Client Guide for Symantec™ Endpoint Protection Small Business Edition

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 12.00.00.00.00

Legal Notice

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

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 maintenance 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 Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers automatic software upgrade protection
- Global support that is available 24 hours a day, 7 days a week
- Advanced features, including Account Management Services

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

www.symantec.com/techsupp/

Contacting Technical Support

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

www.symantec.com/techsupp/

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/techsupp/

Customer service

Customer service information is available at the following URL:

www.symantec.com/techsupp/

Customer Service is available to assist with 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 maintenance contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs or manuals

Maintenance agreement resources

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

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

Additional enterprise services

Symantec offers a comprehensive set of services that allow you to maximize your investment in Symantec products and to develop your knowledge, expertise, and global insight, which enable you to manage your business risks proactively.

Enterprise services that are available include the following:

Symantec Early Warning Solutions	These solutions provide early warning of cyber attacks, comprehensive threat analysis, and countermeasures to prevent attacks before they occur.
Managed Security Services	These services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.
Consulting Services	Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.
Educational Services	Educational Services provide a full array of technical training, security education, security certification, and awareness communication programs.

To access more information about Enterprise services, please visit our Web site at the following URL:

www.symantec.com

Select your country or language from the site index.

Contents

Chapter 1

Introducing the Symantec Endpoint Protection Small Business Edition client

This chapter includes the following topics:

About the Symantec Endpoint Protection Small Business Edition client

The Symantec Endpoint Protection Small Business Edition client combines several layers of protection to proactively secure your computer against known and unknown threats and network attacks.

Figure 1-1 displays how the protection technologies work together to protect your computer.

Figure 1-1 Protection layers

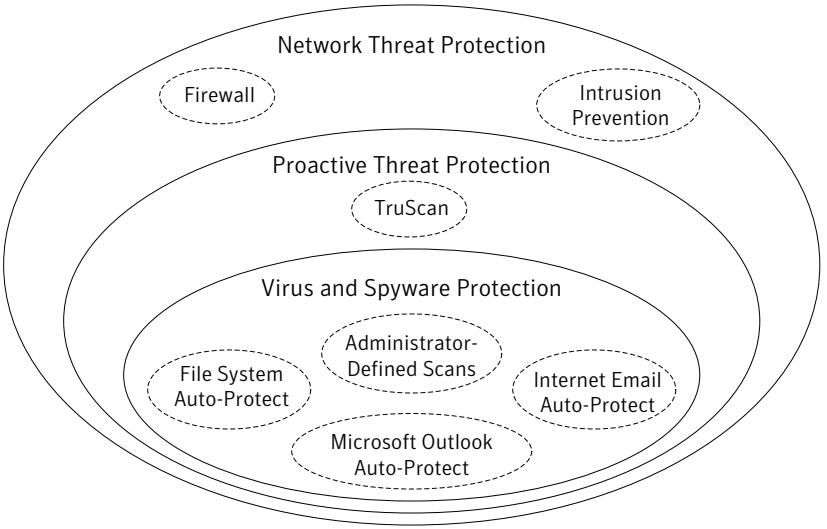


Table 1-1 describes each layer of protection.

Table 1-1 Types of protection

Layer	Description
Virus and Spyware Protection	This layer combats a wide range of threats, including spyware, worms, Trojan horses, rootkits, and adware. File System Auto-Protect continuously inspects all computer files for viruses and security risks. Internet Email Auto-Protect scans the incoming and outgoing email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer (SSL). Microsoft Outlook Auto-Protect scans incoming and outgoing Outlook email messages. See "Managing protection scans" on page 43.

Table 1-1 Types of protection *(continued)*

Layer	Description
Proactive Threat Protection	This layer uses a unique Symantec technology called TruScan proactive threat technology. TruScan proactive threat scans protect against unknown, or zero-day, threats by analyzing suspicious behavior from an application or process. If your administrator enabled TruScan proactive threat scans, the scans run in the background. You can specify the scan to ignore certain files. See "Excluding a process from TruScan proactive threat scans" on page 60.
Network Threat Protection	This layer comprises firewall and intrusion prevention protection. The rules-based firewall prevents unauthorized users from accessing your computer. The intrusion prevention system automatically detects and blocks network attacks. See "Managing Network Threat Protection" on page 64.

Your administrator manages the protection technologies and uses a management server to download them to your client computer.

The client automatically downloads virus definitions and product updates from a management server at your company. Users who travel with portable computers can get virus definitions and product updates directly from .

See "Updating the client's protection" on page 39.

Key features of Symantec Endpoint Protection Small Business Edition

Table 1-2 displays the main features that the client includes to protect your computer.

Table 1-2 Key features of the client

Feature	Description
Protection technologies	The client uses the protection technologies to protect your computer in the following ways: See "About the Symantec Endpoint Protection Small Business Edition client" on page 9. ■ Scans client computers for known viruses and security risks. See "About the types of protection scans" on page 48. ■ Detects and repairs the effects of known viruses and security risks. See "How scans respond to a virus or risk detection" on page 52. ■ Protects Microsoft Exchange servers against email-borne viruses, spam, and security risks. See "Adjusting virus and spyware scan settings" on page 56. ■ Analyzes application behaviors and network communications to detect and actively block against unknown threats. ■ Automatically detects and blocks network attacks. See "About Network Threat Protection" on page 63. ■ Prevents unauthorized users from accessing the computers and networks that connect to the Internet. See "How the firewall works" on page 65.
Centrally managed or self-managed client	Your administrator installs the client so that either you or your administrator manages your computer's protection. See "About centrally managed clients and self-managed clients" on page 33.
Alerts and notifications	The client informs you when the client detects a virus or blocks a network attack. You can also respond to a virus or security risk detection. See "About responding to alerts and notifications" on page 19.

Where to get more information

If you need more information, you can access the online Help.

You can obtain additional information about viruses and security risks from the Symantec Security Response Web site at the following URL:

http://securityresponse.symantec.com

Accessing online Help

The client online Help system has general information and procedures to help you keep your computer safe from viruses and security risks.

Note: Your administrator may have elected not to install the Help files.

To access online Help

- In the main window, do one of the following:
  - Click **Help**, and then click **Help Topics**.
  - Click **Help** on any of the individual dialog boxes.
    Context-sensitive Help is available only in screens on which you can perform actions.
  - Press **F1** in any window. If there is context-sensitive Help available for that window, context-sensitive Help appears. If context-sensitive Help is not available, the full Help system appears.

Accessing the Symantec Security Response Web site

If you are connected to the Internet, you can visit the Symantec Security Response Web site to view items such as the following:

- The Virus Encyclopedia, which contains information about all known viruses
- Information about virus hoaxes
- White papers about viruses and virus threats in general
- General and detailed information about security risks

To access the Symantec Security Response Web site, use the following URL:

- In your Internet browser, type the following Web address:
  http://securityresponse.symantec.com

Technical Support resources

Table 1-3 lists the Symantec Web sites where you can find more information .

Table 1-3 Symantec Web sites

Types of information	Web address
Symantec Endpoint Protection Small Business Edition trialware	http://www.symantec.com/business/products/downloads/
Public Knowledge Base Releases Manuals and documentation updates Contact options Release Notes and additional post-release information	http://www.symantec.com/business/support/overview.jsp?pid=55357
Virus and other threat information and updates	http://securityresponse.symantec.com
Product news and updates	http://enterprisesecurity.symantec.com
Symantec Endpoint Protection Small Business Edition forums	http://www.symantec.com/community
Free online technical training	http://www.symantec.com/education/endpointsecurity

Chapter 2

Getting started with the client

This chapter includes the following topics:

Getting started on the Status page

When you open the client, the main window and the Status page appears.

Table 2-1 displays the main tasks that you can perform from the client's menu bar and Help option.

Table 2-1 Client main window

Click this option	To do these tasks
Help	Access the main online Help and perform the following tasks on the client: ■ View information about your computer, the client, and the client's protection. ■ View information about the client's connection status with the management server. You can also try to connect to the server, if necessary. ■ View any client log. ■ Import and export security policies and communication settings on a self-managed client. ■ View and export debugging logs and a troubleshooting file to help your administrator diagnose a problem with the client or the client's protection. ■ Download a support utility tool to diagnose common issues with the client.
Status	View whether the computer is protected and whether the computer's license is current. The colors and alert icons in the Status page show you which technologies are enabled and protecting the client. See "About alert icons on the Status page" on page 17. You can: ■ Enable or disable one or more protection technologies. See "Enabling and disabling protection technologies" on page 35. ■ View whether you have the latest definitions files for Virus and Spyware Protection, Proactive Threat Protection, and Network Threat Protection. ■ Run an active scan. See "Scanning your computer immediately" on page 31. ■ View the threat list and view the results of the last virus and spyware scan.
Scan for threats	Enable you to do the following tasks: ■ Run an active scan or full scan immediately. See "Scanning your computer immediately" on page 31. ■ Create a scheduled, startup, or on-demand scan. See "Scheduling a user-defined scan" on page 53. See "Scheduling a scan to run on demand or when the computer starts up" on page 55.

