Symantec™ Endpoint Protection and Symantec Network Access Control 12.1.2 Client Guide

Symantec Endpoint Protection and Symantec Network Access Control Client Guide

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

Product version: 12.1.2

Documentation version: 1

Legal Notice

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Getting started on the client

This chapter includes the following topics:

- About the Symantec Endpoint Protection client
- About the Symantec Network Access Control client
- Getting started on the Status page
- About managed clients and unmanaged clients
- Checking whether the client is managed or unmanaged
- About the alert icons on the Status page
- How can I protect my computer with Symantec Endpoint Protection?
- Scanning your computer immediately
- Pausing and delaying scans
- Troubleshooting computer issues with the Symantec Help support tool

About the Symantec Endpoint Protection client

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

Table 1-1 describes each layer of protection.

Table 1-1 Types of protection

Layer	Description
Virus and Spyware Protection	Virus and Spyware Protection 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. Microsoft Outlook Auto-Protect scans incoming and outgoing Outlook email messages. See "Managing scans on your computer" on page 52.
Proactive Threat Protection	Proactive threat technology includes SONAR, which offers real-time protection against zero-day attacks. SONAR can stop attacks even before traditional signature-based definitions detect a threat. SONAR uses heuristics as well as file reputation data to make decisions about applications or files. See "Managing SONAR on your client computer" on page 93.
Network Threat Protection	Network Threat Protection includes a firewall and an intrusion prevention system. The rules-based firewall prevents unauthorized users from accessing your computer. The intrusion prevention system automatically detects and blocks network attacks. See "Managing firewall protection" on page 97.

Your administrator manages the types of protection that the management server should download to your client computer. The client automatically downloads the virus definitions, IPS definitions, and the product updates to your computer. Users who travel with portable computers can get virus definitions and product updates directly from LiveUpdate.

See "Updating the computer's protection" on page 37.

About the Symantec Network Access Control client

The Symantec Network Access Control client evaluates whether a computer is protected and compliant with a security policy before the computer is allowed to connect to the corporate network.

The client ensures that your computer complies with a security policy that your administrator configures. The security policy checks whether your computer runs the most recent security software, such as virus protection and firewall applications. If your computer does not run the required software, either you must update the software manually, or your client may update the software automatically. Until your security software is up to date, your computer may be blocked from connecting to the network. The client runs periodic checks to verify that your computer continues to comply with the security policy.

See “How Symantec Network Access Control works” on page 119.

Getting started on the Status page

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

Table 1-2 displays the main tasks that you can perform from the menu bar on the left-hand side.

Table 1-2 Client main window

Click this option	To do these tasks
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 the alert icons on the Status page” on page 17. You can: ■ Enable or disable one or more protection technologies if your administrator allows it. See “About enabling and disabling protection when you need to troubleshoot problems” on page 44. ■ 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 22. ■ View the threat list for the results of the last virus and spyware scan.
Scan for Threats	■ Run an active scan or full scan immediately. See “Scanning your computer immediately” on page 22. ■ Create a new scan that runs at a specified time, startup, or on demand. See “Scheduling a user-defined scan” on page 65. See “Scheduling a scan to run on demand or when the computer starts up” on page 69. ■ Run a Host Integrity check if you have Symantec Network Access Control installed. See “Running a Host Integrity check” on page 121.

Table 1-2 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 "Customizing virus and spyware scan settings" on page 74. ■ Configure the firewall settings and the intrusion prevention system settings. See "Managing firewall protection" on page 97. ■ View and add exceptions to scans. See "Excluding items from scans" on page 81. ■ Display the notification area icon. See "How to determine whether the client is connected and protected" on page 40. ■ Configure the Tamper Protection settings. See "Enabling, disabling, and configuring Tamper Protection" on page 49. ■ Create a schedule to download content and product updates to the client. See "Updating the content on a schedule" on page 38. See "Managing your computer's protection" on page 35.
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 84.
View Logs	View any of the client logs. See "Viewing the logs" on page 43.
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 the content immediately" on page 38.

About managed clients and unmanaged clients

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

Table 1-3 Differences between a managed client and an unmanaged client

Client type	Description
Managed client	A 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. ■ The administrator manages the client, but you can change all the client settings and perform all the protection tasks.
Unmanaged client	An unmanaged client does not communicate with a management server and an administrator does not manage the client. An unmanaged 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 installation that uses either the default option settings or administrator-preset settings. ■ A remote computer that connects to the corporate network, which 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.

Table 1-4 describes the differences in the user interface between a managed and unmanaged client.

Table 1-4 Differences between a managed client and an unmanaged client by feature area

Feature area	Centrally managed client	Self-managed client
Virus and Spyware Protection	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.

Table 1-4 Differences between a managed client and an unmanaged client by feature area *(continued)*

Feature area	Centrally managed client	Self-managed client
Proactive Threat Protection	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.

See "Checking whether the client is managed or unmanaged" on page 16.

Checking whether the client is managed or unmanaged

To check how much control you have to configure protection on your client, you first check whether your client is managed or unmanaged. You can configure more settings on an unmanaged client than on a managed client.

See "About managed clients and unmanaged clients" on page 14.

To check whether the client is managed or unmanaged

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 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 managed but not currently connected to a management server, this field is **Offline**.
    - If the client is unmanaged, the **Server** field displays **Self-managed**.
4. Click **Close**.

About the 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 1-5 Status page alert icons

Icon	Description
✓	Shows that each protection is enabled.
⚠	Warns you that the client computer virus definitions are out of date. To receive the most current virus definitions, you can run LiveUpdate immediately, if your administrator lets you. The Symantec Network Access Control client computer may have the following issues: ■ The client computer failed the Host Integrity security compliance check. To find out what you need to do to pass the check, check the Client Management Security log. ■ Host Integrity is not connected. See "Updating the computer's protection" on page 37.
✕	Shows that one or more protections are disabled or that the client has an expired license. To enable a protection, you click **Fix** or **Fix All**. See "About enabling and disabling protection when you need to troubleshoot problems" on page 44. See "Enabling or disabling protection on the client computer" on page 46.

How can I protect my computer with Symantec Endpoint Protection?

The default settings in the Symantec Endpoint Protection client protect your computer from many types of malware. Either the client automatically handles the malware, or lets you choose how to handle the malware.

You can check whether your computer is infected, and perform some additional tasks if you want increased security or better performance.

Note: On managed clients, some options do not appear if your administrator has configured them to be unavailable. On unmanaged clients, most options appear.

Table 1-6 Frequently asked questions on how to protect your computer

Question	Description
How do I know that my computer is protected?	In the client console, look at the top of the **Status** page. The color and type of alert icon displays the protection status of your computer. For more information, read the **Status** pane or click **Details**. See "About the alert icons on the Status page" on page 17. See "How to determine whether the client is connected and protected" on page 40.
How can I tell if my computer is infected?	If your computer is infected, you might see any of the following messages: ■ An Auto-Protect detection or manual scan detection. These messages describe the threat and the action that was taken on the threat. You can choose one of several options to handle the threat. You can either remove, clean, exclude, delete, or undo the action you selected. If your administrator has allowed it, you can also pause a scan. See "Responding to a virus or a risk detection" on page 28. See "About scan results" on page 27. See "Pausing and delaying scans" on page 23. ■ A Download Insight detection. This window displays information about the malicious and the unproven files that Download Insight detects when you try to download them. See "Responding to Download Insight messages that ask you to allow or block a file that you try to download" on page 30. See "Types of alerts and notifications" on page 25.
How do I clean my computer if it is infected?	If you see a scan window, your administrator has already set the action that your computer takes on the infection. You may be able to choose an action. If you know that a file is infected, click **Clean** or **Quarantine**. For scheduled scans and Auto-Protect, make sure that the main action is set to **Clean risk** and the secondary action to **Quarantine risk** or **Delete**. See "Responding to a virus or a risk detection" on page 28. See "How virus and spyware scans work" on page 56. See "Configuring actions for malware and security risk detections" on page 76.

Table 1-6 Frequently asked questions on how to protect your computer *(continued)*

Question	Description
How do I increase the security of my computer?	By default, your client computer is protected with the maximum amount of protection. Your administrator may have modified some of the client's security settings to improve the client's performance. Your administrator may have also enabled you to modify your own computer's protection. If you have the ability to modify these settings, you can perform the following tasks: ■ Schedule regular full scans, typically once a day or once a week. See "Scheduling a user-defined scan" on page 65. ■ Keep virus and spyware scans, Auto-Protect, SONAR, intrusion prevention, and Insight installed, enabled, and up-to-date at all times. See "About enabling and disabling protection when you need to troubleshoot problems" on page 44. See "Enabling or disabling protection on the client computer" on page 46. See "Enabling or disabling Auto-Protect" on page 47. On an unmanaged client, you can perform the following tasks: ■ Download and install the correct virus definitions by using LiveUpdate. By default, your client computer receives the latest virus definitions twice a day. However, you can download the latest definitions yourself. See "Updating the content immediately" on page 38. ■ Run a full scan of your computer with all scan enhancements enabled. By default, a full scan runs on your computer weekly. However, you can run a scan at any time. See "Scheduling a user-defined scan" on page 65. See "Scanning your computer immediately" on page 22.

Table 1-6 Frequently asked questions on how to protect your computer *(continued)*

Question	Description
How do I modify my scan settings if the scan slows down my work?	If scans slow down your computer, adjust the following settings: ■ Schedule LiveUpdate to download the latest virus definitions less frequently or at the times that you are not on the computer. See "Updating the content on a schedule" on page 38. ■ Create a scheduled full scan for after hours or when you are not on the computer. See "Scheduling a user-defined scan" on page 65. ■ Exclude the applications and files that you know are safe from being scanned. See "Excluding items from scans" on page 81. ■ Limit scheduled scans, Auto-Protect, and Download Insight to scan file extensions for the file types that commonly carry infections. For example, specify the scan to look for executable files, such as EXE, COM, BAT, and VBS. ■ In Auto-Protect, disable **Scan for security risks**. See "Customizing virus and spyware scan settings" on page 74. **Warning:** You can disable Auto-Protect to improve client computer performance or to troubleshoot the client. However, Symantec recommends that you keep Auto-Protect enabled at all times. See "Enabling or disabling Auto-Protect" on page 47. ■ Disable the scan enhancement options in an active scan, full scan, or custom scan. See "Scheduling a user-defined scan" on page 65. ■ Disable Download Insight and Insight Lookup. See "Customizing Download Insight settings" on page 73. See "Submitting information about detections to Symantec Security Response" on page 89. **Note:** You may not be able to change these settings if your administrator has made them unavailable to you.

Table 1-6 Frequently asked questions on how to protect your computer *(continued)*

Question	Description
What do I do if the firewall blocks my ability to browse the Internet?	By default, the firewall does not block access to the Internet. If you cannot access the Internet, contact your administrator. Your administrator may have blocked access to certain Web sites or may not allow your computer to access a certain browser. You may or may not have the rights to modify the firewall rules. On an unmanaged client, you can modify the firewall rules. However, you should not change or add a firewall rule until you understand whether or not the traffic that the firewall rule blocks is malicious. Before you modify the firewall rule, ask the following questions: ■ Is the Web application that accesses the Internet legitimate? ■ Are the remote ports that the Web application accesses correct? HTTP traffic is legitimate traffic for Web applications, and HTTP traffic uses port TCP 80 and 443. You may not be able to trust traffic from other ports. ■ Is the IP address for the Web site that the application accesses correct or legitimate?
What actions do I take when I get a message in the notification area?	Read the message in the notification area on the toolbar. The notifications tell you one of the following things: ■ Your computer might have been attacked and the client handled the threat. ■ Your computer received a new security policy. The security policy is updated automatically. You can also update your security policy at any time. See "Manually updating policies on the client" on page 39. See "Responding to a virus or a risk detection" on page 28. See "Responding to messages that ask you to allow or block an application" on page 33. You can also go to one of the logs for more information, depending on the type of threat. See "Viewing the logs" on page 43.

See "About managed clients and unmanaged clients" on page 14.

See "Checking whether the client is managed or unmanaged" on page 16.

See "Managing your computer's protection" on page 35.

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 or security risk.

Select anything to scan from a single file to a floppy disk to your entire computer. On-demand scans include the Active Scan and Full Scan. You can also create a custom scan to run on demand.

See “Scheduling a scan to run on demand or when the computer starts up” on page 69.

See “Updating the computer's protection” on page 37.

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.
      You can view the scan progress unless your administrator disables the option. To view scan progress, click the message link that appears for the current scan: ***scan* in progress**.
      See “About scan results” on page 27.

  You can also pause or cancel the scan.

  See “Pausing and delaying scans” on page 23.

To scan your computer from Windows

- In the My Computer window or the Windows Explorer window, right-click a file, folder, or drive, and then click **Scan For Viruses**.

  This feature is supported on both 32-bit and 64-bit operating systems.

  Note: Insight Lookup does not scan a folder or a drive when you perform this type of scan. Insight Lookup does run if you select a file or group of files to scan.

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.

See “Managing scans on your computer” on page 52.

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**.

Troubleshooting computer issues with the Symantec Help support tool

You can download a utility to diagnose common issues you encounter with installing and using Symantec Endpoint Protection Manager or the Symantec Endpoint Protection client.

The support tool helps you with the following issues:

- Lets you quickly and accurately identify known issues.
- When the tool recognizes an issue, the tool redirects you to the resources to resolve the issue yourself.
- When an issue is not resolved, the tool lets you easily submit data to Support for further diagnostics.

To troubleshoot computer issues with the Symantec Help support tool

1. Do one of the following tasks:
   - See the knowledge base article: Symantec Help (SymHelp)
   - In the client, click **Help > Download Support Tool**
2. Follow the on-screen instructions.

Chapter 2

Responding to alerts and notifications

This chapter includes the following topics:

Types of 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 2-1 displays the types of messages you might see and need to respond to.

Table 2-1 Types of alerts and notifications

Alert	Description
<scan name> started on or **Symantec Endpoint Protection Detection Results** dialog box	If a scan detects a virus or a security risk, the scan results or **Symantec Endpoint Protection 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 27.
Other message dialog boxes	You may see pop-up messages for the following reasons: ■ The client automatically updates the client software. See "Responding to messages to update the client software" on page 34. ■ 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 33. ■ The client's evaluation license has expired. See "Responding to expired license messages" on page 33.

Table 2-1 Types of alerts and notifications *(continued)*

Alert	Description

Notification area icon messages	Notifications that appear in 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.
	See "Responding to messages that ask you to allow or block an application" on page 33.
	■ 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 2/14/2010 15:37:58 to 2/14/2010 15:47:58. Port Scan attack is logged.`
	■ The security compliance check failed. Traffic may be blocked from going to and from your computer
	You do not need to do anything else other than read the messages.

See "How to determine whether the client is connected and protected" on page 40.

About scan results

For managed clients, your administrator typically configures a full scan to run at least one time each week. For unmanaged clients, an automatically-generated Active Scan runs when you start up your computer. By default, Auto-Protect runs continuously on your computer.

