical System Protection user account that is assigned to the Administrators role.

Accessing the Tomcat Web server administration tool

Access the Tomcat Web Server Administration tool.

To access the Tomcat Web server administration tool

1. In the management console, click **Admin**.
2. In the Server pane, click **Administration**.
3. In the Tomcat Web Server Administration Tool browser window, enter your user name and password, and then click **Login**.
4. To exit the Tomcat Web Server Administration Tool, click **Log Out**.

Accessing the Tomcat Web Application Manager

Access the Tomcat Web Application Manager.

To access the Tomcat Web Application Manager

1. Access the Tomcat Web Server Administration tool.
2. In the Server pane, click **Management**.
3. In the Connect to local host dialog, enter your user name and password, and then click **OK**.
4. To exit the Tomcat Web Application Manager, close the browser window.

Accessing the Tomcat Server Status

Open the same Tomcat Server Status information as the Server Status link on the Management page.

To access the Tomcat Server Status

1. Access the Tomcat Web Server Administration tool.
2. In the Server pane, click **Status**.
3. In the Connect to local host dialog, enter your user name and password, and then click **OK**.
4. To exit the Server Status, close the browser window.

About Tomcat terminology

You use the following terminology to administer the Tomcat server and Web applications:

- A server is the entire servlet container, which is called Catalina.

- A service is an intermediate component of a server that ties one or more connectors to one engine.
- A connector handles communications with the client. Many connectors are available with Tomcat.
- An engine is a request processing pipeline for a specific service. A service may have multiple connectors, so the engine receives and processes all requests from the connectors and gives the response back to the appropriate connector for transmission to the client.
- A host is a virtual host, an association of a network name such as www.mycompany.com, to the Tomcat server. An engine may contain multiple hosts.
- A context represents an individual Web application, which is associated with a corresponding host.
- A valve is a component that can be inserted into the request processing pipeline for the associated container (engine or host). Different valves have different processing capabilities.
- The variable name $CATALINA_HOME refers to the directory where Tomcat is installed. Relative path names used are relative to this directory. By default, this is <drive>:\Program Files\Symantec\Symantec Critical System Protection\Manager\tomcat.

Using the Tomcat Web Server Administration tool

You can access the Tomcat Web Server Administration Tool from the Admin page in the management console. Before you make configuration changes to the Tomcat server, you should become familiar with Tomcat Server terminology and functionality. Refer to the Tomcat 5.5 documentation on the following Web site:

http://jakarta.apache.org

Do not make modifications to the Tomcat server that you do not fully understand. Inappropriate configuration changes can affect the server's performance or debilitate it completely.

Note: The Tomcat server is configured to authenticate against the Symantec Critical System Protection user database. The User Definition node that is normally used to configure users, groups, and roles from the Tomcat Administration Tool is invalid for Symantec Critical System Protection.

Appendix A

Agent log files

This appendix includes the following topics:

About agent log files

Symantec Critical System Protection agent log files contain all events processed by an agent. Agent log files are stored on a local agent computer. 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).

The agent event log file directory locations are the default directory locations. If different directory locations were specified during agent installation, please refer to those locations.

The agent event log files are normal text files. You can use any text editor, such as Notepad, to view the contents.

Table A-1 lists the Symantec Critical System Protection agent log files.

Table A-1 Symantec Critical System Protection agent log files

File name	Description	Default location
SISIPSService.log	Agent log service. 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 A-1 Symantec Critical System Protection agent log files *(continued)*

File name	Description	Default location
SISIDSEvents*.csv	Event log. Contains all events recorded by the Symantec Critical System Protection agent. If bulk logging is enabled for the agent, this file is uploaded to the management server. The asterisk in the file name represents a version number.	Windows: Program Files\Symantec\Critical System Protection\Agent\scsplog\ UNIX: /var/log/scsplog/
SISIPSRTEvents*.csv	Real-time event log. Contains real-time events processed by the Symantec Critical System Protection agent. The is a temporary file that is used to speed processing of real-time events. Some or all of the events in the file (as configured in the agent's log rules) are forwarded to the management server. The file is deleted once processing is complete. The asterisk in the file name represents a version number.	Windows: Program Files\Symantec\Critical System Protection\Agent\scsplog\ UNIX: /var/log/scsplog/

How agent log files are processed

Event log files are stored on a local agent computer.

An agent processes log files in the following manner:

- The agent creates the following log files:
  - The agent creates SISIDSEvents.csv, which contains all events processed by the agent.
  - The agent creates SISIPSRTEvents.csv, which contains real-time events processed by the agent.
- A log file is closed and a new log file is opened based on the agent's log rotation schedule. Rollover of SISIDSEvents.csv and SISIPSRTEvents.csv are controlled by the same parameters, but the rollover decision is made independently for each file.

- Once a SISIDSEvents.csv log file is closed, the file is renamed and then compressed into a .zip file. The renamed file uses the format YYYYMMDD_HHMMSS_QQQQ-FT_HOSTNAME, where QQQQ is a sequence number, F is the file type, T is the OS type, and HOSTNAME is the agent name, host name, or IP address.
- Log files that are waiting to be uploaded for bulk logging are copied to the upload folder in C:\Program Files\Symantec\Critical System Protection\Agent\scsplog\upload.
- If the option to delete log files after processing is disabled, the SISIDSEvents.csv files that were successfully uploaded are copied to the archive folder in C:\Program Files\Symantec\Critical System Protection\Agent\scsplog\archive.