Table 2-1 Client main window *(continued)*

Click this option	To do these tasks
Change settings	Configure settings for the following protection technologies and features: ■ Enable and configure Auto-Protect settings. See "Adjusting virus and spyware scan settings" on page 56. ■ Configure the firewall settings and the intrusion prevention system settings (self-managed client only). ■ View and add exceptions to scans. See "About excluding items from being scanned" on page 58. ■ Display the notification area icon (self-managed client only). See "About the notification area icon" on page 18. ■ Create a schedule to download content and product updates to the client (self-managed client only). See "Updating your protection on a schedule" on page 40.
View quarantine	View the viruses and security risks that the client has detected and quarantined. You can restore, delete, clean, export, and add files in the quarantine. See "About quarantining files" on page 60.
LiveUpdate	Run LiveUpdate immediately. LiveUpdate downloads the latest content definitions and product updates from a management server that is located within your company's network. See "Updating your protection immediately" on page 40.

About alert icons on the Status page

The top of the Status page displays various alert icons to indicate the protection status of the computer.

Table 2-2 displays the different types of alert icons and what the alert icons mean.

Table 2-2 Status page alert icons

Icon	Description
	Shows that each protection is enabled. Client computers that run Windows XP x64 Edition or Windows Server 2000, 2003, and 2008 do not support Proactive Threat Protection. On these operating systems, the green alert notification remains green although the status is Off.

Table 2-2 Status page alert icons *(continued)*

Icon	Description
	Warns you that the client computer virus definitions are out of date. To receive the most current virus definitions, you can run LiveUpdate immediately. See "Updating the client's protection" on page 39.
	Shows that one or more protections are disabled or that the client has an expired license. To enable a protection, you click Fix. See "Enabling and disabling protection technologies" on page 35.

About the notification area icon

The client uses a notification area icon to indicate whether the client is online or offline and whether the client computer is adequately protected. You can right-click this icon to display frequently used commands. The icon is located in the lower-right hand corner of the desktop.

Note: On centrally managed clients, the notification area icon does not appear.

Table 2-3 displays the Symantec Endpoint Protection Small Business Edition client status icons.

Table 2-3 Symantec Endpoint Protection Small Business Edition status icons

Icon	Description
	The client runs with no problems. It is either offline or self-managed. Self-managed clients are not connected to a server.
	The client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer. The icon displays a green dot.
	The client has a minor problem. For example, the virus definitions may be out of date. The icon displays a yellow dot with a black exclamation mark.
	The client does not run, has a major problem, or has at least one protection technology disabled. For example, Virus and Spyware Protection may be disabled. The icon displays a white dot with a red outline and a red line across the dot.

Chapter 3

Responding to alerts and notifications

This chapter includes the following topics:

About responding to alerts and notifications

The client works in the background to keep your computer safe from malicious activity. Sometimes the client needs to notify you about an activity or to prompt you for feedback.

Table 3-1 displays the types of messages you might see and need to respond to.

Table 3-1 Types of alerts and notifications

Alert	Description
Scan results or Detection Results dialog box	If a scan detects a virus or a security risk, the Detection Results dialog box appears with details about the infection. The dialog box also displays the action that the scan performs on the risk. You usually do not need to take any further actions other than to review the activity and to close the dialog box. You can take action if necessary, however. See "About scan results" on page 20.
Other message dialog boxes	You may see pop-up messages for the following reasons: ■ The client asks you to allow or block an application. See "Responding to messages that ask you to allow or block an application" on page 23. ■ The client's evaluation license has expired. See "Responding to messages about an expired license" on page 24.

Notification area icon messages	Notifications that appear above the notification area icon occur in the following situations:
	
	■ The client blocks an application. For example, you might see the following notification:
	
	`Traffic has been blocked from this application: (application name)`
	
	If the client is configured to block all traffic, these notifications appear frequently. If your client is configured to allow all traffic, these notifications do not appear.
	■ When the client detects a network attack against your computer. You might see the following type of notification:
	
	`Traffic from IP address 192.168.0.3 is blocked from 10/10/2006 15:37:58 to 10/10/2006 15:47:58. Port Scan attack is logged.`
	
	You do not need to do anything else other than to read the messages.

About scan results

For centrally managed clients, your administrator typically configures a full scan to run at least one time each week. For self-managed clients, an automatically

generated Active Scan runs when you start up your computer. By default, Auto-Protect runs continuously on your computer.

See "About centrally managed clients and self-managed clients" on page 33.

When the scans run, a scan dialog box appears to report progress and to show the results of the scan. When the scan is completed, the results appear in the list. If the client detects no viruses or security risks, the list remains empty and the status is completed.

If the client detects risks during the scan, the scan results dialog box shows results with the following information:

- The names of the viruses or security risks
- The names of the infected files
- The actions that the client performs on the risks

If the client detects a virus or security risk, you might need to act on an infected file.

See "Responding to a virus or risk detection" on page 21.

Note: For centrally managed clients, your administrator might choose to hide the scan results dialog box. If the client is self-managed, you can display or hide this dialog box.

If you or your administrator configure the client software to display a scan results dialog box, you can pause, restart, or stop the scan.

See "Pausing and delaying scans" on page 32.

Responding to a virus or risk detection

When an administrator-defined scan, user-defined scan, or Auto-Protect scan runs, you might see a scan results dialog box. You can use the scan results dialog box to act on the file immediately.

See "How scans respond to a virus or risk detection" on page 52.

You can act on the file in the following situations:

- The client detects a virus or security risk.
  The scan might have detected a virus or risk, but the file might not have been infected.
- You want the client to perform a different action on the file.

For example, you might decide to delete a cleaned file because you want to replace it with an original file.

You can also open the Quarantine or the log to act on the file later.

To respond to a virus or risk detection

1. Do one of the following actions:
   - In the scan results dialog box or Detection Results dialog box, select the files that you want to act on.
   - In the client, click **Help >Troubleshooting > Logs**. In the log view, select the files that you want to act on.
2. Right-click the file, and then select one of the following options:

Clean (viruses only)	Removes the virus from the file.
Exclude	Excludes the file from being scanned again. See "About excluding items from being scanned" on page 58.
Delete Permanently	Deletes the infected file and all side effects. For security risks, use this action with caution. In some cases, if you delete security risks you might cause an application to lose functionality.
Undo Action Taken	Reverses the action taken.
Move To Quarantine	Places the infected files in the Quarantine. For security risks, the client also tries to remove or repair the side effects. In some cases, if the client quarantines a security risk, it might cause an application to lose functionality. See "About quarantining files" on page 60.
Properties	Displays the information about the virus or security risk.

   In some cases, the action might not be available.
3. If the client needs to terminate a process or application or stop a service, click **Remove Risks Now**.

   You might not be able to close the dialog box if risks in the dialog box require you to take action.

   See "Responding to a virus or risk detection" on page 21.

4 In the Remove Risk dialog box, click one of the following options:

- **Yes**
  The client removes the risk. The removal of the risk might require a restart. Information in the dialog box indicates whether or not a restart is required.
- **No**
  When you close the results dialog box, the Remove Risk dialog box appears. The dialog box reminds you that you still need to take action. However, the Remove Risk dialog box is suppressed until you restart your computer.

5 Click **Close**.

6 To find out more about detection, check the following logs:

- Check the Risk log or Scan log to find out more about the potentially infected file.
- Check the Traffic Log to look for a lot of network traffic on the port or ports that the virus or security risk used.

See "Viewing the logs" on page 27.

Responding to messages that ask you to allow or block an application

When an application on your computer tries to access the network, the client might ask you to allow or block the application. You may see a notification that asks you whether you want to allow or block an application or service from accessing the network. For example, you might want to block an application that you think is unsafe to run.

See "How the firewall rules work" on page 67.

This type of notification appears for one of the following reasons:

- The application asks to access your network connection.
- An application that has accessed your network connection has been upgraded.
- Your administrator updated the client software.
- The client switches users through Fast User Switching.

You might see the following type of message, which tells you when an application tries to access your computer:

```
IEXPLORE.EXE is attempting to access the network.
Do you want to allow this program to access the network?
```

To respond to messages that ask you to allow or block an application

1. In the Symantec Endpoint Protection dialog box, to suppress this message the next time the application tries to access the network, click **Remember my answer, and do not ask me again for this application**.
2. Do one of the following actions:
   - To allow the application to access the network, click **Yes**.
   - To block the application from accessing the network, click **No**.

   For more information about the connection and the application, click **Detail >>**.

Responding to messages about an expired license

The client uses a license to update the virus definitions for scans and to update the client software. The client may use an evaluation license or a paid license. If either license has expired, the client does not update any content or the client software.

See "Updating the client's protection" on page 39.