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.

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

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

See "About managed clients and unmanaged clients" on page 14.

See "Responding to a virus or a risk detection" on page 28.

See "Pausing and delaying scans" on page 23.

Responding to a virus or a risk detection

When an administrator-defined scan, a user-defined scan, or Auto-Protect runs, you might see a scan results dialog box. You can use the scan results dialog box to act on the affected file immediately. For example, you might decide to delete a cleaned file because you want to replace it with an original file.

If Symantec Endpoint Protection needs to terminate a process or application or stop a service, the **Remove Risks Now** option is active. You might not be able to close the dialog box if risks in the dialog require you to take action.

You can also use the Quarantine or the Risk Log or Scan Log to act on the file later.

To respond to a virus or risk detection in the scan results dialog box

1. In the scan results dialog box, select the files on which you want to act.
2. Right-click the selection, and then select one of the following options:

Clean	Removes the virus from the file. This option is only available for viruses.
Exclude	Excludes the file from being scanned again.
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.
Properties	Displays the information about the virus or security risk.

   In some cases, the action might not be available.

3. In the dialog box, click **Close**.

   You might not be able to close the dialog box if the risks that are listed require you to take action. For example, the client may need to terminate a process or an application, or it may need to stop a service.

   If you need to take action, one of the following notifications appear:

   - **Remove Risk Required**
     Appears when a risk requires process termination. If you choose to remove the risk, you return to the results dialog box. If a restart is also required, the information in the risk's row in the dialog box indicates that a restart is required.
   - **Restart Required**
     Appears when a risk requires a restart.
   - **Remove Risk and Restart Required**
     Appears when a risk requires process termination and another risk requires a restart.

4 If the **Remove Risks Now** dialog box appears, click one of the following options:

- **Remove Risks Now (recommended)**
  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.
- **Do not Remove Risks**
  The results dialog box reminds you that you still need to take action. However, the **Remove Risks Now** dialog box is suppressed until you restart your computer.

5 If the results dialog box did not close in step 3, click **Close**.

If a restart is required, the removal or repair is not complete until you restart the computer.

You might need to take action on a risk but choose not to take action right now.

The risk can be removed or repaired at a later time in the following ways:

- You can open the risk log, right-click the risk, and then take an action.
- You can run a scan to detect the risk and reopen the results dialog box.

You can also take action by right-clicking a risk in the dialog box and by selecting an action. The actions that you can take depend on the actions that were configured for the particular type of risk that the scan detected.

See “How scans respond to a virus or risk detection” on page 63.

See “Viewing the logs” on page 43.

See “Managing scans on your computer” on page 52.

See “Managing quarantined files on your client computer” on page 83.

Responding to Download Insight messages that ask you to allow or block a file that you try to download

Download Insight notifications display information about the malicious files and the unproven files that Download Insight detects when you try to download them.

Note: Regardless of whether or not notifications are enabled, you receive detection messages when the action for unproven files is **Prompt**.

You or your administrator can change how sensitive Download Insight is to malicious files. Changing the sensitivity level might change the number of notifications that you receive.

Download Insight uses Insight, which evaluates and determines a file rating that is based on its global community of millions of users.

The Download Insight notification shows the following information about the detected file:

- File reputation
  The file reputation indicates the trustworthiness of a file. Malicious files are not trustworthy. Unproven files may or may not be trustworthy.
- How common the file is in the community
  The prevalence of a file is important. Files that are not common might be more likely to be threats.
- How new the file is
  The newer a file is, the less information Symantec has about the file.

The information can help you to decide whether to allow or block the file.

To respond to a Download Insight detection that asks you to allow or block a file that you try to download

◆ In the Download Insight detection message, do one of the following actions:

  - Click **Remove this file from my computer**.
    Download Insight moves the file to the Quarantine. This option only appears for unproven files.
  - Click **Allow this file**.
    You might see a permission dialog that asks whether or not you are sure that you want to allow the file.
    If you choose to allow an unproven file that was not quarantined, the file runs automatically. If you choose to allow a quarantined file, the file does not automatically run. You can run the file from your temporary Internet folder.
    Typically the folder location is: `\\Documents and Settings \`*`username`*`\Local Settings\Temporary Internet Files`.
    On unmanaged clients, if you allow a file, the client automatically creates an exception for the file on this computer. On managed clients, if your administrator lets you create exceptions, the client automatically creates an exception for the file on this computer.

See "Managing Download Insight detections on your computer" on page 70.

See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 64.

See “Managing scans on your computer” on page 52.

Responding to the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers

On Windows 8 client computers, pop-up notifications for malware detections and other critical events appear on the Windows 8 style user interface and the Windows 8 desktop. The notifications alert you to an event that occurred in either the Windows 8 style user interface or the Windows 8 desktop, regardless of which interface you are currently viewing. You can see details about the event that produced the notification in a message on the Windows desktop.

On managed clients, your administrator might turn off pop-up notifications.

To respond to the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers

1. In the pop-up notification that appears at the top of the screen, do one of the following tasks:

   - In the Windows 8 style user interface, click the notification.
     The desktop appears.

   - On the desktop, click the notification.
     The notification disappears.

2. Review the detection results or other informational message that appears in the desktop.

   For the virus and spyware detections that do not affect Windows 8 style apps, you might need or want to perform an additional remediation action. For the detections that affect Windows 8 style apps, the only additional action that you can perform is **Exclude**.

   When you return to the Windows 8 style user interface, you might see an icon on an affected app that indicates that you must re-download the app.

See “How to manage the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers” on page 88.

See “Responding to a virus or a risk detection” on page 28.

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 can choose to block an application that you think is unsafe from accessing the network.

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.

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 a message that asks you to allow or block an application

1. Optionally, to suppress the message the next time the application tries to access the network, in the dialog box, 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**.

   You can also change the action of the application in the Running Applications field or in the Applications list.

See "Creating a firewall rule for an application when it accesses the network from your computer" on page 112.

Responding to expired license messages

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 the evaluation license has expired, the client does not update any content or the client software.

Table 2-2 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**.

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.`

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

See "Types of alerts and notifications" on page 25.

See "Viewing the logs" on page 43.

Responding to messages to update the client software

If the client software is automatically updated, you may see the following notification:

```
Symantec Endpoint Protection has detected that
a newer version of the software is available from
the Symantec Endpoint Protection Manager.
Do you wish to download it now?
```

To respond to an automatic update notification

1 Do one of the following actions:

- To download the software immediately, click **Download Now**.
- To be reminded after the specified time, click **Remind me later**.

2 If a message appears after the installation process begins for the updated software, click **OK**.

Chapter 3

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 computer runs an unmanaged client.
  Once an unmanaged client is installed, only you have control over your computer's protection. An unmanaged client is protected by default, but you may need to modify the computer's protection settings.
- 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 or security threat and want to run a scan.

Table 3-1 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 might detect a virus or security risk and display the scan results that ask you to act on the detection. See "Types of alerts and notifications" on page 25.
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 13. See "Enabling or disabling protection on the client computer" on page 46.
Update virus definitions	Check 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 computer's protection" on page 37. You can perform these tasks on a managed client if your administrator allows it.
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 22.
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: ■ Schedule additional scans See "Managing scans on your computer" on page 52. ■ Add firewall rules (unmanaged client only) See "Managing firewall protection" on page 97.

Table 3-1 Process for managing your computer's protection *(continued)*

Step	Description
View logs for detections or attacks	Check the logs to see if your client has detected a virus or network attack. See "Viewing the logs" on page 43.
Update the security policy (Managed client only)	Check that the client received the latest security policy from a management server. 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 "How to determine whether the client is connected and protected" on page 40.

See "About managed clients and unmanaged clients" on page 14.

Updating the computer's protection

Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available through LiveUpdate.

Content updates are the files that keep your Symantec products current with the latest threat protection technology. The content updates that you receive depend on which protections are installed on your computer. For example, LiveUpdate downloads virus definition files for Virus and Spyware Protection and IPS definition files for Network Threat Protection.

LiveUpdate can also provide improvements to the installed client on an as-needed basis. These improvements are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors.

LiveUpdate retrieves the new content files from a Symantec Internet site, and then replaces the old content files. A client computer can receive these improvements directly from a LiveUpdate server. A managed client computer can also receive these improvement updates automatically from a management server at your company. How your computer receives the updates depends on whether your computer is managed or unmanaged, and on how your administrator has configured updates.

Table 3-2 Ways to update content on your computer

Task	Description
Update the content on a schedule	By default, LiveUpdate runs automatically at scheduled intervals. On an unmanaged client, you can disable or change a LiveUpdate schedule. See "Updating the content on a schedule" on page 38.
Update the content immediately	Based on your security settings, you can run LiveUpdate immediately. See "Updating the content immediately" on page 38.

Updating the content immediately

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

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

See "Updating the content on a schedule" on page 38.

See "Updating the computer's protection" on page 37.

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 the content on a schedule

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

See "Updating the content immediately" on page 38.

Note: If you have a managed client, you can only configure LiveUpdate to run on a schedule if your administrator has enabled you to. If the padlock icon appears and the options are grayed out, you cannot update your content on a schedule.

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 **LiveUpdate**.
4. On the **LiveUpdate** tab, check **Enable automatic updates**.
5. In the **Frequency and Time** group box, select whether you want the updates to run daily, weekly, or monthly. Then select the day or week and time of day you want the updates to run.

   The time settings depend on what you select from the **Frequency** group box. The availability of the other options also depends on the frequency that you select.
6. In the **Retry Window** group box, check **Keep trying for**, and then specify the time interval during which the client tries to run LiveUpdate again.
7. In the **Randomization Options** group box, check **Randomize the start time to be + or - 9in hours)**, 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.
8. In the **Idle Detection** group box, check **Delay scheduled LiveUpdates until the system is idle. Overdue sessions will eventually run unconditionally.**

   You can also configure options for proxy server connection to an internal LiveUpdate server. See the online Help for information about the options.
9. Click **OK**.

Manually updating policies on the client

You can manually update the policies on the client computer if you do not think you have the latest policy on the client. If the client does not receive the update, there might be a communication problem.

Check the policy serial number to check whether your managed client computers can communicate with the management server.

To manually update policies from the client computer

1. On the client computer, in the client user interface, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, in the left column, click **Management**.
3. On the **Management** panel, under **Policy Profile**, click **Update**.

How to determine whether the client is connected and protected

You can check the notification area icon on the client to determine whether the client is connected to a management server and adequately protected.

The icon is located in the lower-right hand corner of the client computer desktop. You can also right-click this icon to display frequently used commands.

Note: On managed clients, the notification area icon does not appear if your administrator has configured it to be unavailable.

Table 3-3 Symantec Endpoint Protection client status icons

Icon	Description
🛡	The client runs with no problems. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain yellow shield.
🛡●	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 is a yellow shield with a green dot.
🛡!	The client has a minor problem. For example, the virus definitions may be out of date. The icon is a yellow shield and a light yellow dot that contains a black exclamation mark.
🛡⊘	The client does not run, has a major problem, or has at least one protection technology disabled. For example, Network Threat Protection may be disabled. The icon is a yellow shield with a white dot outlined in red and a red line across the dot.

Table 3-4 displays the Symantec Network Access Control client status icons that appear in notification area.

Table 3-4 Symantec Network Access Control client status icons

Icon	Description
🔑	The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain gold key.

Table 3-4 Symantec Network Access Control client status icons *(continued)*

Icon	Description
🔑	The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It communicates with the server. The icon is a gold key with a green dot.
🔑	The client has either failed the Host Integrity check or has not updated the security policy. The icon is a gold key with a red dot that contains a white "x."

See "Hiding and displaying the notification area icon" on page 41.

Hiding and displaying the notification area icon

You can hide the notification area icon if necessary. For example, you can hide it if you need more space on the Windows taskbar.

See "How to determine whether the client is connected and protected" on page 40.

Note: On managed clients, you cannot hide the notification area icon if your administrator has restricted this functionality.

To hide or display the notification area icon

1. In the main window, in the sidebar, click **Change settings**.
2. On the **Change Settings** page, for **Client Management**, click **Configure Settings**.
3. In the **Client Management Settings** dialog box, on the **General** tab, under **Display Options**, uncheck or check **Show Symantec security icon in notification area**.
4. Click **OK**.

About the logs

Logs contain information about client configuration changes, security-related activities, and errors. These records are called events.

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.

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

Table 3-5 Client logs

Log	Description
Scan Log	Contains the entries about the scans that have run on your computer over time.
Risk Log	Contains the entries about viruses and security risks, such as adware and spyware, which have infected your computer. Security risks include a link to the Symantec Security Response Web page that provides additional information. See "Quarantining a file from the Risk log or Scan log" on page 85.
Virus and Spyware Protection System Log	Contains the 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 the information about the threats that SONAR detected on your computer. SONAR detects any files that act suspiciously. SONAR also detects system changes.
Proactive Threat Protection System Log	Contains the information about system activities on your computer that are related to SONAR.
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 trace traffic back to its source, and troubleshoot 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 the 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. See "Enabling the Packet Log" on page 44.

Table 3-5 Client logs *(continued)*

Log	Description
Control Log	Contains the information about the Windows registry keys, files, and DLLs that an application accesses, as well as the applications that your computer runs.
Security Log	Contains the information about the activities that can pose a threat to your computer. For example, information might appear about such activities as denial-of-service attacks, port scans, and executable file alterations.
Client Management System Log	Contains the information about all of the operational changes that have occurred on your computer. The changes might include the following activities: ■ A service starts or stops ■ The computer detects network applications ■ The software is configured
Tamper Protection Log	Contains the 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.
Debug Logs	Contains the 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.

See "Viewing the logs" on page 43.

Viewing the logs

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

Note: If **Network Threat Protection** or **Network Access Control** are not installed, you cannot view the Security Log, System Log, or Control Log.

To view a log

1. In the main window, in the sidebar, click **View Logs**.
2. Click **View Logs** next to one of the following items:
   - **Virus and Spyware Protection**

- **Proactive Threat Protection**
- **Network Threat Protection**
- **Client Management**
- **Network Access Control**

Some items might not appear, depending on your installation.

3 In the drop-down menu, select the log that you want to view.

See "About the logs" on page 41.

Enabling the Packet Log

All Network Threat Protection logs and Client Management logs are enabled by default, except for the Packet Log. On unmanaged clients, you can enable and disable the Packet Log.

On managed clients, your administrator might let you enable or disable the Packet Log.

See "About the logs" on page 41.

To enable the Packet Log

1 In the client, on the **Status** page, to the right of Network Threat Protection, click **Options**, and then click **Change Settings**.

2 In the **Network Threat Protection Settings** dialog box, click **Logs**.

3 Check **Enable Packet Log**.

4 Click **OK**.

About enabling and disabling protection when you need to troubleshoot problems

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

You might need to temporarily disable either all the protection technologies or individual protection technologies if you have a problem with the client computer. For example, if an application 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, completely uninstall the client. If the problem persists, you know that the problem is not due to Symantec Endpoint Protection.