About bulk log transfer

Bulk log transfer lets you collect events of long-term interest without burdening the network or flooding the Symantec Critical System Protection database.

If bulk log transfer is enabled, the agent event log file is transmitted to the management server, where it is stored. When you are ready to load the events into the database, you run the bulk loader utility. This utility interprets a compressed bulk log file and populates the database with the events from the file.

How bulk log files are processed

Symantec Critical System Protection processes bulk log files as follows:

- The bulk logging thread in the IPS service wakes up every ten seconds to look for files that require file completion processing, and zip files that require uploading.
- Bulk log files are processed based on the upload interval, file interval, idle interval, and backlog interval.

Upload interval	The interval at which the bulk logging thread uploads files.
File processing interval	The interval at which the bulk logging thread performs file completion processing.
Idle interval	The interval at which the bulk logging thread checks for files to process or upload when there is no other processing to perform. Default value: 5 minutes

Backlog interval	The interval at which the bulk logging thread performs file processing or uploads when there is a backlog of files to process or upload. Default value: 1 minute

- Initially, the upload interval and the file processing interval are set to the idle interval.
- If files are backlogged, waiting for file completion processing, the file processing interval is set to the backlog interval. Otherwise, the file processing interval is set to the idle interval.
- If files are backlogged, waiting for uploading, the upload interval is set to the backlog interval. Otherwise, the upload interval is set to the idle interval.
- Upon waking up from the idle interval, the bulk logging thread gets the files to process or upload. The oldest files are processed or uploaded first.
- If a communications error occurs while uploading a file to the management server, the upload interval is set to the idle interval.
- The values for the idle interval and backlog interval are pre-configured in the IPS agent.ini file. The values are not user-configurable.

Loading bulk log events into the management server database

You use the bulk loader utility to load bulk log events into the Symantec Critical System Protection management server database.

The bulk loader utility interprets a compressed bulk log .zip file and then populates the management server database with the events from the file. Events are loaded into the management server database, in the analysis event table (the default) or the real-time event table (CSPEVENT option). You can view the events on the Monitors page.

The bulk loader utility is a command-line tool that communicates with the management server database independently of the Symantec Critical System Protection management console. When running the bulk loader utility, you must provide the path/file name of the compressed bulk log file.

By default, the bulk loader utility is installed in the following directory:

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

The command format is as follows:

```
bulkload [switch] <event_log_file>
```

<event_log_file> is the path and file name of the compressed event log .zip file.

The bulk loader utility command-line switches are as follows:

-m <managername>

This switch is for use with virtual agent log files. It creates a manager subgroup named <managername>, and dynamically registers a virtual agent when no matching agent GUID is found. It assigns all events in the bulk log file to the virtual agent.

Used with forwarded CSP events, the switch lets you specify the original manager's name so it can be saved in the events.

The switch is useful when creating a common CSP server to collect events from all deployed Symantec Critical System Protection management environments.

See "Capturing events forwarded from Symantec Critical System Protection" on page 288.

-f

Forces the bulk load file to be loaded into the management server database, ignoring verification and validation warnings.

The switch force-loads events, event if the agent is not found in the database.

-t <tablename>

Loads events into the ANALYSIS_EVENT or CSPEVENT table.

Use the <tablename> parameter to specify the table to use when loading the events.

Valid parameter values are as follows:

- ANALYSIS_EVENT (default)
  Events that are loaded into the ANALYSIS_EVENT table appear in the Analysis view on the Monitors page.
- CSPEVENT
  Events that are loaded into the CSPEVENT table appear in the normal event views along with real-time events.

?

Displays help for the bulk loader utility.

To load bulk log events into the management server database

1. From a command prompt, navigate to the following directory:

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

2. At the command prompt, type the bulkload command, and then press .

   The following command force-loads bulk log events as real-time events, and assigns the events to a virtual agent within the DMZ manager subgroup.

```
BULKLOAD -f -t CSPEVENT -m DMZ
F:\logfiles\Agent01\20070413_170421_001-EW_Agent01
```

Event variables

This appendix includes the following topics:

- About event variables
- List of event variables

About event variables

You use event variables to define event data.

Event variables are frequently used in detection policies. For example, in the Global_Watch_Policy, event variables are used to extract event data from an alert text file. For example:

```
*event_type={EVENT_TYPE},event_sev={EVENT_SEVERITY}*
```

In the Windows_Template_Policy and the UNIX_Template_Policy, the event variable {Virtual Agent Tag} is used to extract the virtual agent name from a text log file that contains events captured from multiple virtual agents. For example:

```
*agent name={VIRTUAL_TAG}*
```

List of event variables

Enclose event variable names in curly brackets { }.

Variable contents may vary by event type.

Table B-1 contains an alphabetical list of event variables.