Table 3-2 Types of licenses

License type	Description

Evaluation license	If an evaluation license has expired, the top of the client's Status pane is red and displays the following message:
	
	`Evaluation License has expired.`
	
	`All content download will discontinue on` *`date`*`. Please contact your Administrator to purchase a full Symantec Endpoint Protection License.`
	
	You can also view the expiration date by clicking Help > About.

Table 3-2 Types of licenses *(continued)*

License type	Description

Paid license	If a paid license has expired, the top of the client's Status pane is yellow and displays the following message:
	
	`Virus and Spyware Protection definitions are out of date.`
	
	If you click Fix, the following message appears:
	
	`Your license has expired. The content definition updates have been disabled. Please contact your Administrator to review the Symantec Endpoint Protection license.`
	
	See "Viewing the logs" on page 27.

For either type of license, you must contact your administrator to update or renew the license.

About logs

Logs contain information about client configuration changes, security-related activities, and errors. These records are called events. The logs display these events with any relevant additional information.

Security-related activities include information about virus detections, computer status, and the traffic that enters or exits your computer. If you use a managed client, its logs can be regularly uploaded to the management server. An administrator can use their data to analyze the overall security status of the network.

Logs are an important method for tracking your computer's activity and its interaction with other computers and networks. You can use the information in the logs to track the trends that relate to viruses, security risks, and attacks on your computer. If several people use the same computer, you might be able to identify who introduces risks, and help that person to use better precautions.

For more information about a log, you can press F1 to view the help for that log.

Table 3-3 describes the event types that each log displays.

Table 3-3 Client logs

Log	Description
Scan Log	Contains entries about the scans that have run on your computer over time.
Risk Log	Contains entries about viruses and security risks, such as adware and spyware, that have infected your computer. Security risks include a link to the Symantec Security Response Web page that provides additional information.
Virus and Spyware Protection System Log	Contains information about system activities on your computer that are related to viruses and security risks. This information includes configuration changes, errors, and definitions file information.
Threat Log	Contains information about the threats that TruScan proactive threat scans have detected on your computer. These include the commercial applications that can be used for malicious purposes. Examples are Trojan horses, worms, or keyloggers, or mass-mailing worms, macro viruses, and script-based threats.
Proactive Threat Protection System Log	Contains information about system activities on your computer that are related to TruScan proactive threat scans.
Tamper Protection Log	Contains entries about the attempts to tamper with the Symantec applications on your computer. These entries contain information about the attempts that Tamper Protection detected or detected and thwarted.
Traffic Log	Contains the events that concern firewall traffic and intrusion prevention attacks. The log contains information about the connections that your computer makes through the network. The Network Threat Protection logs can help you to detect potentially threatening activity such as port scanning. They can also be used to trace traffic back to its source. You can also use Network Protection logs to help troubleshoot connectivity problems or possible network attacks. The logs can tell you when your computer has been blocked from the network and help you to determine why your access has been blocked.
Packet Log	Contains information about the packets of data that enter or leave through the ports on your computer. By default, the Packet log is disabled. On a managed client, you cannot enable the Packet Log. On an unmanaged client, you can enable the Packet Log.

Table 3-3 Client logs *(continued)*

Log	Description
Security Log	Contains information about the activities that were directed toward your computer that can potentially pose a threat. For example, activities such as denial-of-service attacks, port scans, and executable file alterations are examples.
Client Management System Log	Contains information about all of the operational changes that have occurred on your computer. Examples include activities such as when a service starts or stops, the computer detects network applications, or when the software is configured.
Debug Logs	Contains information about the client, scans, and the firewall for troubleshooting purposes. Your administrator may ask you to enable or configure the logs and then export them.

Viewing the logs

You can view the logs on your computer to see the details of events that have occurred.

To view a log

1. In the client, click **Help > Troubleshooting**.
2. In the Troubleshooting dialog box, click **Logs**.
3. In the Logs panel, click the name of the log, and click **View Log**.

Chapter 4

Making sure that your computer is protected

This chapter includes the following topics:

Managing your computer's protection

By default, your client computer is protected and you should not need to configure the client. However, you may want to monitor your protection for the following reasons:

- Your client runs a self-managed client.
  Once a self-managed client is installed, only you have control over your computer's protection. A self-managed client is protected by default. But you may need to modify the computer's protection settings.
  See "About centrally managed clients and self-managed clients" on page 33.
- You want to enable or disable one or more protection technologies.
- You want to verify that you have the latest virus definitions.
- You have heard of a recent virus and want to run a scan.

Table 4-1 displays the process to make sure that your computer is protected.

Table 4-1 Process for managing your computer's protection

Step	Description
Respond to alerts or notifications	Respond to messages that appear, asking you for input. For example, a scan may have found a detection and displays a scan results dialog box that asks you to act on the detection. See "About responding to alerts and notifications" on page 19.
Check the protection status	Regularly check the Status page to determine that all the types of protections are enabled. See "Getting started on the Status page" on page 15. See "Enabling and disabling protection technologies" on page 35.
Update virus definitions (Self-managed client only)	On a self-managed client, make sure that the latest virus definitions are installed on your computer. ■ Check whether you have the latest protection updates. You can check the date and number of these definitions files on the client's Status page, under each type of protection. ■ Obtain the latest protection updates. See "Updating the client's protection" on page 39.
Scan your computer	Run a scan to see if the computer or your email application has any viruses. By default, the client scans the computer when you turn it on, but you can scan the computer at any time. See "Scanning your computer immediately" on page 31.
Adjust protection settings	In most cases, the default settings provide adequate protection for your computer. If necessary, you can decrease or increase the following types of protection: ■ Scheduling additional scans See "Managing protection scans" on page 43. ■ Adding firewall rules (self-managed client only) See "Managing Network Threat Protection" on page 64.
View logs for detections or attacks	Check the logs to see if your client has found a virus detection or network attack. See "Viewing the logs" on page 27.

Table 4-1 Process for managing your computer's protection *(continued)*

Step	Description
Update the security policy (Centrally managed client only)	Check that the client received the latest security policy. A security policy includes the most current protection technology settings for your client. The security policy is updated automatically. To ensure that you have the latest policy, you can update it manually by right-clicking the client notification area icon and clicking Update Policy. See "About the notification area icon" on page 18.

Scanning your computer immediately

You can manually scan for viruses and security risks at any time. You should scan your computer immediately if you recently installed the client, or if you think you have recently received a virus.

See "Scheduling a scan to run on demand or when the computer starts up" on page 55.

For more information on the options on each dialog box, click Help.

To scan your computer immediately

- Do one of the following actions:
  - In the client, on the Status page, next to Virus and Spyware Protection, click **Options > Run Active Scan**.
  - In the client, in the sidebar, click **Scan for threats**.
    Do one of the following actions:
    - Click **Run Active Scan**.
    - Click **Run Full Scan**.
    - In the scan list, right-click any scan, and then click **Scan Now**.
      The scan starts. A progress window appears on your computer to show the progress of the scan and the results.
      See "About scan results" on page 20.

  You can also pause or cancel the scan.

  See "Pausing and delaying scans" on page 32.

Pausing and delaying scans

The pause feature lets you stop a scan at any point during the scan and resume it at another time. You can pause any scan that you initiate.

Your administrator determines whether you can pause an administrator-initiated scan. If the Pause Scan option is not available, your administrator disabled the pause feature. If your administrator has enabled the Snooze feature, you can delay an administrator-scheduled scan for a set interval of time.

When a scan resumes, it starts from where the scan stopped.

Note: If you pause a scan while the client scans a compressed file, the client might take several minutes to respond to the pause request.

To pause a scan you initiated

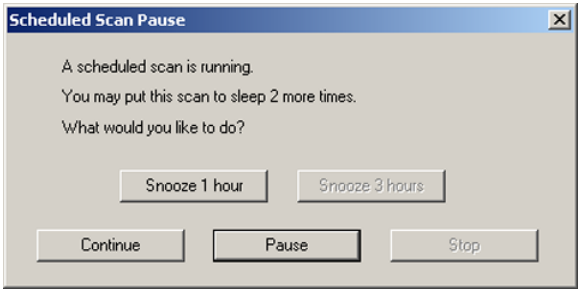
1 When the scan runs, in the scan dialog box, click **Pause Scan**.

The scan stops where it is and the scan dialog box remains open until you start the scan again.

2 In the scan dialog box, click **Resume Scan** to continue the scan.

To pause or delay an administrator-initiated scan

1 When an administrator-initiated scan runs, in the scan dialog box, click **Pause Scan**.



2 In the Scheduled Scan Pause dialog box, do one of the following actions:

- To pause the scan temporarily, click **Pause**.
- To delay the scan, click **Snooze 1 hour** or **Snooze 3 hours**.
  Your administrator specifies the period of time that you are allowed to delay the scan. When the pause reaches the limit, the scan restarts from where it began. Your administrator specifies the number of times that you can delay the scheduled scan before this feature is disabled.
- To continue the scan without pausing, click **Continue**.