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

Table 3-6 describes the reasons why you might want to disable each protection technology.

Table 3-6 Purpose for disabling a protection technology

Protection technology	Purpose for disabling the protection technology
Virus and Spyware Protection	If you disable this 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 might 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 let you 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. **Note:** If you disable Auto-Protect, you also disable Download Insight, even if Download Insight is enabled. SONAR also cannot detect heuristic threats. SONAR detection of host file and system changes continues to function. See "Enabling or disabling Auto-Protect" on page 47. If Auto-Protect causes a problem with an application, it is better to create an exception than to permanently disable the protection. See "Excluding items from scans" on page 81.
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 protection on the client computer" on page 46.

Table 3-6 Purpose for disabling a protection technology *(continued)*

Protection technology	Purpose for disabling the protection technology
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. ■ 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. On a managed client, your administrator might lock Network Threat Protection completely so that you cannot enable or disable it. See "Enabling or disabling intrusion prevention" on page 116. See "Enabling or disabling protection on the client computer" on page 46.
Tamper Protection	Typically, you should keep Tamper Protection enabled. You might want to disable Tamper Protection temporarily if you get an extensive number of false positive detections. For example, some third-party applications might make the changes that inadvertently try to modify Symantec settings or processes. If you are sure that an application is safe, you can create a Tamper Protection exception for the application. See "Enabling, disabling, and configuring Tamper Protection" on page 49.

Enabling or disabling protection on the client computer

For troubleshooting purposes, you may need to disable Auto-Protect, Proactive Threat Protection, or Network Threat Protection.

On the client, when any of the protections are disabled:

- The status bar is red at the top of the **Status** page.
- 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 "How to determine whether the client is connected and protected" on page 40.

On a managed client, your administrator can enable or disable a protection technology at any time. If you disable a protection, your administrator may later enable the protection again. Your administrator might also lock a protection so that you cannot disable it.

Warning: Symantec recommends that you only disable Auto-Protect temporarily if you need to troubleshoot the client computer.

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**.
  - Click **Disable Symantec Endpoint Protection**.

To enable or disable protection technologies from within the client

- In the client, on the **Status** page, beside ***protection type*** **Protection**, do one of the following tasks:
  - Click **Options > Enable *protection type* Protection**.
  - Click **Options > Disable all *protection type* Protection features**.

To enable or disable the firewall

1. On the client, at the top of the **Status** page, next to **Network Threat Protection**, click **Options** > **Change Settings**.
2. On the **Firewall** tab, check or uncheck **Enable Firewall**.
3. Click **OK**.

See "About enabling and disabling protection when you need to troubleshoot problems" on page 44.

See "Enabling or disabling Auto-Protect" on page 47.

Enabling or disabling Auto-Protect

You can enable or disable 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.

On a managed client, your administrator might lock Auto-Protect so that you cannot disable it. Also, your administrator might specify that you can disable Auto-Protect temporarily, but that Auto-Protect turns on automatically after a specified amount of time.

Note: If you disable Auto-Protect, you also disable Download Insight even if Download Insight is enabled. SONAR also cannot detect heuristic threats; however, SONAR continues to detect host file and system changes.

Warning: Symantec recommends that if you need to troubleshoot Auto-Protect on the client computer, you only disable it temporarily.

To enable or disable Auto-Protect for the file system

◆ 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 all Virus and Spyware Protection features**.

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**.
   - On the **Notes Auto-Protect** tab, check or uncheck **Enable Lotus Notes Auto-Protect**.

   Internet Email Auto-Protect is not supported on server operating systems. Microsoft Outlook Auto-Protect is automatically installed on the computers that run Outlook.
4. Click **OK**.

See “About the types of Auto-Protect” on page 62.

See “About the alert icons on the Status page” on page 17.

See “About enabling and disabling protection when you need to troubleshoot problems” on page 44.

Enabling, disabling, and configuring Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents threats and security risks from tampering with Symantec resources. You can enable or disable Tamper Protection. You can also configure the action that Tamper Protection takes when it detects a tampering attempt on the Symantec resources on your computer.

By default, Tamper Protection is set to **Block and do not log**.

Note: On a managed client, your administrator might lock the Tamper Protection settings.

See “About enabling and disabling protection when you need to troubleshoot problems” on page 44.

To enable or disable Tamper Protection

1. In the client, in the sidebar, click **Change settings**.
2. Next to **Client Management**, click **Configure Settings**.
3. On the **Tamper Protection** tab, check or uncheck **Protect Symantec security software from being tampered with or shut down**.
4. Click **OK**.

To configure Tamper Protection

1. In the client, in the sidebar, click **Change settings**.
2. Next to **Client Management**, click **Configure Settings**.
3. On the **Tamper Protection** tab, in the **Action to take if an application attempts to tamper with or shut down Symantec security software** list box, click **Log only**, **Block and do not log** or **Block and log**.
4. Click **OK**.

Chapter 4

Managing scans

This chapter includes the following topics:

- Changing SONAR settings

Managing scans on your computer

By default, the client runs an active scan every day. On a managed client, you might be able to configure your own scans, if your administrator made these settings available. An unmanaged client includes a preset active scan that is disabled, but you can manage your own scans.

Table 4-1 Managing scans

Task	Description
Read about how scans work	Review the types of scans and the types of viruses and security risks. See "How virus and spyware scans work" on page 56.
Update virus definitions	Make sure that you have the latest virus definitions installed on your computer. See "Updating the computer's protection" on page 37.
Check that Auto-Protect is enabled	Auto-Protect is enabled by default. You should always keep Auto-Protect enabled. If you disable Auto-Protect, you also disable Download Insight and you prevent SONAR from making heuristic detections. See "Enabling or disabling Auto-Protect" on page 47.
Scan your computer	Regularly scan your computer for viruses and security risks. Ensure that scans run regularly by checking the last scan date. See "Scanning your computer immediately" on page 22. See "Scheduling a user-defined scan" on page 65. When scans run, you might see a scan results dialog box. You can use the scan results dialog box to perform some actions on the items that scans detect. See "Responding to a virus or a risk detection" on page 28. You can pause a scan that you started. On a managed client, your administrator determines whether you can pause an administrator-initiated scan. See "Pausing and delaying scans" on page 23.

Table 4-1 Managing scans *(continued)*

Task	Description
Adjust scans to improve your computer performance	By default, Symantec Endpoint Protection provides a high level of security while it minimizes the affect on your computer performance. You can customize settings to increase the computer performance even more. For scheduled and on-demand scans you can change the following options: ■ Scan tuning Set the scan tuning to **Best Application Performance**. ■ Compressed files Change the number of levels to scan compressed files. ■ Resumable scans You can specify a maximum time for a scan to run. The scan resumes when the computer is idle. ■ Randomized scans You can specify that a scan randomizes its start time within a specific time interval. You might also want to disable startup scans or change the schedule for your scheduled scans. See "Customizing virus and spyware scan settings" on page 74. See "Scheduling a user-defined scan" on page 65.

Table 4-1 Managing scans *(continued)*

Task	Description
Adjust scans to increase protection on your computer	In most cases, the default scan settings provide adequate protection for your computer. In some cases you might want to increase the protection. If you do increase the protection, you might affect your computer performance. For scheduled and on-demand scans you can change the following options: ■ Scan performance Set the scan tuning to **Best Scan Performance**. ■ Scan actions Change the remediation actions that occur when a virus is detected ■ Scan duration By default, the scheduled scans that run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to **Scan until finished**. ■ Insight Lookup You should make sure that Insight Lookup is enabled. Insight Lookup settings are similar to the settings for Download Insight. ■ Increase the level of Bloodhound protection. Bloodhound locates and isolates the logical regions of a file to detect virus-like behavior. You can change the detection level from **Automatic** to **Aggressive** to increase the protection on your computer. The **Aggressive** setting, however, is likely to produce more false positives. See "Customizing virus and spyware scan settings" on page 74.
Identify scan exceptions	Exclude a safe file or process from being scanned. See "Excluding items from scans" on page 81.
Submit information about detections to Symantec	By default, your client computer sends information about detections to Symantec Security Response. You can turn off submissions or choose which kinds of information to submit. Symantec recommends that you always enable submissions. The information helps Symantec address threats. See "Submitting information about detections to Symantec Security Response" on page 89.

Table 4-1 Managing scans *(continued)*

Task	Description
Manage quarantined files	Symantec Endpoint Protection quarantines infected files and moves them to a location where the files do not infect other files on the computer. If a quarantined file cannot be repaired, you must decide what to do with the file. You can also do the following actions: ■ 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. ■ 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 quarantined files on your client computer" on page 83. See "About quarantining files" on page 84.

Table 4-2 displays additional scan settings that you can modify if you want to increase protection, improve performance, or reduce false positives.

Table 4-2 Scan settings

Task	Description
Modify Auto-Protect settings to improve your computer performance or increase protection	For Auto-Protect, you might want to change the following options: ■ File cache Make sure that the file cache is enabled (the default is enabled). When the file cache is enabled, Auto-Protect remembers the clean files that it scanned and does not rescan them. ■ Network settings When Auto-Protect on remote computers is enabled, make sure that **Only when files are executed** is enabled. ■ You can also specify that Auto-Protect trusts files on remote computers and uses a network cache. By default, Auto-Protect scans files as they are written from your computer to a remote computer. Auto-Protect also scans files when they are written from a remote computer to your computer. A network cache stores a record of the files that Auto-Protect scanned from a remote computer. If you use a network cache, you prevent Auto-Protect from scanning the same file more than one time. See "Customizing virus and spyware scan settings" on page 74.

Table 4-2 Scan settings *(continued)*

Task	Description
Manage ELAM detections	You might want to enable or disable the client early launch anti-malware (ELAM) detection if you believe ELAM that affects your computer's performance. Or you might want to override the default detection setting if you get many false positive ELAM detections. See "Enabling or disabling early launch anti-malware (ELAM)" on page 87.
Manage Download Insight detections	Download Insight inspects the files that you try to download through Web browsers and text messaging clients and other portals. Download Insight uses information from Symantec Insight, which collects information about file reputation. Download Insight uses a file's reputation rating to allow or block a file or prompt the user to take action on the file. See "Managing Download Insight detections on your computer" on page 70.
Manage SONAR	You can adjust the settings for SONAR. See "Managing SONAR on your client computer" on page 93.

How virus and spyware scans work

Virus and spyware 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 63.

Note: Symantec Endpoint Protection does not quarantine or clean any risk that is detected in Windows 8 style apps. Symantec Endpoint Protection deletes the risk instead.

Table 4-3 describes the components that the client scans on your computer.

Table 4-3 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 software uses pattern-based scanning to search for traces of viruses within files. The traces of viruses are called patterns or signatures. Each file is compared to the innocuous signatures that are contained in a virus definitions file, as a way of identifying specific viruses. If a virus is found, by default the client tries to clean the virus from the file. If the file cannot be cleaned, the client quarantines the file to prevent further infection of your computer. The client also uses pattern-based scanning to search for signs of security risks within files and Windows 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.
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.

About viruses and security risks

Symantec Endpoint Protection scans for both viruses and for security risks. Security risks include spyware, adware, rootkits, and other files that can put a computer or a network at risk.

Viruses and security risks can arrive through email messages or instant messenger programs. You can unknowingly download a risk by accepting an End User License Agreement from a software program.

Many viruses and security risks are installed as "drive-by downloads." These downloads usually occur when you visit malicious or infected Web sites, and the application's downloader installs through a legitimate vulnerability on your computer.

You can view information about specific risks on the Symantec Security Response Web site.

The Symantec Security Response Web site provides the latest information about threats and security risks. The Web site also contains extensive reference information, such as white papers and detailed information about viruses and security risks.

See “How scans respond to a virus or risk detection” on page 63.

Figure 4-1 How viruses and security risks attack a computer

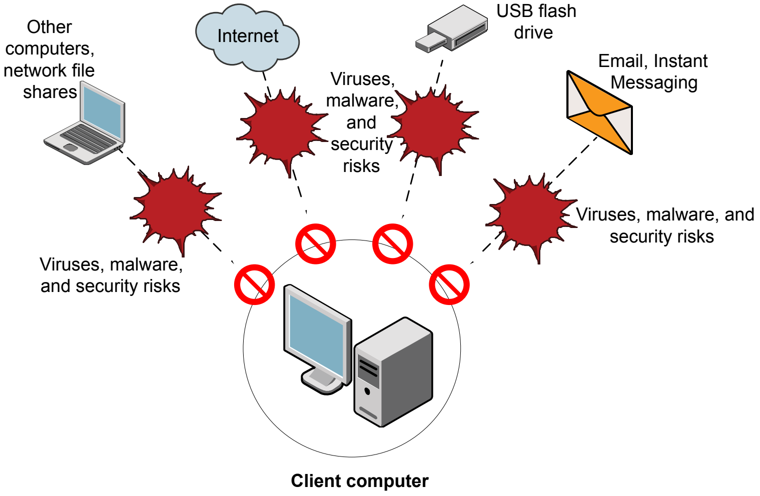
Other computers, network file shares
Internet
USB flash drive
Email, Instant Messaging
Viruses, malware, and security risks
Viruses, malware, and security risks
Viruses, malware, and security risks
Client computer

Table 4-4 lists the type of viruses and risks that can attack a computer.

Table 4-4 Viruses and security risks

Risk	Description
Viruses	Programs or code that attach a copy of themselves to another computer program or file when it runs. When the infected program runs, the attached virus program activates and attaches itself to other programs and files. The following types of threats are included in the virus category: ■ Malicious Internet bots Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites. ■ Worms Programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate in memory to reduce computer performance. ■ Trojan horses Programs that hide themselves in something benign, such as a game or utility. ■ Blended threats 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. ■ Rootkits Programs that hide themselves from a computer's operating system.
Adware	Programs that deliver advertising content.
Dialers	Programs that use a computer, without the user's permission or knowledge, to dial out through the Internet to a 900 number or FTP site. Typically, these numbers are dialed to accrue charges.
Hacking tools	Programs that hackers 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	Programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a joke program might move the recycle bin away from the mouse when the user tries to delete an item.
Misleading applications	Applications that intentionally misrepresent the security status of a computer. These applications typically masquerade as security notifications about fake infections that must be removed.
Parental control programs	Programs that monitor or limit computer usage. The programs can run undetected and typically transmit monitoring information to another computer.

Table 4-4 Viruses and security risks *(continued)*

Risk	Description
Remote access programs	Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer.
Security assessment tool	Programs that are used to gather information for unauthorized access to a computer.
Spyware	Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.
Trackware	Stand-alone or appended applications that trace a user's path on the Internet and send information to the controller or hacker's system.

About the types of scans

Symantec Endpoint Protection includes different types of scans to provide protection against different types of viruses, threats, and risks.

By default, Symantec Endpoint Protection runs an active scan every day at 12:30 P.M. Symantec Endpoint Protection also runs an active scan when new definitions arrive on the client computer. On unmanaged computers, Symantec Endpoint Protection also includes a default startup scan that is disabled.

