Symantec™ Endpoint Protection 14.2.1 Windows Client Guide

Symantec Endpoint Protection for Windows Client Guide

Product version 14.2.1 (14.2 RU1)

Documentation version: 1

This document was last updated on: April 23, 2019

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec Support

Knowledge Base articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com/

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect/

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

Before you contact Symantec Support, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Getting started on the Symantec Endpoint Protection client

This chapter includes the following topics:

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. Microsoft Outlook Auto-Protect scans incoming and outgoing Outlook email messages. For client versions earlier than 14.2 RU1, Internet Email Auto-Protect scans the incoming and outgoing email messages that use the POP3 or SMTP communications protocol. See "Managing scans on your computer" on page 30.
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 computer" on page 69.
Network and Host Exploit Mitigation	This protection includes a firewall, an intrusion prevention system, and Memory Exploit Mitigation. ■ The rules-based firewall prevents unauthorized users from accessing your computer. ■ The intrusion prevention system automatically detects and blocks network attacks. ■ Memory Exploit Mitigation stops attacks on the commonly used applications that run on your Windows computer. See "Managing firewall protection" on page 73. See "Configuring intrusion prevention" on page 89. See "Preventing attacks on vulnerable applications" on page 91.

Your administrator manages the types of protection that the management server downloads to your client computer. The client also downloads virus definitions, IPS definitions, and product updates to your computer. If you travel with a portable computer, you can get virus definitions and product updates directly from LiveUpdate.

See "Updating the client content using LiveUpdate" on page 17.

How do I protect my computer?

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

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 1-2 Frequently asked questions on how to protect your computer

Question	Description
How do I know that my computer is protected?	The Symantec Endpoint Protection client displays the protection status of your computer. Your computer is best protected with all protections installed and updated. See "How to determine whether the client computer is protected using the Status page icons" on page 14. See "Symantec Endpoint Protection client status icons" on page 13.
How can I tell if my computer is infected?	If your computer is infected, you might see any of the following types of messages: ■ An Auto-Protect scan 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. See "Responding to a virus or a risk detection" on page 22. See "About scan results" on page 21. See "Pausing and delaying scans" on page 16. ■ A Download Insight detection. These messages describe 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 24. See "Types of alerts and notifications" on page 19.
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 22. See "How virus and spyware scans work" on page 34. See "Configuring actions for malware and security risk detections" on page 56.

Table 1-2 Frequently asked questions on how to protect your computer *(continued)*

Question	Description
How do I increase the security of my computer?	By default, a managed client computer is protected with the maximum amount of protection. Your administrator may have modified some settings to improve the client's performance. If your administrator has enabled you to modify your own computer's protection 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 the client" on page 46. ■ Keep virus and spyware scans, Auto-Protect, SONAR, the firewall, intrusion prevention, Memory Exploit Mitigation, and Download Insight installed, enabled, and up-to-date at all times. See "Enabling protection on the client computer" on page 98. See "Enabling Auto-Protect" on page 63. See "Preventing attacks on vulnerable applications" on page 91. On an unmanaged client, you can perform the following tasks: ■ Download and install the correct virus definitions and security content by using LiveUpdate. Security Response releases virus definitions multiple times a day, and releases other security content regularly or as needed. By default, Symantec Endpoint Protection clients are scheduled to run LiveUpdate every four hours. You can also launch LiveUpdate at any time. See "Updating the client content using LiveUpdate" on page 17. ■ 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 the client" on page 46. See "Scanning your client computer immediately" on page 15.

Table 1-2 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: ■ Create a scheduled full scan for after hours or when you are not on the computer. See "Scheduling a user-defined scan on the client" on page 46. ■ Exclude the applications and files that you know are safe. See "Excluding items from scans" on page 60. ■ Turn off the scan of compressed files, or reduce the number of levels to expand compressed files within compressed files. See "Customizing virus and spyware scan settings" on page 54. ■ Disable the scan enhancement options for user-defined scans. See "Scheduling a user-defined scan on the client" on page 46. **Note:** You may not be able to change these settings if your administrator has locked them.
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 websites 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 website that the application accesses correct or legitimate? See "Adding firewall rules on the client" on page 80.