Table B-1 Event variables

Variable name	Description
{AGENT_GUID}	Unique ID used by the management server to authenticate an agent.
{AGENT_VERSION}	Complete agent version (such as 5.2.0.194).
{ASSET_RID}	Reference key to the corresponding source agent record in the asset table on the Assets page.
{BINARYDATA}	Additional data. Typically used for error conditions that were encountered while processing events sent to the management server. The field contains the original event contents received at the server.
{DESCRIPTION}	Description captured from the source, or descriptive explanation of an event.
{DISPOSITION}	One of the following single letter codes that represents event disposition: ■ A (allow) ■ D (deny) ■ S (success ■ F (failure) ■ E (error)
{EVENT_CNT}	The event count is always one, unless it reflects the count of events represented by event consolidation.
{EVENT_DT}	The date (YYYY-MM-DD HH:MM:SS) that the event occurred.
{EVENT_DURATION}	For consolidated events, the time span from the first consolidated event to the last consolidated event.
{EVENT_END_DT}	The end date/time for a consolidated event. Always Null unless this is a consolidated event.
{LOCAL_EVENT_DT}	The event date expressed in local agent time.
{LOCAL_DAY}	The event day of month expressed in local agent time.
{LOCAL_DAYOFWEEK}	The event day expressed in local agent time.
{LOCAL_HOUR}	The event hour expressed in local agent time.
{LOCAL_MINUTE}	The event minute expressed in local agent time.
{LOCAL_MONTH}	The event month expressed in local agent time.
{LOCAL_YR}	The event year expressed in local agent time.

Table B-1 Event variables *(continued)*

Variable name	Description
{EVENT_PRIORITY}	The priority (0-100) assigned to the event.
{EVENT_SEVERITY}	One of the following single letter codes that represents event severity: ■ I (Information) ■ N (Notice) ■ W (Warning) ■ E (Error) ■ C (Critical) ■ M (Major) When setting the {Event Severity} variable, the E value cannot be assigned directly. The E value is logically derived when the event type equals MERR.

Table B-1 Event variables *(continued)*

Variable name	Description
{EVENT_TYPE}	Four-letter code representing the class and type of event. The first letter indicates general class (detection, prevention, management). The remaining letters indicate the sub-type. The codes are as follows: ■ DFWW (Filewatch Windows) ■ DFWU (Filewatch UNIX) ■ DRGW (Registry Watch) ■ DNTL (NT Log) ■ DSYS (Syslog) ■ DGEN (Generic Log) ■ DWTM (WTMP/BTMP) ■ DAUD (IDS Audit) ■ DUC2 (UNIX C2) ■ DIPS (IDS of IPS) ■ PNET/ANET (IPS Network) ■ PFIL/AFIL (IPS File) ■ PREG/AREG (IPS Registry) ■ PBOP/ABOP (IPS Overflow) ■ POSC/AOSC (IPS System Call) ■ PMNT/AMNT (IPS Mount) ■ PPST/APST (IPS PSET) ■ PCRE/ACRE (IPS Create) ■ PDES/ADES (IPS Destroy) ■ MERR (IDS Error) ■ MSTD (IDS Status) ■ MSTP (IPS Status) ■ MCOM (COMM Status) ■ MOVR (Agent Override) ■ MCON (Agent Config Status) ■ MSTA (Agent Status) ■ MSOF (Header) ■ MEOF (Trailer) ■ MREP (File Create) ■ MEFR (File Received) ■ MBIN (Server Error) ■ ECAT (Catalog Entry) ■ CAUD (Console Audit)

Table B-1 Event variables *(continued)*

Variable name	Description
HOSTADDR	IP address.
{HOSTNAME}	Computer name.
{IPOCT1} - {IPOCT4}	First through fourth octet of IP address of the source system.
{OPERATION}	OS system call or functions involved in the activity (for example, NtOpenKey).
{OSTYPE}	The operating system type, as follows: ■ W (Windows) ■ S (Solaris) ■ L (Linux) ■ H (HP-UX) ■ A (AIX)
{OSVERSION}	OS version string (such as XP Service Pack 1).
{POLICY_ID}	The identification number of the policy that generated the event.
{POST_DELAY}	Formatted display for the posting delay (nnnd hh:mm:ss). fxample: 12d 11:54:37. Time difference from when event occurred and time posted to database.
{PROCESS_NAME}	Name of the policy applied to the agent that triggered this event.
{PROCESS_PATH}	The process path and name.
{PROCESS_FULL_NAME}	The fully qualified process name.
{PROCESS_ID}	The ID assigned to the process.
{File Name}	Target resource name (such as win.ini). Useful for comparing events to specific resources regardless of installation location.
{RULE_ID}	The identification number of the policy rule that generated the event.
{RULE_NAME}	The name of the policy rule that generated the event.
{TARGET_INFO}	The target file name, registry path, or source name.
{SESSION_ID}	The session identification number of the session that generated the event.