About centrally managed clients and self-managed clients

Your administrator can install the client as either a centrally managed client (administrator-managed installation) or a self-managed client (standalone installation).

Table 4-2 Differences between a centrally managed client and a self-managed client

Client type	Description
Centrally managed client	A centrally managed client communicates with a management server in your network. The administrator configures the protection and the default settings, and the management server downloads the settings to the client. If the administrator makes a change to the protection, the change is almost immediately downloaded to the client. Administrators can change the level at which you interact with the client in the following ways: ■ The administrator manages the client completely. You are not required to configure the client. All the settings are locked or unavailable, but you can view information about what the client does on your computer. ■ The administrator manages the client, but you can change some client settings and perform some tasks. For example, you may be able to run your own scans and manually retrieve client updates and protection updates. The availability of the client settings, as well as the values of the settings themselves, can change periodically. For example, a setting might change when your administrator updates the policy that controls your client's protection.

Table 4-2 Differences between a centrally managed client and a self-managed client *(continued)*

Client type	Description
Self-managed client	A self-managed client does not communicate with a management server and an administrator does not manage the client. A self-managed client can be one of the following types: ■ A standalone computer that is not connected to a network, such as a home computer or a laptop. The computer must include a Symantec Endpoint Protection Small Business Edition installation that uses either the default option settings or administrator-preset settings. ■ A remote computer that connects to the corporate network that must meet security requirements before it connects. The client has default settings when it is first installed. After the client is installed, you can change all the client settings and perform all the protection tasks.

See "Checking whether the client is centrally managed or self-managed" on page 34.

Table 4-3 describes the differences in the user interface between a centrally managed and self-managed client.

Table 4-3 Differences between a centrally managed client and a self-managed client by feature area

Feature area	Centrally managed client	Self-managed client
Virus and Protection options	The client displays a locked padlock option and the option appears dimmed for the options that you cannot configure.	The client does not display either a locked padlock or an unlocked padlock.
Client management and Network Threat Protection settings	The settings that the administrator controls do not appear.	All the settings appear.

Checking whether the client is centrally managed or self-managed

To check how much control you have to configure protection on your client, you first check whether your client is centrally managed or self-managed. You can

configure more settings on a self-managed client than on a centrally managed client.

See "About centrally managed clients and self-managed clients" on page 33.

To check whether the client is centrally managed or self-managed

1. On the Status page, click **Help > Troubleshooting**.
2. In the Troubleshooting dialog box, click **Management**.
3. In the Management panel, under General Information, next to Server, look for the following information:
   - If the client is centrally managed, the Server field displays either the management server's address or the text **Offline**.
     The address can be an IP address, DNS name, or NetBIOS name. For example, a DNS name might be SEPMServer1. If the client is centrally managed but not currently connected to a management server, this field is **Offline**.
   - If the client is self-managed, the Server field is **Self-managed**.
4. Click **Close**.

Enabling and disabling protection technologies

In general, you always want to keep the protection technologies enabled on your computer.

If you have a problem with your client computer, you might want to temporarily disable either all the protection technologies or individual protection technologies. For example, if you have trouble with an application that does not run or does not run correctly, you might want to disable Network Threat Protection.

If you still have the problem after you disable all protection technologies, you know that the problem is not the client.

Table 4-4 describes the reasons why you might want to disable each protection technology.

Table 4-4 Purpose for disabling a protection technology

Protection technology	Purpose for disabling the protection technology
Virus and Spyware Protection	If you disable Virus and Spyware Protection, you disable Auto-Protect only. The scheduled or startup scans still run if you or your administrator has configured them to do so. You or the administrator can enable or disable Auto-Protect for the following reasons: ■ Auto-Protect might block you from opening a document. For example, if you open a Microsoft Word that has a macro, Auto-Protect may not allow you to open it. If you know the document is safe, you can disable Auto-Protect. ■ Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, you might get a warning when you install new computer applications. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect. ■ Auto-Protect may interfere with Windows driver replacement. ■ Auto-Protect might slow down the client computer. See "Enabling or disabling Auto-Protect" on page 37.
Proactive Threat Protection	You might want to disable Proactive Threat Protection for the following reasons: ■ You see too many warnings about the threats that you know are not threats. ■ Proactive Threat Protection might slow down the client computer. See "Enabling or disabling Proactive Threat Protection" on page 38.
Network Threat Protection	You might want to disable Network Threat Protection for the following reasons: ■ You install an application that might cause the firewall to block it. ■ A firewall rule or firewall setting blocks an application due to an administrator's mistake. ■ The firewall or the intrusion prevention system causes network connectivity-related issues. ■ The firewall might slow down the client computer. See "Enabling or disabling Network Threat Protection" on page 38.

Warning: Be sure to enable any of the protections when you have completed your troubleshooting task to ensure that your computer remains protected.

If any of the protection technologies cause a problem with an application, it is better to create an exception than to permanently disable the protection.

See "About excluding items from being scanned" on page 58.

When any of the protections are disabled:

- The status bar at the top of the Status page is red.
- The client's icon appears with a universal no sign, a red circle with a diagonal slash. The client icon appears as a full shield in the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon does not appear.
  See "About the notification area icon" on page 18.

On a centrally managed client, your administrator can enable any protection at any time.

To enable protection technologies from the Status page

- On the client, at the top of the Status page, click **Fix** or **Fix All**.

To enable or disable protection technologies from the taskbar

- On the Windows desktop, in the notification area, right-click the client icon, and then do one of the following actions:
  - Click **Enable Symantec Endpoint Protection Small Business Edition**.
  - Click **Disable Symantec Endpoint Protection Small Business Edition**.

Enabling or disabling Auto-Protect

You can enable or disable File System Auto-Protect for files and processes, Internet email, and email groupware applications. When any type of Auto-Protect is disabled, the virus and spyware status appears red on the Status page.

See "About alert icons on the Status page" on page 17.

See "Enabling and disabling protection technologies" on page 35.

Note: On a centrally managed client, your administrator might lock Auto-Protect so that you cannot disable it. Also, the client enables Auto-Protect automatically five minutes after you disable Auto-Protect.

To enable or disable File System Auto-Protect

- In the client, on the Status page, next to Virus and Spyware Protection, do one of the following actions:
  - Click **Options > Enable Virus and Spyware Protection**.
  - Click **Options > Disable Virus and Spyware Protection**.

To enable or disable Auto-Protect for email

1. In the client, in the sidebar, click **Change settings**.
2. Next to Virus and Spyware Protection, click **Configure Settings**.
3. Do one of the following actions:
   - On the Internet Email Auto-Protect tab, check or uncheck **Enable Internet Email Auto-Protect**.
   - On the Outlook Auto-Protect tab, check or uncheck **Enable Microsoft Outlook Auto-Protect** (self-managed client only).
4. Click **OK**.

Enabling or disabling Proactive Threat Protection

You might need to disable Proactive Threat Protection if the scans display too many warnings or false positives. False positives occur when the scan detects an application or process as a threat when it is not.

On a centrally managed client, your administrator might lock Proactive Threat Protection so that you cannot disable it. Proactive Threat Protection is disabled automatically on the client computers that run Windows XP x64 Edition or Windows Server 2000, 2003, and 2008.

To enable or disable Proactive Threat Protection

- In the client, on the Status page, beside Proactive Threat Protection, do one of the following actions:
  - Click **Options > Enable Proactive Threat Protection**.
  - Click **Options > Disable Proactive Threat Protection**.

Enabling or disabling Network Threat Protection

You might need to disable Network Threat Protection if you cannot open an application. If you are not sure that Network Threat Protection causes the problem, you might need to disable all the protection technologies.

See "Enabling and disabling protection technologies" on page 35.

If you can disable protection, you can reenable it at any time. The administrator can also enable and disable protection at any time, even if it overrides the state you put the protection in.

See "Managing Network Threat Protection" on page 64.

To enable or disable Network Threat Protection

- In the client, on the Status page, beside Network Threat Protection, do one of the following actions:
  - Click **Options > Enable Network Threat Protection**.
  - Click **Options > Disable Network Threat Protection**.

Updating the client's protection

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate. LiveUpdate obtains program and protection updates for your computer by using your Internet connection.

Protection updates are the files that keep your Symantec products current with the latest threat protection technology. LiveUpdate retrieves the new definitions files from a Symantec Internet site, and then replaces the old definitions files. The protection updates you receive depend on which products are installed on your computer.

Protection updates can include the following files:

- Virus definition files for Virus and Spyware Protection.
  See "How virus and spyware scans work" on page 51.
- Heuristic signatures and commercial application lists for Proactive Threat Protection.
- IPS definition files for Network Threat Protection.
  See "About Network Threat Protection" on page 63.

Program updates are improvements to the installed client. These differ from product upgrades, which are newer versions of the product. Product updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis. The client receives product updates directly from a LiveUpdate server. A centrally managed client can also receive product updates automatically from a management server at your company.