On unmanaged clients, you should make sure that you run an active scan every day on your computer. You might want to schedule a full scan once a week or once a month if you suspect that you have an inactive threat on your computer. Full scans consume more computer resources and might impact computer performance.

Table 4-5 Scan types

Scan type	Description
Auto-Protect	Auto-Protect continuously inspects files and email data as they are written to or read from a computer. Auto-Protect automatically neutralizes or eliminates detected viruses and security risks. Auto-Protect also protects some email that you might send or receive. See “About the types of Auto-Protect” on page 62.

Table 4-5 Scan types *(continued)*

Scan type	Description
Download Insight	Download Insight boosts the security of Auto-Protect by inspecting files when users try to download them from browsers and other portals. Download Insight uses information from Symantec Insight, which collects information from millions of users to determine the security reputations of files in the community. Download Insight uses a file's reputation rating to allow or block a file or prompt the user to take action on the file. Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled. If you disable Auto-Protect but enable Download Insight, Download Insight cannot function. See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 64.
Administrator scans and user-defined scans	For managed clients, your administrator might create scheduled scans or run scans on demand. For unmanaged clients, or managed clients for which scan settings are unlocked, you can create and run your own scans. Administrator or user-defined scans detect viruses and security risks by examining all files and processes on the client computer. These types of scans can also inspect memory and load points. The following types of administrator or user-defined scans are available: ■ Scheduled scans A scheduled scan runs on the client computers at designated times. Any 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. You can save your scheduled scan settings as a template. You can use any scan that you save as a template as the basis for a different scan. The scan templates can save you time when you configure multiple policies. A scheduled scan template is included by default in the policy. The default scheduled scan scans all files and folders. ■ Startup scans and triggered scans Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers. ■ On-demand scans On-demand scans are scans that you start manually. You can run scans on demand from the **Scan for Threats** page. See "How virus and spyware scans work" on page 56.

Table 4-5 Scan types *(continued)*

Scan type	Description
SONAR	SONAR can stop attacks even before traditional signature-based definitions detect a threat. SONAR uses heuristics as well as file reputation data to make decisions about applications or files. See "About SONAR" on page 91.

See "Managing scans on your computer" on page 52.

About the types of Auto-Protect

Auto-Protect scans files as well as certain types of email and email attachments.

If your client computer runs other email security products, such as Symantec Mail Security, you might not need to enable Auto-Protect for email.

Auto-Protect works on your supported email client only. It does not protect email servers.

Note: If a virus is detected as you open email, your email may take several seconds to open while Auto-Protect completes its scan.

Table 4-6 Types of Auto-Protect

Type of Auto-Protect	Description
Auto-Protect	Continuously scans files as they are read from or written to your computer Auto-Protect is enabled by default for the file system. It loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services. You can configure Auto-Protect to scan only selected file extensions. When Auto-Protect scans the selected extensions, it can also determine a file's type even if a virus changes the file's extension. If you do not run Auto-Protect for email, your client computers are still protected when Auto-Protect is enabled. Most email applications save attachments to a temporary folder when users launch email attachments. Auto-Protect scans the file as it is written to the temporary folder and detects any virus or security risk. Auto-Protect also detects the virus if the user tries to save an infected attachment to a local drive or network drive.

Table 4-6 Types of Auto-Protect *(continued)*

Type of Auto-Protect	Description
Internet Email Auto-Protect	Scans internet email (POP3 or SMTP) and attachments for viruses and security risks; also performs outbound email heuristics scanning. By default, Internet Email Auto-Protect supports encrypted passwords and email over POP3 and SMTP connections. If you use POP3 or SMTP with Secure Sockets Layer (SSL), then the client detects secure connections but does not scan encrypted messages. **Note:** For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. Internet email scanning also is not supported for 64-bit computers. Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.
Microsoft Outlook Auto-Protect	Scans Microsoft Outlook email (MAPI and Internet) and attachments for viruses and security risks Supported for Microsoft Outlook 98/2000/2002/2003/2007/2010 (MAPI and Internet) If Microsoft Outlook is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Microsoft Outlook Auto-Protect. If you use Microsoft Outlook over MAPI or Microsoft Exchange client and you have Auto-Protect enabled for email, attachments are immediately downloaded. The attachments are scanned when you open the attachment. If you download a large attachment over a slow connection, mail performance is affected. You may want to disable this feature if you regularly receive large attachments. **Note:** On a Microsoft Exchange server, you should not install Microsoft Outlook Auto-Protect.
Lotus Notes Auto-Protect	Scans Lotus Notes email and attachments for viruses and security risks Supported for Lotus Notes 4.5 through 8.x. If Lotus Notes is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Lotus Notes Auto-Protect.

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 4-7 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 84. **Note:** Symantec Endpoint Protection does not quarantine a virus that is detected in Windows 8 style apps and files. Symantec Endpoint Protection deletes the virus instead.
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. **Note:** Symantec Endpoint Protection does not quarantine a security risk that is detected in Windows 8 style apps and files. Symantec Endpoint Protection deletes the risk instead.

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.

How Symantec Endpoint Protection uses reputation data to make decisions about files

Symantec collects information about files from its global community of millions of users and its Global Intelligence Network. The collected information forms a reputation database that Symantec hosts. Symantec products leverage the information to protect client computers from new, targeted, and mutating threats. The data is sometimes referred to as being in the cloud since it does not reside on the client computer. The client computer must request or query the reputation database.

Symantec uses a technology it calls Insight to determine each file's level of risk or security rating.

Insight determines a file's security rating by examining the following characteristics of the file and its context:

- The source of the file
- How new the file is
- How common the file is in the community
- Other security metrics, such as how the file might be associated with malware

Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight relies on reputation information to make detections. If you disable Insight lookups, Download Insight runs but cannot make detections. Other protection features, such as Insight Lookup and SONAR, use reputation information to make detections; however, those features can use other technologies to make detections.

By default, a client computer sends information about reputation detections to Symantec Security Response for analysis. The information helps to refine Insight's reputation database. The more clients that submit information the more useful the reputation database becomes.

You can disable the submission of reputation information. Symantec recommends, however, that you keep submissions enabled.

Client computers also submit other types of information about detections to Symantec Security Response.

See "Managing Download Insight detections on your computer" on page 70.

See "Submitting information about detections to Symantec Security Response" on page 89.

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.

Your computer must be turned on and Symantec Endpoint Protection Services must be loaded when the scan is scheduled to take place. By default, Symantec Endpoint Protection Services are loaded when you start your computer.

For managed clients, the administrator may override these settings.

See “Scanning your computer immediately” on page 22.

See “Managing scans on your computer” on page 52.

Consider the following important points when you set up a scheduled scan:

User-defined scans do not require the user to be logged in	If the user who defined a scan is not logged in, Symantec Endpoint Protection runs the scan anyway. You can specify that the client does not run the scan if the user is logged off.
Multiple simultaneous scans run serially	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.
Missed scheduled scans might not run	If your computer misses a scheduled scan for some reason, by default Symantec Endpoint Protection tries to perform the scan until it starts or until a specific time interval expires. If Symantec Endpoint Protection cannot start the missed scan within the retry interval, it does not run the scan.

Scheduled scan time might drift	Symantec Endpoint Protection might not use the scheduled time if the last run of the scan occurred at a different time because of the scan duration or missed scheduled scan settings. For example, you might configure a weekly scan to run every Sunday at midnight and a retry interval of one day. If the computer misses the scan and starts up on Monday at 6am, the scan runs at 6am. The next scan is performed one week from Monday at 6am rather than the next Sunday at midnight. If you did not restart your computer until Tuesday at 6am, which is two days late and exceeds the retry interval, Symantec Endpoint Protection does not retry the scan. It waits until the next Sunday at midnight to try to run the scan. In either case, if you randomize the scan start time you might change the last run time of the scan.

For more information about 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. You should run an active scan every day.
Full Scan	Scans the entire computer for viruses and security risks. You might want to run a full scan once a week or once a month. Full scans might affect your computer performance.
Custom Scan	Scans the selected areas of the computer for viruses and security risks.

4 Click **Next**.

5 If you selected **Custom Scan**, 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.

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.

See "Scheduling a scan to run on demand or when the computer starts up" on page 69.

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

10 Under **Scan Duration**, you can specify a length of time during which the scan must complete. You can also randomize the scan start time.

11 Under **Missed Scheduled Scans**, you can specify an interval during which a scan can be retried.

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

For example, call the scan: Friday morning

13 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 22.

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 Specify what to scan and any scan options for the scheduled scan.

See "Scheduling a user-defined scan" on page 65.

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**.

Managing Download Insight detections on your computer

Auto-Protect includes a feature that is called Download Insight, which examines the files that you try to download through Web browsers, text messaging clients, and other portals. Auto-Protect must be enabled for Download Insight to function.

Supported portals include Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Windows Live Messenger, and Yahoo Messenger.

Note: In the Risk log, the risk details for a Download Insight detection show only the first portal application that attempted the download. For example, you might use Internet Explorer to try to download a file that Download Insight detects. If you then use Firefox to try to download the file, the **Downloaded by** field in the risk details shows Internet Explorer as the portal.

Note: Auto-Protect can also scan the files that users receive as email attachments.

Table 4-8 Managing Download Insight detections on your computer

Task	Description
Learn how Download Insight uses reputation data to make decisions about files	Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Download Insight uses reputation information exclusively when it makes decisions about downloaded files. It does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or SONAR scans the file when the user opens or runs the file. See "How Symantec Endpoint Protection uses reputation data to make decisions about files" on page 64.

Table 4-8 Managing Download Insight detections on your computer *(continued)*

Task	Description
Respond to Download Insight detections	You might see notifications when Download Insight makes a detection. For managed clients, your administrator might choose to disable Download Insight detection notifications. When notifications are enabled, you see messages when Download Insight detects a malicious file or an unproven file. For unproven files, you must choose whether or not to allow the file. See "Responding to Download Insight messages that ask you to allow or block a file that you try to download" on page 30.
Create exceptions for specific files or Web domains	You can create an exception for an application that your users download. You can also create an exception for a specific Web domain that you believe is trustworthy. By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. Trusted sites are configured on the **Windows Control Panel > Trusted Internet Sites > Security** tab. When the **Automatically trust any file downloaded from an intranet site** option is enabled, Symantec Endpoint Protection allows any file that a user downloads from one of the trusted sites. Download Insight recognizes only explicitly configured trusted sites. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight cannot recognize 10.*.*.* as a trusted site. Download Insight also does not support the sites that are discovered by the **Internet Options > Security > Automatically detect intranet network** option. See "Excluding items from scans" on page 81.
Make sure that Insight lookups are enabled	Download Insight requires reputation data to make decisions about files. If you disable Insight lookups, Download Insight runs but cannot make detections. Insight lookups are enabled by default. See "Submitting information about detections to Symantec Security Response" on page 89.

Table 4-8 Managing Download Insight detections on your computer *(continued)*

Task	Description
Customize Download Insight settings	You might want to customize Download Insight settings for the following reasons: ■ Increase or decrease the number of Download Insight detections. You can adjust the malicious file sensitivity slider to increase or decrease the number of detections. At lower sensitivity levels, Download Insight detects fewer files as malicious and more files as unproven. Fewer detections are false positive detections. At higher sensitivity levels, Download Insight detects more files as malicious and fewer files as unproven. More detections are false positive detections. ■ Change the action for malicious or unproven file detections. You can change how Download Insight handles malicious or unproven files. You might want to change the action for unproven files so that you do not receive notifications for those detections. ■ Get alerts about Download Insight detections. When Download Insight detects a file that it considers malicious, it displays a message on the client computer if the action is set to **Quarantine**. You can undo the quarantine action. When Download Insight detects a file that it considers unproven, it displays a message on the client computer if you set the action for unproven files to **Prompt** or **Quarantine**. When the action is set to **Prompt**, you can allow or block the file. When the action is **Quarantine**, you can undo the quarantine action. You can turn off user notifications so that you do not have a choice when Download Insight detects a file that it considers unproven. If you keep notifications enabled, you can set the action for unproven files to **Ignore** so that these detections are always allowed and you are not notified. When notifications are enabled, the malicious file sensitivity setting affects the number of notifications that you receive. If you increase the sensitivity, you increase the number of user notifications because the total number of detections increases. See "Customizing Download Insight settings" on page 73.
Submit information about reputation detections to Symantec	By default, clients send information about reputation detections to Symantec. Symantec recommends that you enable submissions for reputation detections. The information helps Symantec address threats. See "Submitting information about detections to Symantec Security Response" on page 89.

Customizing Download Insight settings

You might want to customize Download Insight settings to decrease false positive detections on client computers. You can change how sensitive Download Insight is to the file reputation data that it uses to characterize malicious files. You can also change the notification that Download Insight displays on client computers when it makes a detection.

See “Managing Download Insight detections on your computer” on page 70.

Customizing Download Insight settings

1. In the client, in the sidebar, click **Change Settings**.
2. Next to **Virus and Spyware Protection**, click **Configure Settings**.
3. On the **Download Insight** tab, make sure that **Enable Download Insight to detect potential risks in downloaded files based on file reputation** is checked.

   If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.
4. Move the slider to change the malicious file sensitivity.

   Note: If you or your administrator installed basic Virus and Spyware Protection, the malicious file sensitivity is set to level 1 automatically and cannot be changed.

   If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.
5. Check or uncheck the following options to use as additional criteria for examining unproven files:
   - **Files with fewer than *x* users**
   - **Files known by users for less than *x* days**
     When unproven files meet this criteria, Download Insight detects the files as malicious.
6. Make sure that **Automatically trust any file downloaded from an intranet website** is checked.

   This option also applies to Insight Lookup detections.
7. Click **Actions**.
8. Under **Malicious Files**, specify a first action and a second action.
9. Under **Unproven Files**, specify the action.

10 Click **OK**.

11 Click **Notifications**, and specify whether or not to display a notification when Download Insight makes a detection.

You can customize the text of the warning message that appears.

12 Click **OK**.

Customizing virus and spyware scan settings

By default, Symantec Endpoint Protection gives your computer the protection against the viruses and security risks that you need. If you have an unmanaged client, you may want to configure some of the scan settings.

See “Managing scans on your computer” on page 52.

To customize 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 On the **Scan Options** tab, do any of the following tasks:

- To change Insight Lookup settings, click **Insight Lookup**.
  Insight Lookup settings are similar to Download Insight settings.
  See “Customizing Download Insight settings” on page 73.
- To specify fewer file types to scan, click **Selected extensions**, and then click **Extensions**.

  Note: User-defined scans always scan the extensions of container files unless you disable the compressed file option under **Advanced** or you create exceptions for the container extensions.

- To specify a first action and a second action that the client takes on an infected file, click **Actions**.
- To specify notification options, click **Notifications**.
  You can enable or disable the notifications that appear in the Windows 8 style user interface separately.
  See “How to manage the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers” on page 88.
- To configure advanced options for compressed files, backups, and tuning, click **Advanced**.