Table B-1 Event variables *(continued)*

Variable name	Description
{SYSTEM_STATE}	The state of processing characteristics (event processing, prevention policy, event source) when the event occurred. Event processing states are as follows: ■ R (real-time event) ■ V (virtual event) ■ I (injected event) Prevention policy states are as follows: ■ P (prevention policy overridden) ■ X (prevention policy overridden except self-protection) ■ G (policy globally disabled) Event source states are as follows: ■ T (ITA forwarded) ■ C (CSP forwarded) ■ D (collector derived) ■ L (logwatch policy generated) ■ F (config tool generated) ■ S (IPS service generated) Other event attributes are as follows: ■ Z (Solaris non-global zone event) ■ M (special CSP manager virtual agent; flag only exists in database, not CSV) Not all virtual events are injected events. Not all injected events are virtual events. All virtual and injected events must also specify an event source. The Solaris zone flag indicates the event processed came from a non-global zone Examples of system state usage: ■ PR (Real-time event, prevention policy overridden) ■ IS (injected IPS service event) ■ VT (virtual ITA event)
{TIMEZONE_ADJ}	Positive or negative integer representing minutes offset from UTC time (for example, -300 is 5 hours).
{USER_TEXT}	Additional descriptive text that the policy author recorded about the event.
{USER_NAME}	The user name from the event.

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE1}	The value depends on event type, as follows: ■ DFWW: Old Permission Bitmask ■ DFWU: Old Permission Bitmask ■ DRGW: Old Value ■ DNTL: Event Type ■ DSYS: Priority ■ DGEN: Generic Type ■ DWTM: TMP Type ■ DUC2: Source ■ DIPS: IPS PSET ■ PNET/ANET: PSET ■ PFIL/AFIL: PSET ■ PREG/AREG: PSET ■ PBOP/ABOP: PSET ■ POSC/AOSC: PSET ■ PMNT/AMNT: PSET ■ PPST/APST: PSET ■ MERR: Message ID ■ MSTD: Message ID ■ MOVR: Override Duration ■ MSOF: Source Type ■ MEOF: Source Type ■ MBIN: VALUE1 ■ CAUD: Object Version

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE2}	The value depends on event type, as follows: ■ DFWW: New Permission Bitmask ■ DFWU: New Permission Bitmask ■ DRGW: New Value ■ DNTL: Event ID ■ DSYS: Msg ID ■ DGEN: Generic Attr 1 ■ DUC2: File Name ■ DIPS: IPS OS Result ■ PFIL/AFIL: OS Result ■ PREG/AREG: OS Result ■ POSC/AOSC: OS Result ■ PMNT/AMNT: OS Result ■ PPST/APST: Parent PID ■ PCRE/ACRE: Parent PID ■ MSOF: Component Version ■ MEOF: Component Version ■ MBIN: VALUE2 ■ CAUD: Object Type
{VALUE3}	The value depends on event type, as follows: ■ DFWW: Old Size ■ DFWU: Old Size ■ DNTL: Category ■ DGEN: Generic Attr 2 ■ DUC2: Group ■ DIPS: IPS CSP Result ■ PNET/ANET: LocalPort ■ PFIL/AFIL: CSP Result ■ PREG/AREG: CSP Result ■ PBOP/ABOP: CSP Result ■ POSC/AOSC: CSP Result ■ PMNT/AMNT: CSP Result ■ MBIN: VALUE3 ■ CAUD: Object Path

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE4}	The value depends on event type, as follows: ■ DFWW: New Size ■ DFWU: New Size ■ DNTL: Computer Name ■ DGEN: Generic Attr 3 ■ DUC2: Action ■ DIPS: IPS Value4 ■ PNET/ANET: LocalIP ■ PFIL/AFIL: Requested ■ PREG/AREG: Requested ■ PBOP/ABOP: Requested ■ POSC/AOSC: CSP Result ■ PMNT/AMNT: Device ■ MBIN: VALUE4 ■ CAUD: TableName
{VALUE5}	The value depends on event type, as follows: ■ DFWW: New File Name ■ DFWU: Old Link Name ■ DUC2: RemoteHost/IP ■ DIPS: IPS Value5 ■ PNET/ANET: RemoteIP ■ PBOP/ABOP: Injectee Process Name ■ PPST/APST: Parent Proc Name ■ PCRE/ACRE: Parent Proc Name ■ MREP: Checksum ■ MBIN: VALUE5
{VALUE6}	The value depends on event type, as follows: ■ DFWU: New Link Name ■ DUC2: ErrorText ■ DIPS: IPS Value6 ■ PNET/ANET: RemotePort ■ PBOP/ABOP: Injectee Process ID ■ MSTP: Param1 ■ MREP: CntTotal ■ MBIN: VALUE6

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE7}	The value depends on event type, as follows: ■ DFWW: Old Modification Date ■ DFWU: Old Modification Date ■ DIPS: IPS Value7 ■ PFIL/AFIL: NT Create Disp. ■ PREG/AREF: NT Create Opt. ■ PBOP/ABOP: Injectee Thread ID ■ MSTP: Param2 ■ MREP: Orig File Size ■ MBIN: VALUE7
{VALUE8}	The value depends on event type, as follows: ■ DFWW: New Modification Date ■ DFWU: New Modification Date ■ DIPS: IPS Value8 ■ PNET/ANET: Module Path ■ PFIL/AFIL: Module Path ■ PREG/AREF: Module Path ■ PBOP/ABOP: Module Path ■ POSC/AOSC: Module Path ■ PPST/APST: Module Path ■ PCRE/ACRE: Module Path ■ MSTP: Param3 ■ MREP: Compr File Size ■ MBIN: VALUE8