Table 4-5 Ways to update the definitions on your computer

Step	Description
Update your protection on a schedule	By default, LiveUpdate runs automatically at scheduled intervals. On a self-managed client, you might also be able to disable LiveUpdate or change the LiveUpdate schedule. See "Updating your protection on a schedule" on page 40.
Update your protection immediately	Based on your security settings, you can run LiveUpdate immediately. See "Updating your protection immediately" on page 40.

Note: HTTP is supported for LiveUpdate communication, but HTTPS is not supported.

Updating your protection immediately

You can update the definitions files immediately by using LiveUpdate. You should run LiveUpdate manually for the following reasons:

- The client was recently installed.
- It has been a long time since the last scan.
- You suspect you have a virus.

See "Updating the client's protection" on page 39.

To update your protection immediately

- In the client, in the sidebar, click **LiveUpdate**.

  LiveUpdate connects to the Symantec server, checks for available updates, then downloads and installs them automatically.

Updating your protection on a schedule

You can create a schedule so that LiveUpdate runs automatically at scheduled intervals. You may want to schedule run LiveUpdate during a time that you do not use your computer.

You can configure LiveUpdate to run on a schedule on a self-managed client only.

To update your protection on a schedule

1. In the client, in the sidebar, click **Change settings**.
2. Beside Client Management, click **Configure Settings**.
3. In the Client Management Settings dialog box, click **Scheduled Updates**.
4. On the Scheduled Updates tab, check **Enable automatic updates**.
5. In the Frequency group box, select whether you want the updates to run daily, weekly, or monthly.
6. In the When group box, select the day or week and time of day you want the updates to run.

   The When group box settings depend on the Frequency group box settings.
7. Check **Keep trying for**, and then specify the time interval during which the client tries to run LiveUpdate again.
8. Check **Randomize the start time to be + or -**, and then specify the number of hours or days.

   This option sets a range of time before or after the scheduled time for the update to start.
9. Click **OK**.

Chapter 5

Managing scans

This chapter includes the following topics:

Managing protection scans

By default, a centrally managed client runs a full scan once a week. A self-managed client runs an active scan each day.

If you have a self-managed client, you can manage your own protection scans. On a centrally managed client, you might be able to configure your own scans, if your administrator made these settings available.

Table 5-1 lists suggestions for managing protection scans.

Table 5-1 Steps for managing protection scans

Step	Description
Read about how protection scans work	Learn about how protection scans detect and respond to a virus or security risk detection. See "About viruses and security risks" on page 45. See "About the types of protection scans" on page 48. See "How scans respond to a virus or risk detection" on page 52.
Update virus definitions	Make sure that you have the latest virus definitions installed on your computer. See "Updating the client's protection" on page 39.
Check that Auto-Protect is enabled	Ensure that Auto-Protect is enabled. Ensure that scans run regularly by checking the last scan date. See "Enabling or disabling Auto-Protect" on page 37.
Scan your computer	Regularly scan your computer for viruses and security risks. See "Scanning your computer immediately" on page 31.
Adjust scan settings	In most cases, the default scan settings provide adequate protection for your computer. If necessary, you can increase or decrease protection as follows: ■ Change the time that a scan is scheduled to run ■ Change the remediation actions that occur when a virus is detected ■ Modify a scan's notification actions. Configure the scan results dialog box to appear on your computers when a virus is detected. ■ Schedule a startup scan to run when you log on to your computer See "Scheduling a user-defined scan" on page 53. See "Adjusting virus and spyware scan settings" on page 56.

Table 5-1 Steps for managing protection scans *(continued)*

Step	Description
Identify scan exceptions	Exclude a safe file or process from being scanned. See "About excluding items from being scanned" on page 58.
Manage quarantined files	You can quarantine infected files. Quarantine is a repair action in Virus and Spyware Protection. See "About quarantining files" on page 60. If a quarantined file cannot be fixed, you must decide what to do with the file. Suggestions for managing quarantined files are as follows: ■ Delete a quarantined file if a backup file exists or a replacement file is available from a trustworthy source. ■ Leave files with unknown infections in the Quarantine until Symantec releases new virus definitions. ■ Monitor quarantined files. Periodically check quarantined files to prevent accumulating large numbers of files. Check quarantined files when a new virus outbreak appears on the network. See "Managing a quarantined file" on page 61.

If a virus or security risk is detected on a computer, you might need to act on the detection. For example, worms can travel by shared resources without user interaction.

See "Responding to a virus or risk detection" on page 21.

About viruses and security risks

The client can scan for both viruses and for security risks. By default, the user-defined scans and Auto-Protect scans check for viruses, Trojan horses, worms, and all categories of security risks.

Figure 5-1 How viruses and security risks attack the computer

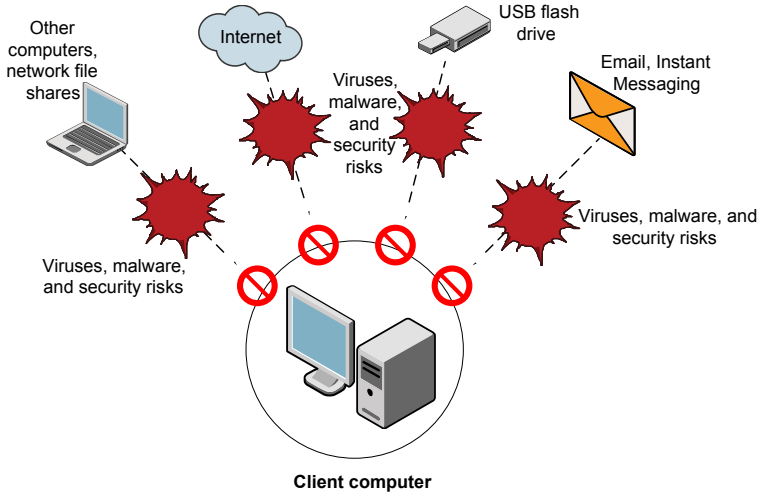


Table 5-2 describes the types of viruses and malware that the client protects against.

Table 5-2 Viruses, Trojan horses, and worms

Virus	Description
Viruses	The programs or the code that attach a copy of themselves to another computer program or document when it runs. Whenever the infected program runs or a user opens a document that contains a macro virus, the attached virus program activates. The virus can then attach itself to other programs and documents. The viruses generally deliver a payload, such as displaying a message on a particular date. Some viruses specifically damage data by corrupting programs, deleting files, or reformatting disks. A macro virus is a virus that is written in a language that is built in a software application, such as Microsoft Word.
Trojan horses	The programs that contain the code that is disguised as or hiding in something benign, such as a game or utility.
Worms	The programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.

Table 5-3 describes the types of security risks that the client protects against.

Table 5-3 Types of security risks

Security risk	Description
Malicious Internet bots	The programs that run automated tasks over the Internet for malicious purposes. Bots can be used to automate attacks on computers or to collect information from Web sites.
Blended threats	The threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage throughout the network.
Adware	The programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.
Dialers	The programs that use a computer, without the user's permission or knowledge, to dial a 900 number or an FTP site. The programs typically accrue charges.
Hacking tools	The programs that hacker use to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.
Joke programs	The programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can then move the Recycle Bin away from the mouse when the user tries to delete it. It can also cause the mouse to click in reverse.
Other	Any other security risks that do not conform to the strict definitions of viruses, Trojan horses, worms, or other security risk categories.
Remote access programs	The programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. You might install a legitimate remote access program. A process might install this type of application without your knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.

Table 5-3 Types of security risks *(continued)*

Security risk	Description
Spyware	The programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer. Spyware can be downloaded from Web sites, email messages, instant messages, and from direct-file connections. Additionally, a user may unknowingly receive spyware by accepting an End User License Agreement from a software program.
Trackware	The standalone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.

By default, the scans detect, remove, and repair the side effects of these viruses and security risks.

See "How scans respond to a virus or risk detection" on page 52.

About the types of protection scans

Scans protect the computer from the viruses and security risks that spread from hard drives and floppy disks, and the others that travel across networks. Computers are also protected from the viruses and security risks that spread through email attachments or some other means. For example, a security risk may install itself on your computer without your knowledge when you access the Internet.

Note: Virus and spyware scans refer to Auto-Protect scans, administrator-defined scans, and user-defined scans.

Table 5-4 lists the types of protection scans.

Table 5-4 Scan types

Scan type	Description
Auto-Protect scans	Auto-Protect scans continuously inspect files and email data as they are written to or read from a computer. Auto-Protect scans automatically neutralize or eliminate detected viruses and security risks. The Auto-Protect scans are as follows: ■ File System Auto-Protect File System Auto-Protect loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can scan files by file extension. It can scan the files on remote computers. It can check floppies for boot viruses. File System Auto-Protect can back up files before it attempts to repair them. It can terminate processes and stop services. ■ Internet Email Auto-Protect Internet Email Auto-Protect scans the incoming and outgoing email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer. It scans the message text and attachments. ■ Microsoft Outlook Auto-Protect (configurable on a self-managed client only) Microsoft Outlook Auto-Protect scans incoming and outgoing Outlook email messages. It scans the message text and attachments. **Note:** On a centrally managed client, you can configure File System Auto-Protect only. See "Adjusting virus and spyware scan settings" on page 56.