You might want to change the tuning options to improve your client computer performance.

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

4 Click **OK**.

To change global scan settings

1 Do one of the following actions:

- In the client, in the sidebar, click **Change settings**, and the next to Virus and Spyware Protection, click **Configure Settings**
- In the client, in the sidebar, click **Scan for Threats**, and then click **View Global Scan Settings**.

2 On the **Global Settings** tab, under **Scan Options**, change settings for Insight or Bloodhound.

3 To view or create scan exceptions, click **View List**. Click **Close** after you view or create exceptions.

4 Under **Log Retention** or **Internet Browser Protection**, make any changes that you want.

5 Click **OK**.

To customize Auto-Protect

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 a first action and a second action that the client takes on an infected file, click **Actions**.
- To specify notification options, click **Notifications**.

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

4 On the **Auto-Protect** tab, click **Advanced**.

You can change options for the file cache as well as options for Risk Tracer and backups. You might want to change these options to improve your computer performance.

5 Click **Network** to change settings for trusting files on remote computers and setting a network cache.

6 Click **OK**.

Configuring actions for malware and security risk detections

You can configure the actions that you want the Symantec Endpoint Protection client to take when it detects malware or a security risk. You can configure a first action and a second action to take if the first action fails.

Note: If an administrator manages your computer, and these options display a lock icon, you cannot change these options because your administrator has locked them.

You configure actions for any type of scan in the same way. Each scan has its own configuration for actions. You can configure different actions for different scans.

Note: You configure actions for Download Insight and SONAR separately.

See "Customizing virus and spyware scan settings" on page 74.

See "Customizing Download Insight settings" on page 73.

See "Changing SONAR settings" on page 94.

You can click Help for more information about the options that are used in the procedures.

To configure actions for malware and security risk detections

1. In the client, in the sidebar, click **Change settings** or **Scan for Threats**.
2. Do one of the following actions:
   - Next to Virus and Spyware Protection, click **Configure Settings**, and then on any Auto-Protect tab, click **Actions**.
   - Select a scan and then right-click and select **Edit**, and then click **Scan Options**.
3. Click **Actions**.
4. In the **Scan Actions** dialog box, in the tree, select the category or subcategory under **Malware** or **Security Risks**.

   By default, each subcategory is automatically configured to use the actions that are set for the entire category.

   The categories change dynamically over time as Symantec gets new information about risks.

5 To configure actions for a subcategory only, do one of the following actions:

- Check **Override actions configured for Malware**, and then set the actions for that subcategory only.

  Note: There might be a single subcategory under a category, depending on how Symantec currently classifies risks. For example, under Malware, there might be a single subcategory called Viruses.

- Check **Override actions configured for Security Risks**, and then set the actions for that subcategory only.

6 Select a first and second action from the following options:

Clean risk

Removes the virus from the infected file. This setting is the default first action for viruses.

Note: This action is only available as a first action for viruses. This action does not apply to security risks.

This setting should always be the first action for viruses. If the client successfully cleans a virus from a file, you do not need to take any other action. Your computer is free of viruses and is no longer susceptible to the spread of that virus into other areas of your computer.

When the client cleans a file, it removes the virus from the infected file, boot sector, or partition tables. It also eliminates the ability of the virus to spread. The client can usually find and clean a virus before it causes damage to your computer. By default, the client backs up the file.

In some instances, however, the cleaned file might not be usable. The virus might have caused too much damage.

Some infected files cannot be cleaned.

Note: Symantec Endpoint Protection does not clean malware that is detected in Windows 8 style apps and files. Symantec Endpoint Protection deletes the detection instead.

Quarantine risk

Moves the infected file from its original location to the Quarantine. Infected files within the Quarantine cannot spread viruses.

For viruses, moves the infected file from its original location to the Quarantine. This setting is the default second action for viruses.

For security risks, the client moves the infected files from their original location to the Quarantine and tries to remove or repair any side effects. This setting is the default first action for security risks.

Quarantine contains a record of all the actions that were performed. You can return the computer to the state that existed before the client removed the risk.

Note: Symantec Endpoint Protection does not quarantine malware that is detected in Windows 8 style apps and files. Symantec Endpoint Protection deletes the detection instead.

Delete risk	Deletes the infected file from your computer’s hard drive. If the client cannot delete a file, information about the action that the client performed appears in the Notification dialog box. The information also appears in the Event Log. Use this action only if you can replace the file with a backup copy that is free of viruses or security risks. When the client deletes a risk, it deletes the risk permanently. The infected file cannot be recovered from the Recycle Bin. **Note:** Use this action with caution when you configure actions for security risks. In some cases, deleting security risks can cause applications to lose functionality.
Leave alone (log only)	Leaves the file as is. If you use this action for viruses, the virus remains in the infected files. The virus can spread to other parts of your computer. An entry is placed in the Risk History to keep a record of the infected file. You can use Leave alone (log only) as a second action for both malware and security risks. Do not select this action when you perform large-scale, automated scans, such as scheduled scans. You might want to use this action if you intend to view the scan results and take an additional action later. An additional action might be to move the file to the Quarantine. For security risks, this action leaves the infected file as is and places an entry in the Risk History to keep a record of the risk. Use this option to take manual control of how the client handles a security risk. This setting is the default second action for security risks. Your administrator might send a customized message that explains how to respond.

7. Repeat these steps for each category for which you want to set specific actions, and then click **OK**.
8. If you selected a security risk category, you can select custom actions for one or more specific instances of that security risk category. You can exclude a security risk from scanning. For example, you might want to exclude a piece of adware that you need to use in your work.
9. Click **OK**.

About excluding items from scans

Exceptions are known security risks, files, file extensions, and 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 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. Your administrator can also prevent you from configuring any or all types of exceptions.

Note: If your email application stores all email in a single file, you should create a file exception to exclude the Inbox file from scans. By default, scans quarantine viruses. If a scan detects a virus in the Inbox file, the scan quarantines the entire Inbox. If the scan quarantines the Inbox, you cannot access your email.

Table 4-9 Exception types

Exception Type	Description
File	Applies to virus and spyware scans Scans ignore the file that you select.
Folder	Applies to virus and spyware scans or SONAR or both Scans ignore the folder that you select.
Known risks	Applies to virus and spyware scans Scans ignore any known risk that you select.
Extensions	Applies to virus and spyware scans Scans ignore any files with the specified extensions.
Web domain	Applies to virus and spyware scans Download Insight ignores the specified trusted Web domain.
Application	Applies to virus and spyware scans and SONAR Scans ignore, log, quarantine, or terminate the application that you specify here.

Table 4-9 Exception types *(continued)*

Exception Type	Description
DNS or host file change	Applies to SONAR Scans ignore, log, or block an application or prompt the user when a specific application tries to change DNS settings or change a host file.

See "Excluding items from scans" on page 81.

Excluding items from scans

Exceptions are known security risks, files, folders, file extensions, Web domains, or applications that you want to exclude from scans. 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. You can also create exceptions for applications that try to make a DNS or host file change. Typically you do not need to create exceptions.

For 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.

SONAR does not support file exceptions. Use an application exception to exclude a file from SONAR.

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.

To exclude items from security risk scans

1. In the client, in the sidebar, click **Change Settings**.
2. Next to **Exceptions**, click **Configure Settings**.
3. In the **Exceptions** dialog box, under **User-defined Exceptions**, click **Add > Security Risk Exceptions**.
4. Select one of the following exception types:
   - **Known Risks**
   - **File**
   - **Folder**
   - **Extensions**

- **Web Domain**

5. Do one of the following actions:
   - For known risks, check the security risks that you want to exclude from scans.
     If you want to log an event when the security risk is detected and ignored, check **Log when the security risk is detected**.
   - For files or folders, select the file or folder that you want to exclude, or enter a file or folder name.
     Select the scan type (**All scans**, **Auto-Protect**, or **Scheduled and on-demand**) and then click **OK**.
   - For extensions, type the extension that you want to exclude.
     You can only include one extension name in the text box. If you type multiple extensions, the client treats the entry as a single extension name.
   - For domains, enter a Web site or IP address that you want to exclude from Download Insight and SONAR detection.
6. Click **OK**.

To exclude a folder from SONAR

1. In the client, in the sidebar, click **Change Settings**.
2. Next to **Exceptions**, click **Configure Settings**.
3. In the **Exceptions** dialog box, under **User-defined Exceptions**, click **Add > SONAR Exception > Folder**.
4. Select the folder that you want to exclude, check or uncheck **Include Subfolders**, and then click **OK**.
5. Click **Close**.

To change how all scans handle an application

1. In the client, in the sidebar, click **Change Settings**.
2. Next to **Exceptions**, click **Configure Settings**.
3. In the **Exceptions** dialog box, under **User-defined Exceptions**, click **Add > Application Exception**.
4. Select the filename of the application
5. In the **Action** drop-down box, select **Ignore**, **Log Only**, **Quarantine**, **Terminate**, or **Remove**.
6. Click **OK**.
7. Click **Close**.

See “Managing scans on your computer” on page 52.

See “About excluding items from scans” on page 80.

Managing quarantined files on your client computer

By default, Symantec Endpoint Protection tries to clean a virus from an infected file when it is detected. If the file cannot be cleaned, the scan places the file in the Quarantine on your computer. For security risks, scans move infected files to the Quarantine and repair any side effects of the security risk. Download Insight and SONAR might also quarantine files.

See “About quarantining files” on page 84.

Table 4-10 Managing quarantined files on your client computer

Task	Description
Restore a quarantined file to its original location	Occasionally, a clean file does not have a location to which to be returned. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. You must release the file and specify a location.
Manually quarantine an item	You can manually quarantine a file by adding it to the Quarantine or by selecting the file from the virus and spyware logs or SONAR logs. See “Quarantining a file from the Risk log or Scan log” on page 85.
Permanently delete files from the Quarantine	You can manually delete the files that you no longer need from the Quarantine. You can also set up a time period by which files are deleted automatically. **Note:** Your administrator may specify a maximum number of days that items are allowed to stay in the Quarantine. Items are automatically deleted from the Quarantine after that time limit.
Rescan files in the Quarantine after you receive new definitions	When you update definitions, files in the Quarantine might get scanned, cleaned, and restored automatically. For some files, the Repair Wizard appears. Follow the on-screen instructions to complete the rescan and repair. You can also rescan virus-infected files in the Quarantine manually.

Table 4-10 Managing quarantined files on your client computer *(continued)*

Task	Description
Export Quarantine information	You can export the contents of the Quarantine to either a comma-delimited (.csv) file or a Microsoft Access Database (.mdb) file.
Submit infected files in the Quarantine to Symantec Security Response	After items in the Quarantine are rescanned, you might want to submit a file that is still infected to Symantec Security Response for further analysis. See "Manually submitting a potentially infected file to Symantec Security Response for analysis" on page 85.
Clear backup items	Before trying to clean or repair items, the client makes backup copies of infected items by default. After the client successfully cleans a virus, you should manually delete the item from the Quarantine because the backup is still infected.
Automatically delete files from the Quarantine	You can set up the client to automatically remove items from the Quarantine after a specified time interval. You can also specify that the client removes items when the folder where the items are stored reaches a certain size. This configuration prevents the buildup of files that you may forget to remove manually from these areas. See "Automatically deleting files from the Quarantine" on page 86.

About quarantining files

When the client moves an infected file to the Quarantine, the virus or risk cannot 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.

Most 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 manually quarantine the file.

Note: The language of the operating system on which you run the client might not be able to interpret some characters in risk names. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some Unicode risk names might contain double-byte characters. On those computers that run the client on an English operating system, these characters appear as question marks.

See "Managing quarantined files on your client computer" on page 83.

Quarantining a file from the Risk log or Scan log

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

See "About quarantining files" on page 84.

See "Managing quarantined files on your client computer" on page 83.

To quarantine a file from the Risk log or Scan log

1. In the client, click **View Logs**.
2. Beside **Virus and Spyware Protection**, click **View Log** and then select **Risk Log** or **Scan Log**.
3. Select the file that you want to quarantine, and then click **Quarantine**.
4. Click **OK**, and then click **Close**.

Manually submitting a potentially infected file to Symantec Security Response for analysis

When you submit an infected item from your quarantine list to Symantec Security Response. Symantec Security Response can analyze this item to make sure that it is not infected. Symantec Security Response also uses this data to protect against new or developing threats.

Note: The submission option is not available if your administrator disables these types of submissions.

See "Managing quarantined files on your client computer" on page 83.

To submit a file to Symantec Security Response from the Quarantine

1. In the client, in the sidebar, click **View Quarantine**.
2. Select the file in the list of quarantined items.
3. Click **Submit**.
4. Follow the on-screen instructions in the wizard to collect the necessary information and submit the file for analysis.

Automatically deleting files from the Quarantine

You can set up your software to automatically remove items from the Quarantine list after a specified time interval. You can also specify that the client removes items when the folder where the items are stored reaches a certain size. This configuration prevents the buildup of files that you may forget to remove manually from these areas.

See "Managing quarantined files on your client computer" on page 83.

To automatically delete files from the Quarantine

1. In the client, in the sidebar, click **View Quarantine**.
2. Click **Purge Options**.
3. In the **Purge Options** dialog box, select one of the following tabs:
   - **Quarantine Items**
   - **Backup Items**
   - **Repaired Items**
4. Check or uncheck **Length of time stored exceeds** to enable or disable the ability of the client to delete the files after the configured time expires.
5. If you check the **Length of time stored exceeds** check box, type or click an arrow to enter the amount of time.
6. Select the unit of time from the drop-down list. The default is 30 days.
7. If you check the **Total folder size exceeds** check box, type in the maximum folder size to allow, in megabytes. The default is 50 megabytes.

   If you check both check boxes, all files that are older than the time that you have set are deleted first. If the size of the folder still exceeds the limit that you set, the client deletes the oldest files individually. The client deletes the oldest files until the folder size does not exceed the limit.
8. Repeat steps 4 through 7 for any of the other tabs.
9. Click **OK**.

Enabling or disabling early launch anti-malware (ELAM)

Early launch anti-malware (ELAM) provides protection for your computer when it starts up and before third-party drivers initialize. Malicious software that can load as a driver or rootkits might attack before the operating system completely loads and Symantec Endpoint Protection starts. Rootkits can sometimes hide themselves from virus and spyware scans. Early launch anti-malware detects these rootkits and bad drivers at startup.

Symantec Endpoint Protection provides an early launch anti-malware driver that works with the Microsoft early launch anti-malware driver to provide the protection. The settings are supported on Microsoft Windows 8.

Note: You cannot create exceptions for individual ELAM detections; however, you can create a global exception to log all bad drivers as unknown.

For some ELAM detections that require remediation, you might be required to run Power Eraser. Power Eraser is part of the Symantec Endpoint Protection support tool.

To enable or disable early launch anti-malware

1. In the client, in the sidebar, click **Change Settings**.
2. Next to **Virus and Spyware Protection**, click **Configure Settings**.
3. On the **Early Launch Anti-Malware** tab, check or uncheck **Enable Symantec Early Launch Anti-Malware**.