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE9}	The value depends on event type, as follows: ■ DFWW: Old Access Date ■ DFWU: Old Access Date ■ DIPS: IPS Value9 ■ PNET/ANET: Thread ID ■ PFIL/AFIL: Thread ID ■ PREG/AREF: Thread ID ■ PBOP/ABOP: Injector Thread ID ■ POSC/AOSC: Thread ID ■ PMNT/AMNT: Thread ID ■ PPST/APST: Thread ID ■ PCRE/ACRE: Thread ID ■ PDES/ADES: Thread ID ■ MSTP: Param4 ■ MREP: LocalFileName ■ MBIN: VALUE9
{VALUE10}	The value depends on event type, as follows: ■ DFWW: New Access Date ■ DFWU: New Access Date ■ DNTL: USRVAL1 ■ DSYS: USRVAL1 ■ DGEN: USRVAL1 ■ DWTM: USRVAL1 ■ DUC2: USRVAL1 ■ DIPS: Fmt OS Result ■ PNET/ANET: Port service ■ PFIL/AFIL: Fmt OS Result ■ PREG/AREF: Fmt OS Result ■ POSC/AOSC: Fmt OS Result ■ PMNT/AMNT: Fmt OS Result ■ MSTP: Param5 ■ MREP: Start TimeStamp ■ MBIN: VALUE10

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE11}	The value depends on event type, as follows: ■ DFWW: Old # of Hard Links ■ DFWU: Old # of Hard Links ■ DNTL: USRVAL2 ■ DSYS: USRVAL2 ■ DGEN: USRVAL2 ■ DWTM: USRVAL2 ■ DUC2: USRVAL2 ■ DIPS: R/W Flag ■ PFIL/AFIL: R/W Flag ■ PREG/AREF: R/W Flag ■ MREP: End TimeStamp ■ MBIN: VALUE11
{VALUE12}	The value depends on event type, as follows: ■ DFWW: New # of Hard Links ■ DFWU: New # of Hard Links ■ DNTL: USRVAL3 ■ DSYS: USRVAL3 ■ DGEN: USRVAL3 ■ DWTM: USRVAL3 ■ DUC2: USRVAL3 ■ MBIN: VALUE12
{VALUE13}	The value depends on event type, as follows: ■ DFWW: Old Creation Date ■ DFWU: Old Creation Date ■ DNTL: USRVAL4 ■ DSYS: USRVAL4 ■ DGEN: USRVAL4 ■ DWTM: USRVAL4 ■ DUC2: USRVAL4 ■ MSOF: Collector Agent GUID ■ MEOF: Collector Agent GUID ■ MBIN: VALUE13

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE14}	The value depends on event type, as follows: ■ DFWW: New Creation Date ■ DFWU: New Creation Date ■ DNTL: USRVAL5 ■ DSYS: USRVAL5 ■ DGEN: USRVAL5 ■ DWTM: USRVAL5 ■ DUC2: USRVAL5 ■ DIPS: IPS Event Cat ■ MSOF: Collector Host Name ■ MEOF: Collector Host Name ■ MBIN: VALUE14
{VALUE15}	The value depends on event type, as follows: ■ DFWU: DirectoryChange ■ DNTL: USRVAL6 ■ DSYS: USRVAL6 ■ DGEN: USRVAL6 ■ DWTM: USRVAL6 ■ DUC2: USRVAL6 ■ DIPS: IPS Event Type ■ MSOF: Collector IP Address ■ MEOF: Collector IP Adress ■ MBIN: VALUE15
{VALUE16}	The value depends on event type, as follows: ■ DFWU: SymlinkChange ■ DNTL: USRVAL7 ■ DSYS: USRVAL7 ■ DGEN: USRVAL7 ■ DWTM: USRVAL7 ■ DUC2: USRVAL7 ■ DIPS: IPS PolicyID ■ MBIN: VALUE16

Table B-1 Event variables *(continued)*

Variable name	Description
{VALUE17}	The value depends on event type, as follows: ■ DFWW: Old Owner ■ DFWU: Old Owner ■ DNTL: USRVAL8 ■ DSYS: USRVAL8 ■ DGEN: USRVAL8 ■ DWTM: USRVAL8 ■ DUC2: USRVAL8 ■ DIPS: IPS RuleID ■ MBIN: VALUE17
{VALUE18}	The value depends on event type, as follows: ■ DFWW: New Owner ■ DFWU: New Owner ■ DNTL: USRVAL9 ■ DSYS: USRVAL9 ■ DGEN: USRVAL9 ■ DWTM: USRVAL9 ■ DUC2: USRVAL8 ■ DIPS: IPS Event Severity ■ MBIN: VALUE18
{VALUE19}	The value depends on event type, as follows: ■ DFWW: Old Primary Group ■ DFWU: Old group ■ DNTL: USRVAL10 ■ DSYS: USRVAL10 ■ DGEN: USRVAL10 ■ DWTM: USRVAL10 ■ DUC2: USRVAL10 ■ DIPS: IPS SequenceNum ■ MBIN: VALUE19
{VALUE20}	The value depends on event type, as follows: ■ DFWW: New Primary Group ■ DFWU: New group ■ DIPS: IPS PolicyName ■ MBIN: VALUE20

Table B-1 Event variables *(continued)*

Variable name	Description
{VIRTUAL_TAG}	The name of the virtual agent. See the detection policies Windows_Template_Policy and UNIX_Template_Policy.