Table 5-4 Scan types *(continued)*

Scan type	Description
Administrator-defined scans and user-defined scans	Administrator-defined and user-defined scans detect viruses and security risks by examining files and processes. These scans can inspect memory and load points. These scans include the following types: ■ Scheduled scans Scheduled scans run on client computers at designated times. The concurrently scheduled scans run sequentially. If a computer is turned off during a scheduled scan, the scan does not run unless it is configured to retry missed scans. You can schedule an active, full, or custom scan. See "Scheduling a user-defined scan" on page 53. ■ On-demand scan On-demand scans provide immediate results. You can run an on-demand scan from the Scan for threats page. ■ Startup and trigger scans Startup scans run when you log on to your computers. Trigger scans run when new virus definitions are downloaded to computers. See "Scheduling a scan to run on demand or when the computer starts up" on page 55.
TruScan proactive threat scans	TruScan proactive threat scans use heuristic analysis to identify the unknown behavior anomalies in applications and processes. The scans detects whether the application or the process exhibits characteristics of the following known threats: ■ Trojan horses ■ Worms ■ Keyloggers ■ Adware and spyware ■ Applications that are used for malicious purposes TruScan proactive threat scans run on your computer in the background. On a self-managed client, you can enable and disable these scans. You can also specify a process that is excluded from being scanned. See "Excluding a process from TruScan proactive threat scans" on page 60.

How virus and spyware scans work

Protection scans identify and neutralize or eliminate viruses and security risks on your computers. A scan eliminates a virus or risk by using the following process:

- The scan engine searches within files and other components on the computer for traces of viruses within files. Each virus has a recognizable pattern that is called a signature. Installed on the client is a virus definitions file that contains the known virus signatures, without the harmful virus code. The scan engine compares each file or component with the virus definitions file. If the scan engine finds a match, the file is infected.
- The scan engine uses the definitions files to determine whether a virus or a risk caused the infection. The scan engine then takes a remediation action on the infected file. To remediate the infected file, the client cleans, deletes, or quarantines the file.
  See "How scans respond to a virus or risk detection" on page 52.

Table 5-5 describes the components that the client scans on your computer.

Table 5-5 Computer components that the client scans

Component	Description
Selected files	The client scans individual files. For most types of scans, you select the files that you want scanned. The client also uses pattern-based scanning to search for signs of security risks within files and registry keys. If a security risk is found, by default the client quarantines the infected files and repairs the risk's effects. If the client cannot quarantine the files, it logs the attempt.
Computer memory	The client searches the computer's memory. Any file virus, boot sector virus, or macro virus may be memory-resident. Viruses that are memory-resident have copied themselves into a computer's memory. In memory, a virus can hide until a trigger event occurs. Then the virus can spread to a floppy disk in the disk drive, or to the hard drive. If a virus is in memory, it cannot be cleaned. However, you can remove a virus from memory by restarting your computer when prompted.
Boot sector	The client checks the computer's boot sector for boot viruses. Two items are checked: the partition tables and the master boot record.

Table 5-5 Computer components that the client scans *(continued)*

Component	Description
Floppy drive	A common way for a virus to spread is through the floppy disks. A floppy disk might remain in a disk drive when you start up or turn off your computer. When a scan starts, the client searches the boot sector and partition tables of a floppy disk that is located in the disk drive. When you turn off your computer, you are prompted to remove the disk to prevent possible infection.

How scans respond to a virus or risk detection

When viruses and security risks infect files, the client responds to the threat types in different ways. For each threat type, the client uses a first action, and then applies a second action if the first action fails.

Table 5-6 How a scan responds to viruses and security risks

Threat type	Action
Virus	By default, when the client detects a virus, the client: ■ Tries first to clean the virus from the infected file. ■ If the client cleans the file, the client completely removes the risk from your computer. ■ If the client cannot clean the file, it logs the failure and moves the infected file to the Quarantine. See "About quarantining files" on page 60.
Security risk	By default, when the client detects a security risk: ■ It quarantines the infected file. ■ It tries to remove or repair any changes that the security risk made. ■ If the client cannot quarantine a security risk, it logs the risk and leaves it alone. In some instances, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec has determined that quarantining the risk does not harm the computer, then the client quarantines the risk. If the client quarantines the risk immediately, its action might leave the computer in an unstable state. Instead, the client waits until the application installation is complete before it quarantines the risk. It then repairs the risk's effects.

For each scan type, you can change the settings for how the client handles viruses and security risks. You can set different actions for each category of risk and for individual security risks.

Scheduling a user-defined scan

A scheduled scan is an important component of threat and security risk protection. You should schedule a scan to run at least one time each week to ensure that your computer remains free of viruses and security risks. When you create a new scan, the scan appears in the scan list in the Scan for threats pane.

Note: If your administrator has created a scheduled scan for you, it appears in the scan list in the Scan for threats pane.

For centrally managed clients, the administrator may override these settings.

If you schedule multiple scans to occur on the same computer and the scans start at the same time, the scans run serially. After one scan finishes, another scan starts. For example, you might schedule three separate scans on your computer to occur at 1:00 P.M. Each scan scans a different drive. One scan scans drive C. Another scan scans drive D. Another scan scans drive E. In this example, a better solution is to create one scheduled scan that scans drives C, D, and E.

See "Scanning your computer immediately" on page 31.

For more information on the options on each dialog box, click Help.

To schedule a user-defined scan

1. In the client, in the sidebar, click **Scan for threats**.
2. Click **Create a New Scan**.
3. In the Create New Scan - What To Scan dialog box, select one of the following types of scans to schedule:

Active Scan	Scans the areas of the computer that viruses and security risks most commonly infect.
Full Scan	Scans the entire computer for viruses and security risks.
Custom Scan	Scans the selected areas of the computer for viruses and security risks.

4. Click **Next**.

5 If you selected **Custom**, check the appropriate check boxes to specify where to scan, and then click **Next**.

The symbols have the following descriptions:

The file, drive, or folder is not selected. If the item is a drive or folder, the folders and files in it are also not selected.

The individual file or folder is selected.

The individual folder or drive is selected. All items within the folder or drive are also selected.

The individual folder or drive is not selected, but one or more items within the folder or drive are selected.

6 In the Create New Scan - Scan Options dialog box, you can modify any of the following options:

File Types	Change which file extensions the client scans. The default setting is to scan all files.
Actions	Change first and second actions to take when viruses and security risks are found.
Notifications	Construct a message to display when a virus or security risk is found. You can also configure whether or not you want to be notified before remediation actions occur.
Advanced	Change additional scan features, such as displaying the scan results dialog box.
Scan Enhancements	Change which computer components the client scans. The options that are available depend on what you selected in step 3.
Centralized Exceptions	Add items that the client excludes from being scanned.

7 Click **Next**.

8 In the Create New Scan - When To Scan dialog box, click **At specified times**, and then click **Next**.

You can also create an on-demand or startup scan.

You can create a startup scan for a self-managed client only.

See "Scheduling a scan to run on demand or when the computer starts up" on page 55.

9 In the Create New Scan - Schedule dialog box, specify the frequency and when to scan, and then click **Next**.

10 In the Create New Scan - Scan Name dialog box, type a name and description for the scan.

For example, call the scan: Friday morning

11 Click **Finish**.

Scheduling a scan to run on demand or when the computer starts up

You can supplement a scheduled scan with an automatic scan whenever you start your computer or log on. Often, a startup scan is restricted to critical, high-risk folders, such as the Windows folder and folders that store Microsoft Word and Excel templates.

If you regularly scan the same set of files or folders, you can create an on-demand scan that is restricted to those items. At any time, you can quickly verify that the specified files and folders are free from viruses and security risks. You must run on-demand scans manually.

If you create more than one startup scan, the scans run sequentially in the order in which they were created. Your administrator may have configured the client so that you cannot create a startup scan.

See "Scanning your computer immediately" on page 31.

For more information on the options on each dialog box, click Help.

To schedule a scan to run on demand or when the computer starts up

1 In the client, in the sidebar, click **Scan for threats**.

2 Click **Create a New Scan**.

3 Follow steps 3 to 7 for creating a scheduled scan.

See "Scheduling a user-defined scan" on page 53.

4 In the Create New Scan - When to Run dialog box, do one of the following actions:

- Click **At startup**.
- Click **On demand**.

5 Click **Next**.

6 In the Create New Scan - Scan Name dialog box, type a name and description for the scan.

For example, call the scan: MyScan1

7 Click **Finish**.

Adjusting virus and spyware scan settings

By default, the client gives your computer the protection against the viruses and security risks that you need. If you have a self-managed client, you may want to configure some of the scan settings.