   The Windows early launch anti-malware driver must be enabled for this option to take effect.
4. If you want to log the detections only, under **When Symantec Endpoint Protection detects a potentially malicious driver**, select **Log the detection as unknown so that Windows allows the driver to load**.
5. Click **OK**.

See “Managing scans on your computer” on page 52.

See “Troubleshooting computer issues with the Symantec Help support tool” on page 24.

See “Excluding items from scans” on page 81.

How to manage the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers

By default pop-up notifications appear on the Windows 8 style user interface and the Windows 8 desktop for malware detections and other critical Symantec Endpoint Protection events.

You can perform the following actions to manage the pop-up notifications:

- In the client, modify the global setting for Windows 8 style user interface notifications on the **Client Management Settings** page.
- In Windows 8, change the notification settings for the operating system.
  Symantec Endpoint Protection notifications only appear if Windows 8 is configured to show them. See the Windows 8 user documentation for more information.

On managed clients, your administrator might control whether or not you see pop-up notifications in Windows 8.

See "Responding to the Symantec Endpoint Protection pop-up notifications that appear on Windows 8 computers" on page 32.

About submitting information about detections to Symantec Security Response

You can configure your computer to automatically submit information about detections to Symantec Security Response for analysis.

Symantec Response and the Global Intelligence Network use this submitted information to quickly formulate responses to new and developing security threats. The data that you submit improves Symantec's ability to respond to threats and customize protection. Symantec recommends that you always allow submissions.

See "About the Symantec Endpoint Protection client" on page 11.

You can choose to submit any of the following types of data:

- File reputation
  Information about the files that are detected based on their reputation. The information about these files contributes to the Symantec Insight reputation database to help protect your computers from new and emerging risks.
- Antivirus detections
  Information about virus and spyware scan detections.

- Antivirus advanced heuristic detections

  Information about potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.

  These detections are silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.
- SONAR detections

  Information about threats that SONAR detects, which include high or low risk detections, system change events, and suspicious behavior from trusted applications.
- SONAR heuristics

  SONAR heuristic detections are silent detections that do not appear in the Risk log. This information is used for statistical analysis.

You can also manually submit a sample to Response from the Quarantine or through the Symantec Web site. To submit a file through the Symantec Web site, contact Symantec Technical Support.

See “Submitting information about detections to Symantec Security Response” on page 89.

See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 64.

Submitting information about detections to Symantec Security Response

Symantec Endpoint Protection can protect computers by monitoring the information that comes into and out of the computer, and by blocking attack attempts.

You can enable your computer to submit information about detected threats to Symantec Security Response. Symantec Security Response uses this information to protect your client computers from new, targeted, and mutating threats. Any data you submit improves Symantec's ability to respond to threats and customize protection for your computer. Symantec recommends that you submit as much detection information as possible.

You can also manually submit a sample to Symantec Response from the Quarantine page. The Quarantine page also lets you determine how items are submitted to Symantec Security Response.

To configure submissions to Symantec Security Response

1. Select **Change Settings** > **Client Management**.
2. On the **Submissions** tab, check **Let this computer automatically forward selected anonymous security information to Symantec**. This option lets Symantec Endpoint Protection submit information about the threats that are found on your computer.

   Symantec recommends that you keep this option enabled.
3. Select the types of information to submit.

   Click **Help** for more information about these options.
4. Enable **Allow Insight lookups for threat detection** to allow Symantec Endpoint Protection to use Symantec's reputation database to make decisions about threats.
5. Click **OK**.

See “Managing quarantined files on your client computer” on page 83.

See “About submitting information about detections to Symantec Security Response” on page 88.

About the client and the Windows Security Center

If you use Windows Security Center (WSC) on Windows XP with Service Pack 2 or Service Pack 3, you can see Symantec Endpoint Protection status in WSC.

Table 4-11 shows the protection status reporting in WSC.

Table 4-11 WSC protection status reporting

Symantec product condition	Protection status
Symantec Endpoint Protection is not installed	NOT FOUND (red)
Symantec Endpoint Protection is installed with full protection	ON (green)
Symantec Endpoint Protection is installed, and virus and security risk definitions are out of date	OUT OF DATE (red)
Symantec Endpoint Protection is installed and Auto-Protect for the file system is not enabled	OFF (red)
Symantec Endpoint Protection is installed, Auto-Protect for the file system is not enabled, and virus and security risk definitions are out of date	OFF (red)

Table 4-11 WSC protection status reporting *(continued)*

Symantec product condition	Protection status
Symantec Endpoint Protection is installed and ccSvcHst is turned off manually	OFF (red)

Table 4-12 shows the Symantec Endpoint Protection firewall status reporting in WSC.

Table 4-12 WSC firewall status reporting

Symantec product condition	Firewall status
Symantec firewall is not installed	NOT FOUND (red)
Symantec firewall is installed and enabled	ON (green)
Symantec firewall is installed but not enabled	OFF (red)
Symantec firewall is not installed or enabled, but a third-party firewall is installed and enabled	ON (green)

Note: In Symantec Endpoint Protection, the Windows Firewall is disabled by default.

If there is more than one firewall enabled, WSC reports that multiple firewalls are installed and enabled.

About SONAR

SONAR is a real-time protection that detects potentially malicious applications when they run on your computers. SONAR provides "zero-day" protection because it detects threats before traditional virus and spyware detection definitions have been created to address the threats.

SONAR uses heuristics as well as reputation data to detect emerging and unknown threats. SONAR provides an additional level of protection on your client computers and complements your existing Virus and Spyware Protection, intrusion prevention, and firewall protection.

SONAR uses a heuristics system that leverages Symantec's online intelligence network with proactive local monitoring on your computer to detect emerging threats. SONAR also detects changes or behavior on your computer that you should monitor.

Note: Auto-Protect also uses a type of heuristic that is called Bloodhound to detect suspicious behavior in files.

SONAR might inject some code into the applications that run in Windows user mode to monitor them for suspicious activity. In some cases, the injection might affect the application performance or cause problems with running the application. You can create an exception to exclude the file, folder, or application from this type of monitoring.

Note: SONAR does not inject code into applications on Symantec Endpoint Protection 12.1 or earlier clients. If you use Symantec Endpoint Protection Manager 12.1.2 to manage clients, a SONAR file exception in an Exceptions policy is ignored on your legacy clients. If you use a legacy Symantec Endpoint Protection Manager to manage clients, the legacy policy does not support SONAR file exceptions for your Symantec Endpoint Protection 12.1.2 clients. You can prevent SONAR code injection into applications on these clients, however, by creating an **Application to monitor** exception in the legacy policy. After the client learns the application, you can configure an application exception in the policy.

SONAR does not make detections on application type, but on how a process behaves. SONAR acts on an application only if that application behaves maliciously, regardless of its type. For example, if a Trojan horse or keylogger does not act maliciously, SONAR does not detect it.

SONAR detects the following items:

Heuristic threats	SONAR uses heuristics to determine if an unknown file behaves suspiciously and might be a high risk or low risk. It also uses reputation data to determine whether the threat is a high risk or low risk.
System changes	SONAR detects applications or the files that try to modify DNS settings or a host file on a client computer.
Trusted applications that exhibit bad behavior	Some good trusted files might be associated with suspicious behavior. SONAR detects these files as suspicious behavior events. For example, a well-known document sharing application might create executable files.

If you disable Auto-Protect, you limit SONAR's ability to make detections of high and low risk files. If you disable Insight lookups (reputation queries), you also limit the SONAR's detection capability.

See “Managing SONAR on your client computer” on page 93.

See “Excluding items from scans” on page 81.

Managing SONAR on your client computer

You manage SONAR as part of Proactive Threat Protection. On managed clients, your administrator might lock some of the settings.

Table 4-13 Managing SONAR on your client computer

Task	Description
Make sure that SONAR is enabled	For the best protection on your client computer, SONAR should be enabled. SONAR is enabled by default. You enable SONAR by enabling Proactive Threat Protection. See “About enabling and disabling protection when you need to troubleshoot problems” on page 44.
Make sure that Insight lookups are enabled	SONAR uses reputation data in addition to heuristics to make detections. If you disable Insight lookups (reputation queries), SONAR makes detections by using heuristics only. The rate of false positives might increase, and the protection that SONAR provides is limited. See “Submitting information about detections to Symantec Security Response” on page 89.
Change SONAR settings	You can enable or disable SONAR. You can also change the detection action for some types of threats that SONAR detects. You might want to change the detection action to reduce false positive detections. See “Changing SONAR settings” on page 94.
Create exceptions for applications that you know are safe	SONAR might detect the files or the applications that you want to run on your computer. You can create SONAR exceptions for the files, folders, or applications on the **Exceptions > Change Settings** page. You can also create an exception from the Quarantine. See “Excluding items from scans” on page 81.

Table 4-13 Managing SONAR on your client computer *(continued)*

Task	Description
Prevent SONAR from examining some applications	In some cases an application might become unstable or cannot run when SONAR injects code into the application to examine it. You can create a file or application exception for the application. See "Excluding items from scans" on page 81.
Submit information about SONAR detections to Symantec Security Response	Symantec recommends that you send information about detections to Symantec Security Response. The information helps Symantec address threats. Submissions are enabled by default. See "Submitting information about detections to Symantec Security Response" on page 89.

See "Managing scans on your computer" on page 52.

See "About the types of scans" on page 60.

Changing SONAR settings

You might want to change SONAR actions to reduce the rate of false positive detections. You can also change notifications for SONAR heuristic detections.

Note: On managed clients, your administrator might lock these settings.

To change SONAR settings

1 In the client, in the sidebar, click **Change settings**.

2 Next to **Proactive Threat Protection**, click **Configure Settings**

3 On the **SONAR** tab, change the actions for high risk or low risk heuristic threats.

   You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.

4 Optionally, change the notification settings.

5 On the **Suspicious Behavior Detection** tab, change the action for high risk or low risk detections. SONAR makes these detections when trusted files are associated with suspicious behavior.

6 On the **System Change Events** tab, change the scan action for detections of changes to the DNS server settings or a host file.

7 Click **OK**.

See “Managing SONAR on your client computer” on page 93.

Chapter 5

Managing the firewall and intrusion prevention

This chapter includes the following topics:

Managing firewall protection

By default, the Symantec Endpoint Protection client provides an appropriate level of firewall protection that your computer needs.

However, your administrator may have changed some of the default firewall rules and settings. If your administrator has given you the ability to modify your firewall protection, you can modify the firewall rules or firewall settings

Table 5-1 describes the firewall tasks you can perform to protect your computer. All of these tasks are optional and can be performed in any order.

Table 5-1 Managing firewall protection

Task	Description
Read about how the firewall works	Learn how the firewall protects your computer from network attacks. See "How a firewall works" on page 99.
Add and customize firewall rules	You can add new firewall rules or edit existing firewall rules. 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 "Managing firewall rules" on page 100. You can also configure a firewall rule to allow applications to access the network or prevent the applications from accessing the network. See "Creating a firewall rule for an application when it accesses the network from your computer" on page 112.
Configure firewall settings	In addition to creating firewall rules, you can also enable and configure firewall settings to further enhance your firewall protection. See "Enabling or disabling firewall settings" on page 107.
View firewall logs	You can regularly check the firewall protection status on your computer to determine the following: ■ The firewall rules that you created work correctly. ■ The client blocked any network attacks. ■ The client blocked any applications that you expected to run. You can use the Traffic Log and the Packet Log to check the firewall protection status. By default, the Packet log is disabled on managed clients. See "About the logs" on page 41. See "Enabling the Packet Log" on page 44.

Table 5-1 Managing firewall protection *(continued)*

Task	Description
Allow or blocking applications and certain types of traffic	For extra security, you can block network traffic from accessing your computer in the following situations. ■ You can block traffic when your computer's screensaver is on. ■ You can block traffic when the firewall does not run. ■ You can block all traffic at any time. See "Configuring the client to block traffic when the screensaver is active or the firewall does not run" on page 113. ■ You can allow, block, or display a message to allow or block an application from accessing the network. These applications already run on your computer. See "Allowing or blocking applications from accessing the network" on page 111. See "Creating a firewall rule for an application when it accesses the network from your computer" on page 112.
Enable or disable the firewall	You can disable Network Threat Protection temporarily for troubleshooting purposes. For example, you might need to disable it so that you can open a certain application. See "Enabling or disabling protection on the client computer" on page 46.

How a firewall works

A firewall does all of the following tasks:

- Prevents any unauthorized users from accessing the computers and networks in your organization that connect to the Internet
- Monitors the communication between your computers and other computers on the Internet
- Creates a shield that allows or blocks attempts to access the information on your computer
- Warns you of connection attempts from other computers
- Warns you of connection attempts by the applications on your computer that connect to other computers

The firewall reviews the packets of data that travel across the Internet. 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.

Packets contain information about the following:

- Sending computers
- Intended recipients

- How the packet data is processed
- Ports that receive the packets

Ports are the channels that divide the stream of data that comes from the Internet. 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.

See "Managing firewall protection" on page 97.

Managing firewall rules

Firewall rules control how the firewall protects computers from malicious incoming traffic and applications. The firewall checks all incoming packets and outgoing packets against the rules that you enable. It allows or blocks the packets based on the conditions that you specify in the firewall rule.

The Symantec Endpoint Protection client includes default firewall rules to protect your computer. However, you can modify the firewall rules for additional protection if your administrator permits it, or if your client is unmanaged.

Table 5-2 describes what you need to know to manage firewall rules.

Table 5-2 Managing firewall rules

Subject	Description
Learn how firewall rules work and what makes up a firewall rule	Before you modify the firewall rules, you should understand the following information about how firewall rules work. ■ How to order rules to ensure that the most restrictive rules are evaluated first and the most general rules are evaluated last. See "About the firewall rule, firewall setting, and intrusion prevention processing order" on page 103. ■ That the client uses stateful inspection, which eliminates the need for you to create additional rules. See "How the firewall uses stateful inspection" on page 104. ■ The firewall components that make up the firewall rule. See "The elements of a firewall rule" on page 101.

Table 5-2 Managing firewall rules *(continued)*

Subject	Description
Add a new firewall rule	You can perform the following tasks to manage firewall rules: ■ Symantec Endpoint Protection installs with default firewall rules, but you can add your own rules. See "Adding a firewall rule" on page 105. ■ You can customize a default rule or one that you created by changing any of the firewall rule criteria. ■ Export and import firewall rules Another way that you can add a firewall rule is to export existing firewall rules from another Firewall policy. You can then import the firewall rules and settings so that you do not have to re-create them. See "Exporting and importing firewall rules" on page 106. ■ Copy and paste firewall rules
Enable or disable a firewall rule	Firewall rules are automatically enabled. However, you may need to temporarily disable a firewall rule to test the rule. The firewall does not inspect disabled rules. See "Enabling and disabling firewall rules" on page 106.