Virtual agent examples

This appendix includes the following topics:

Capturing static policy-based virtual events from a text log file

This example monitors a mainframe text log file and assigns all the events in the file to the same agent. Symantec Critical System Protection processes the virtual events indirectly via a text log rule in the Windows_Template_Policy.

In the example, the virtual agent Mainframe01 is registered manually. The collector host is a Symantec Critical System Protection agent that runs on Windows operating system. SalesMainframe is the name of the source system that originally processed the virtual events. The mainframe text log file is named mainframe01.txt; it is stored in C:\myevents on the Windows agent. All the events in the text log file are for virtual agent Mainframe01; each record corresponds to one virtual event. A user-defined application periodically populates C:\myevents\mainframe01.txt with new virtual events.

To capture static policy-based virtual events from a text log file

1. In the management console, on the Admin page, enable the virtual agent system-wide settings.
2. In the management console, on the Configs page, configure the log rules for the Windows agent that acts as the collector host.
3. On the Windows agent computer, copy mainframe01.txt to C:\myevents.
4. In the management console, manually register virtual agent Mainframe01.

   Specify the following values:

Name	Mainframe01
Agent Type	External
Host Name	SalesMainframe
IP Address	(Leave blank)
Manager Name	(Leave blank)
Operating System	Other

5. In the management console, on the Policies page, in the Symantec folder, edit the Windows_Template_Policy and create a text log rule.

   Enable the text log rule that you created, and specify the following rule options:

Text log path	C:\myevents\mainframe01.txt
Log file contains events coming from a virtual agent	Select this check box to indicate that the events in C:\myevents\mainframe01.txt are for a virtual agent. Value box: Mainframe01

   See the *Symantec Critical System Protection Detection Policy Reference Guide* for additional rule options.

6 Apply the modified Windows_Template_Policy to the Windows agent where the mainframe text log file is periodically populated with new virtual events.

7 In the management console, on the Monitors page, verify the virtual events.The Source Machine column should list Mainframe01. The Description column should list the events collected from C:\myevents\mainframe01.txt. The Source Type should be External. The Collector Host should be the Windows agent that collected the virtual events. The Collector tab should list the Windows agent that collected an event for Mainframe01.

Capturing variable policy-based virtual events from a text log file

This example monitors a text log file and assigns the events in the file to multiple virtual agents. Symantec Critical System Protection processes the virtual events indirectly via a text log rule in the Symantec Critical System Protection template policy.

In the example, the virtual agents are registered dynamically, based on the virtual agent name in the event data. The collector host is a Symantec Critical System Protection agent that runs on Windows operating system. The mainframe text log file is named mainframe01.txt; it is stored in C:\myevents on the Windows agent. The events in the text log file are from multiple virtual agents, and each record corresponds to one virtual event. A user-defined application periodically populates C:\myevents\mainframe01.txt with new virtual events.

To capture variable policy-based virtual events from a text log file

1 In the management console, on the Admin page, enable the virtual agent system-wide settings.

2 In the management console, on the Configs page, configure the log rules for the Windows agent that acts as the collector host.

3 On the Windows agent computer, copy mainframe01.txt to C:\myevents.

4 In the management console, on the Policies page, in the Symantec folder, edit the Windows_Template_Policy and create a text log rule.

Enable the text log rule that you created, and specify the following rule options:

Text log path	C:\myevents\mainframe01
Log file contains events coming from a virtual agent	Select this check box to indicate that the records in C:\myevents\mainframe01.txt are from a virtual agent. In the Value box, specify the virtual agent name variable as {VIRTUAL_TAG}.
Parse definitions	Select this check box to indicate that a parse string defines the virtual agent name. In the Value box, specify the parse string as agent name={VIRTUAL_TAG}

See the *Symantec Critical System Protection Detection Policy Reference Guide* for additional rule options.

5 Apply the modified Windows_Template_Policy to the Windows agent where the mainframe text log file is periodically populated with new virtual events.

6 In the management console, on the Monitors page, verify the virtual events.The Source Machine column should list the virtual agent name. The Description column should list the events collected from C:\myevents\mainframe01.txt. The Source Type should be External. The Collector Host should be the Windows agent that collected the virtual events. The Collector tab should list the Windows agent that collected all the virtual events.

Capturing virtual events derived from the Windows event log

This example captures virtual events derived from the Windows event log. The virtual agents are registered dynamically as part of the event flow.

The example assumes that an environment was set up for multiple remote systems to forward Windows event log events to a collector computer where Symantec Critical System Protection agent is installed. This setup includes configuring the remote computers to forward events, configuring the collector computer to collect events, and specifying which events are forwarded to the collector computer. The example assumes that the event log collectors were modified to automatically derive the source system from the event data and represent the events as coming from those systems.