Table 5-7 displays the settings that you can modify for a user-defined scan or an Auto-Protect scan. You can adjust these settings in any order.

Table 5-7 Actions to adjust protection scan settings

Action	Description
Modify the scan's file types	Specify which files and folders the client scans. By default, the client scans all files. To increase the speed of the scan, you can reduce which files the client scans. However, you get less protection.
Modify the remediation actions	Change the actions that occur when a virus or security risk is detected.
Modify the notification actions	Configure a message to appear on the client computers when a virus is detected. Configure a notification to trigger when the client detects a virus or security risk.
Exclude risks and processes from being scanned	Exclude security risks and processes from the protection scans. On a centrally managed client, your administrator can control the types of exceptions that you can add. See "Excluding items from being scanned" on page 58.

To adjust a user-defined scan

1. In the client, in the sidebar, click **Scan for threats**.
2. In the Scan for threats page, right-click a scan and click **Edit**.
3. In the <*scan name*> Properties dialog box, click **Scan Options**.
4. On the Scan Options tab, do any of the following tasks:
   - To specify fewer file types to scan, click **Selected extensions**, and then click **Extensions**.
   - To specify which a first and second action that the client takes on an infected file, click **Actions**.
   - To specify notification options, click **Notifications**.
   - To configure advanced options for compressed files, backups, and performance, click **Advanced**.
   - To add a process or file that the scan should exclude, click **Centralized Exceptions**.
     See "About excluding items from being scanned" on page 58.

   For more information on the options on each dialog box, click **Help**.
5. Click **OK**.

To adjust an Auto-Protect scan

1. In the client, in the sidebar, click **Change settings**.
2. Next to Virus and Spyware Protection, click **Configure Settings**.
3. On any Auto-Protect tab, do the following tasks:
   - To specify fewer file types to scan, click **Selected**, and then click **Extensions**.
   - To specify which a first and second action that the client takes on an infected file, click **Actions**.
   - To specify notification options, click **Notifications**.
   - To add a process or file that the scan should exclude, click **Centralized Exceptions**.
     See "About excluding items from being scanned" on page 58.

   For more information on the options on each dialog box, click **Help**.
4. Click **OK**.

About excluding items from being scanned

Exceptions are known security risks, files, file extensions, processes that you want to exclude from a scan. If you have scanned your computer and know that certain files are safe, you can exclude them. In some cases, exceptions can reduce scan time and increase system performance. Typically you do not need to create exceptions.

For centrally managed clients, your administrator may have created exceptions for your scans. If you create an exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.

Table 5-8 lists the types of exceptions that you can exclude from the protection scans.

Table 5-8 Exception types

Type	Description
Security risk exceptions	You can exclude the following security risks: ■ Known security risks ■ Files ■ Folders ■ Extensions Your administrator may have configured the client so that you cannot exclude any of these items from being scanned. See "Excluding items from being scanned" on page 58.
TruScan proactive threat scan exceptions	You can exclude processes from the TruScan proactive threat scans. You can specify a different action to take for a known process that the TruScan proactive threat scans detect. You can force the detection of a process. Your administrator may have configured the client so that you cannot exclude a process from being scanned. See "Excluding a process from TruScan proactive threat scans" on page 60.

Excluding items from being scanned

You can create an exception from the Change settings page. You can also configure exceptions when you create or modify a user-defined scan, or when you modify Auto-Protect settings.

See "Adjusting virus and spyware scan settings" on page 56.

See "About excluding items from being scanned" on page 58.

Exceptions apply across all scans. If you configure an exception when you create or edit a particular scan, the exception applies to all scans.

Note: On the Server Core installation of Windows Server 2008, the appearance of the dialog boxes might differ from the ones that are described in these procedures.

For more information on the options on each dialog box, click Help.

To exclude a security risk from being scanned

1. In the client, in the sidebar, click **Change settings**.
2. Next to Centralized Exceptions, click **Configure Settings**.
3. In the Centralized Exceptions dialog box, on the User-defined Exceptions tab, click **Add > Security Risk Exceptions > Known Risks**.
4. In the Add Known Security Risk Exceptions dialog box, check the security risks that you want to exclude from scans.
5. If you want to log an event when the security risk is detected and ignored, check **Log when the security risk is detected**.
6. Click **OK**.
7. In the Centralized Exceptions dialog box, click **Close**.

To exclude a file or folder from being scanned

1. In the client, in the sidebar, click **Change settings**.
2. Next to Centralized Exceptions, click **Configure Settings**.
3. In the Centralized Exceptions dialog box, on the User-defined Exceptions tab, click **Add > Security Risk Exceptions**
4. Do one of the following tasks:
   - Click **File**. In the Add Security Risk File Exceptions dialog box, select the file that you want to exclude, and then click **Add**.
   - Click **Folder**. In the Add Security Risk Folder Exceptions dialog box, select the folder, check or uncheck **Include subfolders**, and then click **Add**.
5. In the Centralized Exceptions dialog box, click **Close**.

Excluding a process from TruScan proactive threat scans

You can create exceptions for proactive threat scans unless your administrator locks the settings.

See "About excluding items from being scanned" on page 58.

To create an exception, you select a file that is currently available on your computer. When a proactive threat scan detects an active process that uses the file, the client applies the action that you specify in the exception.

For example, you might run an application on your computer that uses a file called foo.exe. A proactive threat scan runs when foo.exe runs. The client determines that foo.exe might be malicious. The scan results dialog appears and shows that the client quarantined foo.exe. You can create an exception that specifies that proactive threat scans ignore foo.exe. The client then restores foo.exe. When you run foo.exe again, the client ignores foo.exe.

Your administrator might also create centralized exceptions for your scans. If you create a centralized exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.

To exclude a process from TruScan proactive threat scans

1. In the client, in the side bar, click **Change settings**.
2. Next to Centralized Exceptions, click **Configure Settings**.
3. On the User-defined Exceptions tab, click **Add**, and then select **TruScan Proactive Threat Scan Exception**.
4. In the Add TruScan Proactive Threat Scan Exception dialog box, locate the process or file for which you want to create an exception.
5. In the Action drop-down list, select **Ignore**, **Log only**, **Quarantine**, or **Terminate**.
6. Click **Add**.
7. In the Centralized Exceptions dialog box, click **Close**.

About quarantining files

When the client moves an infected file to the Quarantine, the virus or risk cannot copy itself and infect other files on your computer or other computers in the network. However, the Quarantine action does not clean the risk. The risk stays on your computer until the client cleans the risk or deletes the file. You do not have access to the file. But you can remove the file from the Quarantine.

When you update your computer with new virus definitions, the client automatically checks the Quarantine. You can rescan the items in the Quarantine. The latest definitions might clean or repair the previously quarantined files.

Viruses and macro viruses can be quarantined. Boot viruses reside in the boot sector or partition tables of a computer; these items cannot be moved to the Quarantine. Sometimes the client detects an unknown virus that cannot be eliminated with the current set of virus definitions. If you have a file that you believe is infected but scans do not detect an infection, you should quarantine the file.

See "Managing a quarantined file" on page 61.

Quarantining a file from the Risk or Scan log

Based on the preset action for a threat detection, the client might or might not be able to perform the action you selected when a detection occurred. You can use the Risk log or Scan log to quarantine a file later.

See "Managing a quarantined file" on page 61.

See "About quarantining files" on page 60.

To quarantine a file from the Risk log or Scan log

1. In the client, click **Help > Troubleshooting**.
2. In the Troubleshooting dialog box, click **Logs**.
3. In the Logs panel, under Virus and Spyware Protection, select **Scan Log**, and then click **View Log**.
4. Select the file that you want to quarantine, and then click **Quarantine**.
5. Click **OK**, and then click **Close**.

Managing a quarantined file

After a file is moved to the Quarantine, you can perform any of the following actions on the file:

- Restore the selected file to its original location.
- Permanently delete the selected file.
- Rescan the files after you receive updated virus definitions.
- Export the contents of the Quarantine to either a comma-delimited (.csv) file or a Microsoft Access database (.mdb) file.

- Manually add a file to the Quarantine. You can browse to the location of and select the file that you want to move to the Quarantine.
- Submit a file to Symantec Security Response. Follow the instructions in the on-screen wizard to submit the selected file for analysis.

See "About quarantining files" on page 60.

See "Quarantining a file from the Risk or Scan log" on page 61.

To manage a quarantined file

1. In the client, in the sidebar, click **View quarantine**.
2. Select the file and then click any one of the following options:
   - **Restore**
   - **Delete**
   - **Rescan All**
   - **Export**
   - **Add**
   - **Submit**

Chapter 6

Managing the firewall and intrusion prevention

This chapter includes the following topics:

About Network Threat Protection

The Symantec Endpoint Protection Small Business Edition client can protect your computer by monitoring the information that comes into and out of your computer, and by blocking network attack attempts. Network Threat Protection blocks threats from accessing your computer by using firewall rules and signatures.

See "About the Symantec Endpoint Protection Small Business Edition client" on page 9.