The elements of a firewall rule

Firewall rules control how the client protects your computer 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 traffic 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.

As soon as a firewall rule is triggered, no other firewall rules are evaluated. If no rule is triggered, the packet is automatically blocked and the event is not logged.

A firewall rule describes the conditions in which a network connection may be allowed or blocked. For example, a rule may allow network traffic between remote port 80 and the IP address 192.58.74.0, between 9 A.M. and 5 P.M. daily.

Table 5-3 describes the criteria that you use to define a firewall rule.

Table 5-3 Firewall rule conditions

Condition	Description
Triggers	The firewall rule triggers are as follows: ■ Applications When the application is the only trigger that you define in an allow traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and define no other triggers. 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 particular network protocols and hosts with which communication is allowed. ■ Hosts The local host is always the local client computer and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. When you define host triggers, you specify the host on the remote side of the described network connection. ■ Protocols A protocol trigger identifies one or more network protocols that are significant in relation to the described traffic. The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic. ■ Network adapters If you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter. You can specify either any adapter or the one that is currently associated with the client computer. You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address. When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall does not apply the rule.
Conditions	Schedule and screen saver state. The conditional parameters do not describe an aspect of a network connection. Instead, the conditional parameters determine the active state of a rule. The conditional parameters are optional and if not defined, not significant. You may set up a schedule or identify a screen saver state that dictates when a rule is considered to be active or inactive. The firewall does not evaluate the inactive rules when the firewall receives packets.

Table 5-3 Firewall rule conditions *(continued)*

Condition	Description
Actions	Allow or block, and log or do not log. The action parameters specify what actions the firewall takes when it successfully matches a rule. If the rule is selected in response to a received packet, the firewall performs all actions. The firewall either allows or blocks the packet and logs or does not log the packet. If the firewall allows traffic, it lets the traffic that the rule specifies access your network. If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access your network.

See "How the firewall uses stateful inspection" on page 104.

See "Adding a firewall rule" on page 105.

See "Managing firewall rules" on page 100.

About the firewall rule, firewall setting, and intrusion prevention processing order

Firewall rules are ordered sequentially, from highest to lowest priority 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:

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

Table 5-4 shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

Table 5-4 Processing order

Priority	Setting
First	Custom IPS signatures
Second	Intrusion Prevention settings, traffic settings, and stealth settings
Third	Built-in rules
Fourth	Firewall rules
Fifth	Port scan checks
Sixth	IPS signatures that are downloaded through LiveUpdate

See “Changing the order of firewall rules” on page 105.

See “How a firewall works” on page 99.

See “How intrusion prevention works” on page 115.

How the firewall uses stateful inspection

Firewall protection uses stateful inspection to track current connections. Stateful inspection tracks source and destination IP addresses, ports, applications, and other connection information. Before the client inspects the firewall rules, it makes the traffic flow decisions that are based on the connection information.

For example, if a firewall rule allows a computer to connect to a Web server, the firewall logs the connection information. When the server replies, the firewall discovers that a response from the Web server to the computer is expected. It permits the Web server traffic to flow to the initiating computer without inspecting the rule base. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection eliminates the need to create new rules. For the traffic that is initiated in one direction, you do not have to create the rules that permit the traffic in both directions. The client traffic that is initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). The client computers initiate this outbound traffic; you create a rule that permits the outbound traffic for these protocols. Stateful inspection automatically permits the return traffic that responds to the outbound traffic. Because the firewall is stateful in nature, you only need to create the rules that initiate a connection, not the characteristics of a particular packet. All packets that belong to an allowed connection are implicitly allowed as being an integral part of that same connection.

Stateful inspection supports all rules that direct TCP traffic.

Stateful inspection does not support the rules that filter ICMP traffic. For ICMP traffic, you must create the rules that permit the traffic in both directions. For example, for the clients to use the ping command and receive replies, you must create a rule that permits ICMP traffic in both directions.

See "How a firewall works" on page 99.

See "Managing firewall rules" on page 100.

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.

Firewall rules are automatically enabled when you create them.

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, click on each tab and configure it as needed.
6. To define the time period when the rule is active or inactive, on the **Scheduling** tab, click **Enable Scheduling**, and then set up a schedule.
7. When you finish making changes, click **OK**.
8. Click **OK**.

See "The elements of a firewall rule" on page 101.

See "Enabling and disabling firewall rules" on page 106.

Changing the order of firewall rules

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 order, it affects the order for the currently selected location only.

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

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**.

See “About the firewall rule, firewall setting, and intrusion prevention processing order” on page 103.

Enabling and disabling firewall rules

You must enable rules so that the firewall can process them. When you add firewall rules, they are automatically enabled.

You can disable a firewall rule if you need to allow specific access to a computer or application.

To enable and disable firewall rules

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, in the **Rule Name** column, check or uncheck the check box beside the rule that you want to enable or disable.
4. Click **OK**.

See “Adding a firewall rule” on page 105.

Exporting and importing firewall rules

You can share the rules with another client so that you do not have to recreate them. You can export the rules from another computer and import them into your computer. When you import rules, they are added to the bottom of the firewall rules list. Imported rules do not overwrite existing rules, even if an imported rule is identical to an existing rule.

The exported rules and imported rules are saved in a .sar file.

To export firewall rules

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 rules you want to export.
4. Right-click the rules, and then click **Export Selected Rules**.
5. In the **Export** dialog box, type a file name, and then click **Save**.
6. Click **OK**.

To import firewall rules

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, right-click the firewall rules list, and then click **Import Rule**.
4. In the **Import** dialog box, locate the .sar file that contains the rules you want to import.
5. Click **Open**.
6. Click **OK**.

See “Adding a firewall rule” on page 105.

Enabling or disabling firewall settings

You can enable the client's firewall settings to protect your computer against certain types of network attacks. Some of the settings replace the firewall rules that you would otherwise need to add.

Note: Your administrator may not have made some of these settings available for you to configure.

Table 5-5 describes the types of firewall settings that you can configure to further customize your firewall protection.

Table 5-5 Firewall settings

Category	Description
Built-in rules for essential network services	Symantec Endpoint Protection provides the built-in rules that allow for the normal exchange of certain essential network services. Built-in rules eliminate the need to create the firewall rules that explicitly allow those services. During processing, these built-in rules are evaluated before firewall rules so that the packets that match an active occurrence of a built-in rule are allowed. You can define built-in rules for DHCP, DNS, and WINS services.
Traffic and stealth Web browsing	You can enable various traffic settings and stealth Web browsing settings to protect against certain types of network attacks on the client. You can enable traffic settings to detect and block the traffic that communicates through drivers, NetBIOS, and token rings. You can configure settings to detect the traffic that uses more invisible attacks. You can also control the behavior for the IP traffic that does not match any firewall rules.
Network file and print sharing	You can enable the client to either share its files or to browse for shared files and printers on your local network. To prevent network-based attacks, you can disable network file and printer sharing. See "Enabling network file and printer sharing" on page 108.
Block an attacking computer	When the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client then automatically blocks all communication to and from the IP address of the attacking computer for a period of time. The IP address of the attacking computer is blocked for a single location.

To enable or disable firewall settings

1. In the client, click **Change Settings**.
2. Beside **Network Threat Protection**, click **Configure Settings**.
3. On the **Firewall** tab, check the settings that you want to enable.

   Click **Help** for more information on the settings.
4. Click **OK**.

See "Managing firewall rules" on page 100.

Enabling network file and printer sharing

You can enable the client to either share its files or to browse for shared files and printers on your local network. To prevent network-based attacks, you can disable network file and printer sharing.

Table 5-6 Ways to enable network file and print sharing

Task	Description
Automatically enable the network file and printer sharing settings on the **Microsoft Windows Networking** tab.	If a firewall rule blocks this traffic, the firewall rule takes priority over the settings. To automatically enable network file and print sharing
Manually enable network file and printer sharing by adding firewall rules.	You can add the firewall rules if you want more flexibility than what the settings provide. For example, when you create a rule, you can specify a particular host rather than all hosts. The firewall rules allow access to the ports to browse and share files and printers. You can create one set of firewall rules so that the client can share its files. You create a second set of firewall rules so that the client can browse for other files and printers. To manually enable clients to browse for files and printers To manually enable other computers to browse files on the client

To automatically enable network file and print sharing

1 In the client, in the sidebar, click **Change settings**.

2 Beside **Network Threat Protection**, click **Configure Settings**.

3 On the **Microsoft Windows Networking** tab under **Settings**, click the drop-down menu and select the adapter for which these settings apply.

4 To browse other computers and printers in the network, click **Browse files and printers on the network**.

5 To enable other computers to browse files on your computer, click **Share my files and printers with others on the network**.

6 Click **OK**.

To manually enable clients to browse for files and printers

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 click **Allow this traffic**.

5 On the **Ports and Protocols** tab, in the **Protocol** drop-down list, click **TCP**.

6 In the **Remote ports** drop-down list, type:

88, 135, 139, 445

7 Click **OK**.

8 In the **Configure Firewall Rules** dialog box, click **Add**.

9 On the **General** tab, type a name for the rule and click **Allow this traffic**.

10 On the **Ports and Protocols** tab, in the **Protocol** drop-down list, click **UDP**.

11 In the **Remote ports** drop-down list, type:

88

12 In the **Local ports** drop-down list, type:

137, 138

13 Click **OK**.

To manually enable other computers to browse files on the client

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 click **Allow this traffic**.

5 On the **Ports and Protocols** tab, in the **Protocol** drop-down list, click **TCP**.

6 In the **Local ports** drop-down list, type:

88, 135, 139, 445

7 Click **OK**.

8 In the **Configure Firewall Rules** dialog box, click **Add**.

9 On the **General** tab, type a name for the rule and click **Allow this traffic**.

10 On the **Ports and Protocols** tab, in the **Protocol** drop-down list, click **UDP**.

11 In the **Local ports** drop-down list, type:

88, 137, 138

12 Click **OK**.

See “Enabling or disabling firewall settings” on page 107.

Allowing or blocking applications from accessing the network

You can specify the action that the client takes on an application when it tries to access the network from your computer or tries to access your computer. For example, you can block Internet Explorer from accessing any Web sites from your computer.

Table 5-7 describes the actions that the client takes on network traffic.

Table 5-7 Actions that the firewall takes when applications access the client or network

Action	Description
Allow	Allows the inbound traffic to access the client computer and the outbound traffic to access the network. If the client receives traffic, the icon displays a small blue dot in the lower left-hand corner. If the client sends traffic, the icon displays the dot in the lower right-hand corner.
Block	Blocks the inbound traffic and the outbound traffic from accessing the network or an Internet connection.
Ask	Asks you whether you want the application to access the network the next time you attempt to run the application.
Terminate	Stops the process.

To allow or block an application from accessing the network

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options > View Network Activity**.
3. In the **Network Activity** dialog box, right-click the application or service, and then click the action that you want the client to take on that application.
4. Click **Close**.

   If you click **Allow**, **Block**, or **Ask**, you can create a firewall rule for that application only.

   See “Creating a firewall rule for an application when it accesses the network from your computer” on page 112.

Creating a firewall rule for an application when it accesses the network from your computer

You can create a firewall rule that specifies whether an application that runs on your computer may access the network. The client can allow or block the application, or ask you first whether to allow or block the application. For example, you can configure the client to block any Web site from appearing in your Web browser.

You can also specify the conditions for when and how the application is allowed or blocked. For example, you can specify that a video game can access the network only during specific hours. These rules are called application-based firewall rules.

Note: If there is a conflict between a firewall rule and an application-based firewall rule, the firewall rule takes precedence. For example, a firewall rule that blocks all traffic between 1:00 A.M. and 8:00 A.M. overrides an application-rule that allows iexplore.exe to run at all times.

The applications that appear in the **Network Activity** dialog box are the applications and the services that have run since the client service started.

See "Allowing or blocking applications from accessing the network" on page 111.

To create a firewall rule for an application when it accesses the network from your computer

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options > View Application Settings**.
3. Optionally, in the **View Application Settings** dialog box, you can change the action by right-clicking the application and clicking **Allow**, **Ask**, or **Block**.
4. Click **Configure**.
5. In the **Configure Application Settings** dialog box, configure the restrictions for this application.

   For more information, either mouse over the text field and option, or click **Help**.

   If the action is set to **Allow** in step 3, any settings that you configure are restrictions to the rule. If you clicked **Block**, the settings that you configure are exceptions to the rule.

6 Click **OK**.

You can remove the conditions that you put on the application by clicking **Remove** or **Remove All**. When you remove the restrictions, the action that the client takes on the application is also erased. When the application or the service tries to connect to the network again, you may be asked again whether to allow or block the application.

7 Click **OK**.

See “Adding a firewall rule” on page 105.

Configuring the client to block traffic when the screensaver is active or the firewall does not run

You can configure your computer to block inbound traffic and outbound traffic in the following situations:

When your computer's screen saver is activated.	You can configure your computer to block all the inbound and the outbound network neighborhood traffic when your computer’s screen saver is activated. As soon as the screen saver turns off, your computer returns to the previously assigned security level. To block traffic when the screen saver is activated
When the firewall does not run.	The computer is unprotected after the computer starts and before the firewall service starts or after the firewall service stops and the computer turns off. This time frame is a security hole that can allow unauthorized communication. To block traffic when the firewall does not run
When you want to block all inbound traffic and outbound traffic at any time.	You may want to block all traffic when a particularly destructive virus attacks your company's network or subnet. You would not block all traffic under normal circumstances. **Note:** Your administrator may have configured this option to be unavailable. You cannot block all traffic on an unmanaged client. To block all traffic at any time

You can allow all traffic by disabling Network Threat Protection.

See “Enabling or disabling protection on the client computer” on page 46.

To block traffic when the screen saver is activated

1. In the client, in the sidebar, click **Change settings**.
2. Beside Network Threat Protection, click **Configure Settings**.
3. On the **Microsoft Windows Networking** tab under **Screen Saver Mode**, click **Block Microsoft Windows Networking traffic while the screen saver runs**.
4. Click **OK**.

To block traffic when the firewall does not run

1. In the client, in the sidebar, click **Change settings**.
2. Beside Network Threat Protection, click **Configure Settings**.
3. On the **Firewall** tab under **Traffic Settings**, click **Block all traffic until the firewall starts and after the firewall stops**.
4. Optionally click **Allow initial DHCP and NetBIOS traffic**.
5. Click **OK**.

To block all traffic at any time

1. In the client, in the sidebar click **Status**.
2. Beside **Network Threat Protection**, click **Options > View Network Activity**.
3. Click **Tools > Block All Traffic**.
4. To confirm, click **Yes**.
5. To return to the previous firewall settings that the client uses, uncheck **Tools > Block All Traffic**.

See "Enabling or disabling firewall settings" on page 107.

Managing intrusion prevention

You manage intrusion prevention as part of Network Threat Protection.

Table 5-8 Managing intrusion prevention

Action	Description
Learn about intrusion prevention	Learn how intrusion prevention detects and blocks network and browser attacks. See "How intrusion prevention works" on page 115.