To capture virtual events derived from the Windows event log

1. In the management console, on the Admin page, enable the system-wide virtual agent settings.
2. Set up an environment for multiple remote systems to forward Windows event log events to a collector computer where Symantec Critical System Protection agent is installed.
3. On the Windows agent, set the localagent.ini Derive Virtual Agents switch to 1, and restart the IDS service.
4. Perform activities on the remote systems that periodically forward events to the Windows agent.
5. In the management console, in the Master view, on the Assets page, verify dynamic virtual agent registration.

   Virtual agents not previously registered should be registered dynamically in the appropriate OS Forwarded Master group.
6. In the management console, on the Monitors page, verify the virtual events.

   Verify that the Source Machine column lists the virtual agent name, the Description column lists the events derived from the Windows event log, the Source Type is Derived, and the Collector Host is the Windows agent that collected the virtual events. Verify that the Collector tab lists the Windows agent that collected all the virtual events.

Capturing events from Symantec Intruder Alert

This example captures virtual events from legacy Symantec Intruder Alert systems and represents those events in the Symantec Critical System Protection management console.

The following tools are used to produce a periodic stream of ITA events:

- Symantec Intruder Alert IA Query Event Management Service (IAQuery) extracts events from ITA for external use.
- The IAQFLT tool, used in conjunction with IAQuery, translates extracted ITA events into the .csv format used by Symantec Critical System Protection.
- The IAQFLTCONFIG tool installs and configures IAQuery and IAQFLT.

In this example, IAQFLT and IAQuery produce a periodic stream of ITA events, which are collected and assigned to virtual agents. Virtual agents that were not previously registered are dynamically registered into the appropriate ITA Forwarded group and Manager sub-group.

To prevent losing ITA events that were generated prior to configuring the IDS Agent, perform the following steps before you run the ITA virtual agent tools.

To prevent losing ITA events that were generated prior to configuring the IDS Agent

1. Add the following field to %SCSPAgentRoot%/IDS/system/custlogwatch.ini.

   ```
   [File1]

   FileName=C:\iaqflt\iaqfltout*.log

   Delimiter=\n

   StringsToParse=0

   S1=

   Description=

   IncludeDelimiter=0

   InjectEvent=1

   SourceType=2

   [Log Files]

   Files=1
   ```

2. Restart the IDS Agent.
3. Before you run the iaqfltconfig tool, create the ITA formatted events output file that IDS will read.

   Create the file under the ITA virtual agent tool folder (for example, C:\iaqflt). The default ITA formatted events output file is iaqfltout.log.

To capture events from Symantec Intruder Alert

1. In the management console, on the Admin page, under System Settings, select the check boxes to allow virtual agents to register automatically and to allow virtual events to be stored in real time.
2. In the management console, manually register at least one virtual agent that is expected from the ITA event stream.

   All other virtual agents will be dynamically registered.
3. On the ITA host system, run IAQFLTCONFIG to produce a periodic stream of ITA events.

   See "About IAQFLTCONFIG" on page 285.

About IAQFLTCONFIG

You use the IAQFLTCONFIG tool to install and configure IAQuery and IAQFLT to produce a periodic stream of ITA events.

IAQuery uses the following files to extract events from ITA for external use:

config.iaq	IAQuery configuration file This file is included on the Symantec Critical System Protection installation CD.
iaqfltinp.log	IAQuery writes extracted events to this output file. The default output file is /<iaqflt_install_dir>/iaqfltinp.log. This output file becomes the input file for IAQFLT.
iaqflt.fmt	Defines the format of the output file. This file is included on the Symantec Critical System Protection installation CD.

The IAQFLT tool, used in conjuction with IAQuery, translates extracted ITA events into the .csv format that can be read by the Symantec Critical System Protection text log collector. IAQFLT runs as a period batch process using the OS batch scheduler. IAQFLT controls the execution of the IAQuery service, and gets its input from IAQuery.

IAQFLT uses the following files:

iaqfltinp.log	IAQFLT input file, which contains extracted events from IAQuery. The default file is /<iaqflt_install_dir>/iaqfltinp.log.
iaqfltout.log	IAQFLT writes.csv formatted records to the output. The default file is /<iaqflt_install_dir>/iaqfltout.log.
iaqflt.ini	Defines the format of the IAQFLT output file. This file is included on the installation CD.

IAQFLT parses events based on type, and extracts the relevant field data for the event types.

IAQFLT supports the following event types:

- NT Event (NT Event Log)
- NT Registry
- UNIX syslog

- UNIX wtmp
- UNIX btmp
- UNIX C2
- Log

Event types that are not recognized by IAQFLT as belonging to a collector-specific event are categorized as Generic. Events of this type are generally ITA or IAQuery internal status events.

Installing IAQFLTCONFIG

The IAQFLTCONFIG tool installs and configures IAQuery and IAQFLT.

To install IAQFLTCONFIG

1. Create an IAQFLT installation directory on the ITA host system.
2. Copy the following files from the Symantec Critical System Protection installation CD (tools/iaqflt/iaquery directory) to your IAQFLT installation directory:
   - config.iaq
   - iaqflt.fmt
   - iaqflt.ini
   - iaquery.exe

Running IAQFLTCONFIG

The IAQFLTCONFIG command format is as follows:

```
iaqfltconfig -q -f
--managers=<manager1, manager2, ...>
--user=<user_account>
--password=<user_password>
--output=<file_name>
--begin=<datetime> --format_file=<file_name>
```

Table C-1 shows the command-line parameters.