Table 6-1 displays the tools that Network Threat Protection uses to protect your computer from network attacks.

Table 6-1 Network Threat Protection tools

Tool	Description
Firewall	The firewall protects unauthorized users from accessing your computer and the networks that connect to the Internet. The firewall detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic. The firewall allows or blocks inbound and outbound traffic. See "How the firewall works" on page 65.
Intrusion Prevention System	The intrusion prevention system (IPS) automatically detects and blocks network attacks. The IPS scans every packet that enters and exits a computer for attack signatures. The IPS relies on an extensive list of attack signatures to detect and block suspicious network activity. Symantec supplies the known threat list, which you can update on the client by using Symantec LiveUpdate. The Symantec IPS engine and corresponding set of IPS signatures are installed on the client by default.

Managing Network Threat Protection

On a centrally managed client, your administrator configures the firewall settings and the intrusion prevention settings for you. You do not have to configure any additional settings.

By default, the firewall engine is enabled but the firewall is not. By default, the firewall allows all incoming and outgoing network traffic.

On any client, you can disable Network Threat Protection temporarily for troubleshooting purposes. For example, you might not be able to open an application.

See "Enabling or disabling Network Threat Protection" on page 38.

On a self-managed client, you configure your own firewall and intrusion prevention settings. You should not change any other default firewall settings or intrusion prevention settings.

See "About centrally managed clients and self-managed clients" on page 33.

Table 6-2 displays the Network Threat Protection tasks you can perform on a self-managed client but are not available on a centrally managed client.

Table 6-2 Steps that you can do on the self-managed client only

Step	Description
Read about how the firewall works	Learn how the firewall protects your computer from network attacks. See "How the firewall works" on page 65.
Add firewall rules	Supplement the client's default firewall rules with the firewall rules that you configure. For example, you might want to block an application that you do not want to run on your computer, such as an adware application. See "Adding a firewall rule" on page 68.
Download the latest IPS signatures.	Download the latest IPS attack signatures. See "Updating the client's protection" on page 39.
View the Traffic Log	View the Traffic Log to see whether: ■ The firewall rules that you created work correctly. ■ The client blocked any network attacks. ■ The client blocked any applications that you expected to run. The Packet Log is not enabled for either a centrally managed client or a self-managed client. See "Viewing the logs" on page 27.

How the firewall works

Firewall protection prevents unauthorized users from accessing your computers and networks that connect to the Internet.

The packets of data that travel across the Internet contain information about the following:

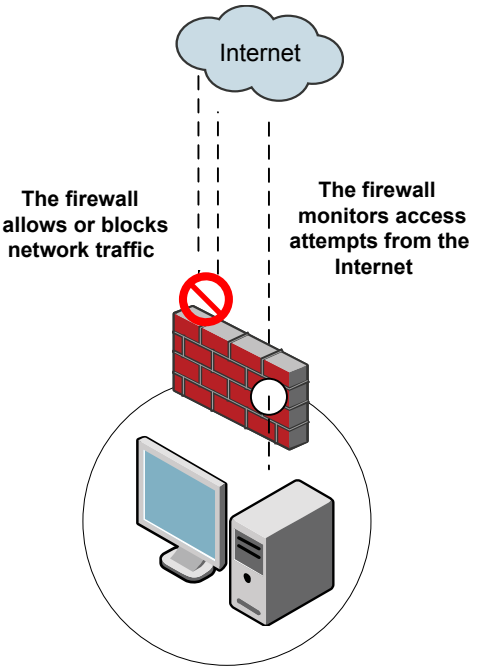
- Sending computers
- Intended recipients
- How the packet data is processed
- Ports that receive the packets

A packet is a discrete chunk of data that is part of the information flow between two computers. Packets are reassembled at their destination to appear as an unbroken data stream.

The ports are the channels that divide the stream of data that comes from the Internet. The applications that run on a computer listen to the ports. The applications accept the data that is sent to the ports.

Network attacks exploit weaknesses in vulnerable applications. Attackers use these weaknesses to send the packets that contain malicious programming code to ports. When vulnerable applications listen to the ports, the malicious code lets the attackers gain access to the computer.

Firewall protection works in the background. Firewall protection monitors the communication between your computers and other computers on the Internet. It creates a shield that allows or blocks attempts to access the information on your computers. It warns you of connection attempts from other computers. It warns you of connection attempts by the applications on your computer that connect to other computers.



Firewall protection uses firewall rules to allow or block network traffic.

See "How the firewall rules work" on page 67.

How the firewall rules work

Firewall rules control how the client protects your computers from malicious network traffic. When a computer attempts to connect to another computer, the firewall compares the connection type with the firewall rules. The firewall automatically checks all the inbound and outbound traffic packets against the rules. The firewall allows or blocks the packets according to the rules.

You can use triggers such as applications, hosts, and protocols to define the firewall rules. For example, a rule can identify a protocol in relation to a destination address. When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any trigger is false for the current packet, the firewall does not apply the rule.

Table 6-3 lists the rule parameters that describe the conditions in which a network connection is allowed or blocked.

Table 6-3 Firewall rule parameters

Parameter	Description
Action	The action that the firewall takes when it successfully matches a rule. You can specify one of the following actions: ■ Allow The firewall allows the network connection. ■ Block The firewall blocks the network connection.
Application	The applications that trigger the rule. When an application is the only trigger in an allow traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operation that the application performs. For example, suppose you allow Internet Explorer, and define no other triggers. Computer users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the network protocols and hosts with which communication is allowed.
Host	The remote hosts that trigger the rule. The local host is the local client computer. The remote host is the computer that communicates with the client computer. If the client communicates with a Web server, the remote host is the Web server.

Table 6-3 Firewall rule parameters *(continued)*

Parameter	Description
Service	The network services that trigger a rule. A network service is a collection of the protocols and the port numbers that are grouped under one name. The network services list contains commonly used network services. For example, HTTP Server is the name for the HTTP server traffic that uses TCP local ports 80 and 443. DHCP Server is the name for the DHCP server traffic that uses UDP ports 67 and 68. When you define TCP or UDP service triggers, you identify the ports on both sides of the network connection. The port relationship is independent of the traffic direction. The local computer owns the local port. The remote computer owns the remote port.

See "About the rule processing order" on page 69.

You can enable and disable firewall rules. The firewall does not inspect disabled rules.

You can configure firewall rules on a self-managed client only.

Adding a firewall rule

When you add a firewall rule, you must decide what effect you want the rule to have. For example, you may want to allow all traffic from a particular source or block the UDP packets from a Web site.

You can add firewall rules on self-managed clients only.

To add a firewall rule

1. In the client, in the sidebar, click **Status**.
2. Beside Network Threat Protection, click **Options > Configure Firewall Rules**.
3. In the Configure Firewall Rules dialog box, click **Add**.
4. On the General tab, type a name for the rule, and then click either **Block this traffic** or **Allow this traffic**.
5. To define the triggers for the rule, select any one of the following tabs:
   - Hosts
   - Ports and Protocols
   - Applications

   For more information about the options on each tab, click **Help**.

6 To define the time period when the rule is active or inactive, click **Enable Scheduling**, and then set up a schedule.

7 When you finish making changes, click **OK**.

8 In the Configure Firewall Rules dialog box, make sure the check mark appears in the Rule Name column to enable the rule.

You can also change the order that the firewall processes the rule.

See "Changing the order of a firewall rule" on page 69.

9 Click **OK**.

About the rule processing order

Firewall rules are ordered sequentially, from highest to lowest priority, or from the top to bottom in the rules list. If the first rule does not specify how to handle a packet, the firewall inspects the second rule. This process continues until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies. Subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

You can order rules according to exclusivity. The most restrictive rules are evaluated first, and the most general rules are evaluated last. For example, you should place the rules that block traffic near the top of the rules list. The rules that are lower in the list might allow the traffic.

The best practices for creating a rule base include the following order of rules:

1. Rules that block all traffic.
2. Rules that allow all traffic.
3. Rules that allow or block specific computers.
4. Rules that allow or block specific applications, network services, and ports.

See "Changing the order of a firewall rule" on page 69.

Changing the order of a firewall rule

The firewall processes the list of firewall rules from the top down. You can determine how the firewall processes firewall rules by changing their order. When you change the ordering, it affects the order only for the currently selected location.

Note: For better protection, place the most restrictive rules first, and the least restrictive rules last.

See "About the rule processing order" on page 69.

See "Adding a firewall rule" on page 68.

To change the order of a firewall rule

1. In the client, in the sidebar, click **Status**.
2. Beside Network Threat Protection, click **Options > Configure Firewall Rules**.
3. In the Configure Firewall Rules dialog box, select the rule that you want to move.
4. Do one of the following actions:
   - To have the firewall process this rule before the rule above it, click the up arrow.
   - To have the firewall process this rule after the rule below it, click the down arrow.
5. When you finish moving rules, click **OK**.

Index

S

T

U

V

W