Table 5-8 Managing intrusion prevention *(continued)*

Action	Description
Download the latest IPS signatures	By default, the latest signatures are downloaded to the client. However you might want to download the signatures manually immediately. See "Updating the computer's protection" on page 37.
Enable or disable network intrusion prevention or browser intrusion prevention	You might want to disable intrusion prevention for troubleshooting purposes or if client computers detect an excessive number of false positives. Typically, you should not disable intrusion prevention. You can enable or disable the following types of intrusion prevention: ■ Network intrusion prevention ■ Browser intrusion prevention See "Enabling or disabling intrusion prevention" on page 116. You can also enable or disable intrusion prevention when you enable or disable Network Threat Protection. See "About enabling and disabling protection when you need to troubleshoot problems" on page 44.
Configure intrusion prevention notifications	You can configure notifications to appear when Symantec Endpoint Protection detects an intrusion. See "Configuring intrusion prevention notifications" on page 117.

How intrusion prevention works

Intrusion prevention is part of Network Threat Protection.

Intrusion prevention automatically detects and blocks network attacks and attacks on browsers. Intrusion prevention is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Intrusion prevention intercepts data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. Intrusion prevention detects attacks on operating system components and the application layer.

Intrusion prevention provides two types of protection.

Table 5-9 Types of intrusion prevention

Type	Description
Network intrusion prevention	Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures. You cannot create custom signatures on the client. But you can import the custom signatures that you or your administrator created in Symantec Endpoint Protection Manager.
Browser intrusion prevention	Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers. Firefox might disable the Symantec Endpoint Protection plug-in, but you can re-enable it. This type of intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers. For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer. See the following knowledge base article for the latest information about the browsers that browser intrusion prevention protects: Supported browser versions for browser intrusion prevention.

See “Managing intrusion prevention” on page 114.

Enabling or disabling intrusion prevention

Typically, when you disable intrusion prevention on your computer, your computer is less secure. However, you might want to disable these settings to prevent false positives or to troubleshoot your computer.

Symantec Endpoint Protection logs intrusion attempts and events in the Security log. Symantec Endpoint Protection might also log intrusion events in the Packet log if your administrator configured it to do so.

See “Managing intrusion prevention” on page 114.

See "Viewing the logs" on page 43.

You can enable or disable two types of intrusion prevention:

- Network intrusion prevention
- Browser intrusion prevention

Note: You administrator may have configured these options to be unavailable.

See "About enabling and disabling protection when you need to troubleshoot problems" on page 44.

To enable or disable intrusion prevention settings

1. In the client, in the sidebar, click **Change settings**.
2. Beside **Network Threat Protection**, click **Configure Settings**.
3. On the **Intrusion Prevention** tab, check or uncheck either of the following settings:
   - **Enable Network Intrusion Prevention**
   - **Enable Browser Intrusion Prevention**

   For more information on the settings, click **Help**.
4. Click **OK**.

Configuring intrusion prevention notifications

You can configure notifications to appear when the client detects a network attack on your computer or when the client blocks an application from accessing your computer. You can set the length of time that these notifications appear and whether you hear a beep when the notification appears. You must enable the intrusion prevention system for the intrusion prevention notifications to appear.

If Intrusion Prevention is enabled on the computer, both Windows clients and Mac clients can trigger these notifications.

Note: Your administrator may have configured these options to be unavailable.

See "Managing intrusion prevention" on page 114.

To configure intrusion prevention notifications on a Windows client

1. In the client, in the sidebar, click **Change settings**.
2. Beside Network Threat Protection, click **Configure Settings**.

3 In the **Network Threat Protection Settings** dialog box, click **Notifications**.

4 Check **Display Intrusion Prevention notifications**.

5 To configure a beep to sound when the notification appears, check **Use sound when notifying users**.

6 Click **OK**.

To configure intrusion prevention notifications on a Mac client

1 On the Symantec QuickMenu, click **Symantec Endpoint Protection > Open Intrusion Prevention Preferences**.

2 Click the lock icon to make changes or to prevent further changes from being made.

You must provide your administrator name and password to lock or unlock Intrusion Prevention preferences.

3 Click **Display Intrusion Prevention notification**.

Click **Use sound when notifying users**, if desired.

Chapter 6

Managing Symantec Network Access Control

This chapter includes the following topics:

How Symantec Network Access Control works

The Symantec Network Access Control client validates and enforces policy compliance for the computers that try to connect to the network. This process begins before the computer connects to the network and continues throughout the duration of the connection. The Host Integrity policy is the security policy that serves as the basis for all evaluations and actions. Host Integrity is also referred to as "Security Compliance."

Table 6-1 describes the process that Network Access Control uses to enforce policy compliance on the client computer.

Table 6-1 How Symantec Network Access Control works

Action	Description
The client continuously evaluates its compliance	You turn on the client computer. The client runs a Host Integrity check that compares the computer's configuration with the Host Integrity policy that was downloaded from the management server. The Host Integrity check evaluates your computer for compliance with the Host Integrity policy for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check how recently its virus definitions have been updated, and which were the latest patches applied to the operating system. See "Running a Host Integrity check" on page 121.
A Symantec Enforcer authenticates the client computer and either grants the computer network access or blocks and quarantines non-compliant computers	If the computer meets all the policy's requirements, the Host Integrity check passes. The Enforcer grants full network access to computers that pass the Host Integrity check. If the computer does not meet the policy's requirements, the Host Integrity check fails. When a Host Integrity check fails, the client or a Symantec Enforcer blocks or quarantines your computer until you remediate your computer. Quarantined computers have limited or no access to the network. See "How the client works with an Enforcer" on page 121.
Your administrator may have set up the policy so that a Host Integrity check passes even if a specific requirement fails	The client may display a notification every time the Host Integrity check passes. See "Types of alerts and notifications" on page 25.
The client remediates non-compliant computers	If the Host Integrity check fails, the client installs or requests you to install the required software. After your computer is remediated, it tries to access the network again. If the computer is fully compliant, the network grants the computer network access. See "Remediating your computer" on page 122.
The client proactively monitors compliance	The client actively monitors the compliance state for all client computers. If at any time the computer's compliance status changes, so do the network access privileges of the computer.

You can view more information about the Host Integrity check results in the security log.

See "Viewing the logs" on page 43.

See "Viewing the Symantec Network Access Control logs" on page 126.

How the client works with an Enforcer

The client interacts with a Symantec Enforcer. The Enforcer ensures that all the computers that connect to the network that it protects run the client software and have a correct security policy.

See "How Symantec Network Access Control works" on page 119.

An Enforcer must authenticate the user or the client computer before it allows the client computer to access the network. Symantec Network Access Control works with several types of Enforcers to authenticate the client computer. The Symantec Enforcer is the network hardware appliance that verifies Host Integrity results and the client computer's identity before it allows that computer to have access to the network.

The Enforcer checks the following information before it allows a client to access the network:

- The version of the client software that the computer runs.
- The client has a unique identifier (UID).
- The client has been updated with the latest Host Integrity policy.
- The client computer passed the Host Integrity check.

See "Configuring the client for 802.1x authentication" on page 122.

Running a Host Integrity check

Your administrator configures the frequency that the client uses to run a Host Integrity check. You may need to run a Host Integrity check immediately rather than wait for the next check. For example, a failed Host Integrity check may find that you need to update the virus protection signatures on your computer. The client may let you choose whether to download the required software immediately or postpone the download. If you download the software immediately, you must run the Host Integrity check again to verify that you have the correct software. You can either wait until the next scheduled Host Integrity check runs or you can run the check immediately.

To run a Host Integrity check

1. In the client, in the sidebar, click **Status**.
2. Next to **Network Access Control**, click **Options > Check Compliance**.
3. Click **OK**.

   If you had been blocked from network access, you should regain network access when your computer has been updated to comply with the security policy.

See "How Symantec Network Access Control works" on page 119.

Remediating your computer

If the client finds that a Host Integrity policy requirement is not met, it responds in one of the following ways:

- The client downloads the software update automatically.
- The client prompts you to download the required software update.

To remediate your computer

◆ In the Symantec Endpoint Protection dialog box that appears, do one of the following actions:

  - To see which security requirements that your computer failed, click **Details**.
  - To immediately install the software, click **Restore Now**
    You may or may not have the option to cancel the installation after it has started.
  - To postpone the software install, click **Remind me later in** and select a time interval in the drop-down list.
    The administrator can configure the maximum number of times you can postpone the installation.

Configuring the client for 802.1x authentication

If your corporate network uses a LAN Enforcer for authentication, the client computer must be configured to perform 802.1x authentication. Either you or your administrator can configure the client. Your administrator may or may not have given you permission to configure 802.1x authentication.

The 802.1x authentication process includes the following steps:

- An unauthenticated client or third-party supplicant sends the user information and compliance information to a managed 802.1x network switch.
- The network switch relays the information to the LAN Enforcer. The LAN Enforcer sends the user information to the authentication server for authentication. The RADIUS server is the authentication server.
- If the client fails the user-level authentication or is not in compliance with the Host Integrity policy, the Enforcer may block network access. The Enforcer places the non-compliant client computer in a quarantine network where the computer can be remediated.
- After the client remediates the computer and brings it into compliance, the 802.1x protocol reauthenticates the computer and grants the computer access to the network.

To work with the LAN Enforcer, the client can use either a third-party supplicant or a built-in supplicant.

Table 6-2 describes the types of options you can configure for 802.1x authentication.

Table 6-2 802.1x authentication options

Option	Description
Third-party supplicant	Uses a third-party 802.1x supplicant. The LAN Enforcer works with a RADIUS server and third-party 802.1x supplicants to perform user authentication. The 802.1x supplicant prompts you for user information. The LAN Enforcer passes that user information to the RADIUS server for user-level authentication. The client sends the client profile and the Host Integrity status to the Enforcer so that the Enforcer authenticates the computer. **Note:** If you want to use the Symantec Network Access Control client with a third-party supplicant, then the Network Threat Protection module of the Symantec Endpoint Protection client must be installed.

Table 6-2 802.1x authentication options *(continued)*

Option	Description
Transparent mode	Uses the client to run as an 802.1x supplicant. You use this method if the administrator does not want to use a RADIUS server to perform user authentication. The LAN Enforcer runs in transparent mode and acts as a pseudo-RADIUS server. Transparent mode means that the supplicant does not prompt you for user information. In transparent mode, the client acts as the 802.1x supplicant. The client responds to the switch's EAP challenge with the client profile and the Host Integrity status. The switch, in turn, forwards the information to the LAN Enforcer, which acts as a pseudo-RADIUS server. The LAN Enforcer validates the Host Integrity and client profile information from the switch and can allow, block, or dynamically assign a VLAN, as appropriate. **Note:** To use a client as an 802.1x supplicant, you need to uninstall or disable third-party 802.1x supplicants from the client computer.
Built-in supplicant	Uses the client computer's built-in 802.1x supplicant. The built-in authentication protocols include Smart Card, PEAP, or TLS. After you enable 802.1x authentication, you must specify which authentication protocol to use.

Warning: Contact your administrator before you configure your client for 802.1x authentication. You must know whether your corporate network uses the RADIUS server as the authentication server. If you configure 802.1x authentication incorrectly, you may break your connection to the network.

To configure the client to use a third-party supplicant

1. In the client, in the sidebar, click **Status**.
2. Beside Network Access Control, click **Options > Change Settings > 802.1x Settings**.
3. In the **Network Access Control Settings** dialog box, click **Enable 802.1x authentication**.
4. Click **OK**.

   You must also set up a firewall rule that allows third-party 802.1x supplicant drivers onto the network.

   See "Adding a firewall rule" on page 105.

   You can configure the client to use the built-in supplicant. You enable the client for both 802.1x authentication and as an 802.1x supplicant.

To configure the client to use either transparent mode or a built-in supplicant

1. In the client, in the sidebar, click **Status**.
2. Beside Network Access Control, click **Options > Change Settings > 802.1x Settings**.
3. In the **Network Access Control Settings** dialog box, click **Enable 802.1x authentication**.
4. Click **Use client as an 802.1x supplicant**.
5. Do one of the following actions:
   - To select transparent mode, check **Use Symantec Transparent Mode**.
   - To configure a built-in supplicant, click **Allows you to choose the authentication protocol**.
     You then need to choose the authentication protocol for your network connection.
6. Click **OK**.

To choose an authentication protocol

1. On the client computer, click **Start > Settings > Network Connections** and then click **Local Area Connection**.

   Note: These steps are written for computers running Windows XP. Your procedure may vary.

2. In the **Local Area Connection Status** dialog box, click **Properties**.
3. In the **Local Area Connection Properties** dialog box, click the **Authentication** tab.
4. On the **Authentication** tab, click the **EAP type** drop-down list, and select one of the authentication protocols.

   Make sure that the **Enable IEEE 802.1x authentication for this network** check box is checked.
5. Click **OK**.
6. Click **Close**.

See “How Symantec Network Access Control works” on page 119.

Reauthenticating your computer

If your computer passed the Host Integrity check but the Enforcer blocks your computer, you may need to reauthenticate your computer. Under normal circumstances, you should never need to reauthenticate your computer.

The Enforcer may block the computer when one of the following events have occurred:

- The client computer failed the user authentication because you typed your user name or your password incorrectly.
- Your client computer is in the wrong VLAN.
- The client computer did not obtain a network connection. A broken network connection usually happens because the switch between the client computer and the LAN Enforcer did not authenticate your user name and password.
- You logged on to a client computer that authenticated a previous user.
- The client computer failed the compliance check.

You can reauthenticate the computer only if you or your administrator configured the computer with a built-in supplicant.

Note: Your administrator may not have configured the client to display the **Re-authentication** command.

To reauthenticate your computer

1. Right-click the notification area icon.
2. Click **Re-authentication...**.
3. In the **Re-authenticate** dialog box, type your user name and password.
4. Click **OK**.

See “How Symantec Network Access Control works” on page 119.

Viewing the Symantec Network Access Control logs

The Symantec Network Access Control client uses the following logs to monitor different aspects of its operation and the results of the Host Integrity check:

Security	Records the results and status of Host Integrity checks.
System	Records all operational changes for the client, such as the connection to the management server and updates to the client security policy.

If you use a managed client, both of the logs may be regularly uploaded to the server. Your administrator can use the content in the logs to analyze the overall security status of the network.

You can export the log data from these logs.

To view Symantec Network Access Control logs

1. In the client, in the sidebar, click **Status**.
2. To view the Security Log, next to **Network Access Control**, click **Options > View Logs**.
3. In the Security Log, select the top log entry.

   In the lower-left corner, the Host Integrity check results appear. If the client was already installed, the predefined firewall requirement passes. If the client was not installed, the predefined firewall requirement fails but is reported as having passed.
4. To view the System Log, in the **Security Log - Symantec Network Access Control Logs** dialog box, click **View > System Log**.
5. Click **File > Exit**.

   See "About the logs" on page 41.

Index