Table C-1 IAQFLTCONFIG command-line parameters

Parameter	Description
-q	Installs and registers IAQuery with the Service Control Manager.
-f	Installs IAQFLT, and creates a batch job to schedule its execution.
--managers=<manager1, manager2, ...>	The ITA managers that forward events to IAQuery. Example: --managers=192.168.0.150
--user=<user_account>	The ITA user account that is used to connect to the ITA managers. Example: --user=iaquery
--password=<user_password>	The ITA password that is used to connect to the ITA managers. Example: --password=secret
--output=<file_name>	The output file from IAQuery. Example: --output="C:\ITA2SCSP\iaqfltinp.log"
--format_file=<file_name>	The format file that describes how events are written to the IAQuery output file. Example: --format_file="C:\ITA2SCSP\config\iaqflt.fmt"
--begin=<datetime>	Instructs IAQuery to collect events starting from the specified date and time. Optional. --begin=mmddyyyyhhmm For example, --begin=103120070800 collects events starting from October 31, 2007 after 8 A.M. If the option is ommitted, then the default value is used. The default is the current time minus the iaqflt_query_offset value in iaqflt.ini. By default, iaqflt_query_offset is set to 15 minutes.

To run IAQFLTCONFIG

- At a command-line prompt, type and run IAQFLTCONFIG.

  For example:

  ```
  C:\ITA2SCSP>iaqfltconfig.exe -q -f --managers=192.168.0.150
  --user=iaquery --password=secret
   --output="C:\ITA2SCSP\iaqfltinp.log"
  --begin=103120070800
  --format_file="C:\ITA2SCSP\config\iaqflt.fmt"
  ```

Capturing events forwarded from Symantec Critical System Protection

This example forwards events from multiple Symantec Critical System Protection servers into a common Symantec Critical System Protection server (and console) that can display events from agents in the entire deployed environment.

Event capturing is accomplished using the bulk loader utility, which interprets a compressed bulk log file and populates the database with the events from the file.

See “Loading bulk log events into the management server database” on page 260.

In this example, multiple Symantec Critical System Protection servers exist in the demilitarized zone (DMZ), Richmond, Chicago, New York, and San Francisco. Each Symantec Critical System Protection management environment produces bulk log files. Using the bulk loader utility, events are force-loaded as real-time events to a virtual agent within the DMZ subgroup.

To capture CSP forwarded events

1. In the management console, on the Admin page, enable the system-wide virtual agent settings.
2. Establish a remote file share for each Symantec Critical System Protection management environment.
3. Use a batch script to force-load bulk log files on a scheduled basis into the common server.

   The batch script only needs to detect new files added since the last script execution.

   The following is a typical command to load a bulk log file:

   ```
   BULKLOAD -f -t CSPEVENT -m DMZ
   F:\logfiles\Agent01\20070413_170421_001-EW_Agent01
   ```

Agent config tool

This appendix includes the following topics:

About the agent config tool

The agent config tool is a command-line tool that you can use to view and modify a Symantec Critical System Protection agent's configuration.

The agent config tool has many uses, including the following:

- Set the management server port and host name
- Set the management server communications protocol
- Set the path to the SSL client certificate file
- Display and modify an agent's management server list
- Force an agent to re-register with the management server
- Enable or disable the state of IPS driver
- Force the agent log file to rollover

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

Windows agents	Named sisipsconfig on Windows agents, the agent config tool is located in the agent/ips/bin directory.
UNIX agents	Named sisipsconfig.sh on UNIX agents, the agent config tool is located in the agent/ips directory.

About the commands

The agent config tool commands are as follows:

Help	Describe all available commands and syntax.
-view	Display an agent's current management server list.
-host (-h)	Set the management server host name.
-port (-p)	Set the management server port.The port number must be between 1 and 65535.
-protocol	Set the management server communications protocol.
-certfile (-c)	Set the path to the SSL client certificate file.
-failbackinterval	Set the failback interval for the agent to try to communicate with the primary management server.
-test (-t)	Test the connection information with the nth server in the management server list.
-forcereg	Force the agent to re-register with the management server.
-setpolicy (-s)	Replace the current policy with the applied policy.
-resetpolicy (-r)	Replace the current policy with the default policy.
-toggleIPSState (-i)	Enable or disable the state of IPS driver.
-trace	Set Trace to the desired value.
-rollagent (-a)	Force the agent log file to rollover.
-rollcsv (-csv)	Force the CSV log file to rollover.
-retranslate (-n)	Force a policy re-translation.
-export (-export)	Print the config file.

Running the agent config tool

Note: To run the agent config tool, you must have administrative privilege.

If an agent's policy prevents running the agent config tool, do one of the following:

- Apply the null policy to the agent.

- Override the agent's current policy.

See the *Symantec Critical System Protection Prevention Policy Reference Guide* for details on policy override.

To run the agent config tool

1 Log on to the agent computer.

2 Navigate to the directory that contains the agent config tool.

3 At a command prompt, type `sisipsconfig` (Windows) or `sisipsconfig.sh` (UNIX) followed by a command, and then press **Enter** .

   Example: `sisipsconfig -view`

Index