Table 1-2 Frequently asked questions on how to protect your computer *(continued)*

Question	Description
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. See "Responding to a virus or a risk detection" on page 22. See "Responding to messages that ask you to allow or block an application" on page 26. ■ Your computer automatically received a new security policy. You can also go to one of the logs for more information, depending on the type of threat. See "Viewing the logs" on page 102.

See "Checking whether the client is managed or unmanaged" on page 97.

See "Managing the client" on page 93.

Symantec Endpoint Protection client status icons

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 notification area icon is sometimes referred to as the system tray icon.

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 1-3 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 client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer.
	The client has a minor problem. For example, the virus definitions may be out of date.

Table 1-3 Client status icons *(continued)*

Icon	Description
	The client does not run, has a major problem, has an expired license, or has at least one protection technology disabled.

See "Hiding and displaying the notification area icon on the Symantec Endpoint Protection client" on page 98.

How to determine whether the client computer is protected using the Status page icons

When you open the Symantec Endpoint Protection client, the top of the Status page displays various alert icons to indicate the protection status of the computer. If there is further action you must take, the text that appears with the icons provides more information.

Table 1-4 Status page alert icons

Icon	Description
	Shows that each protection is enabled.
	Warns you that virus definitions or security content on the client computer is out of date. To receive the most current virus definitions or security content, you can run LiveUpdate immediately, if your administrator lets you. This status may also indicate Symantec Endpoint Protection requires a restart. A Symantec Endpoint Protection client computer with an active Host Integrity policy may also 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. ■ The client computer failed to download Host Integrity content. See "Updating the client content using LiveUpdate" on page 17.
	Shows that one or more protections are disabled or that the client has an expired license. To enable a protection, click **Fix** or **Fix All**. See "Enabling protection on the client computer" on page 98.

Scanning your client 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 USB drive 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.

You can scan your computer immediately in one of the following ways:

- To scan your Windows computer immediately from the Scan for Threats page
- To scan your Windows computer immediately from the Status page
- To scan your computer immediately from Windows

To scan your Windows computer immediately from the Scan for Threats page

- In the client, in the sidebar, click **Scan for threats**.
  - Click **Run Active Scan** to scan the most commonly infected areas.
  - Click **Run Full Scan** to scan the entire computer.
  - Click **Run Host Integrity Scan** to check for compliance with security policies.

    Note: Run Host Integrity Scan appears only if the client has a Host Integrity policy enabled.

  - In the scan list, right-click any scan, and then click **Scan Now**.

  The scan starts immediately.

  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**.

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

  You can also pause or cancel the scan.

To scan your Windows computer immediately from the Status page

- In the client, on the **Status** page next to **Virus and Spyware Protection**, click **Options > Run Active Scan**.

To scan your computer immediately 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.

See “About scan results” on page 21.

See “Pausing and delaying scans” on page 16.

See “Scheduling a scan to run on demand or when the computer starts up” on page 49.

See “Updating the client content using LiveUpdate” on page 17.

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 30.

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**.

Updating the client content using LiveUpdate

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.

Starting in 14, clients also have access to the full set of content in the cloud. Scans that run on a standard or embedded/VDI client that is connected to the cloud get the full definitions set in the cloud.

See "How Windows clients receive definitions from the cloud" on page 43.

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. These updates can come through the management server for managed clients if it is configured to do so.

LiveUpdate retrieves the new content files from a Symantec Internet site, and then replaces the old content files. A managed client computer most commonly receives content updates from its management server. A managed or an unmanaged client computer can receive this content directly from a LiveUpdate server. How your computer receives the updates depends on whether your computer is managed or unmanaged, and on how your administrator has configured updates.

Table 1-5 Ways to update content on your computer

Task	Description
Update the content on a schedule	By default, LiveUpdate runs automatically at scheduled intervals. You can also modify the 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. On managed clients, you can only configure LiveUpdate to run on a schedule or modify the existing schedule if enabled by the administrator. If the padlock icon appears and the options are grayed out, you cannot update your content on a schedule, or modify the existing schedule. On an unmanaged client, you can disable or change a LiveUpdate schedule. See "To update the content on a schedule with LiveUpdate" on page 18.

Table 1-5 Ways to update content on your computer *(continued)*

Task	Description
Update the content immediately	Based on your security settings, you can run LiveUpdate immediately. 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. **Note:** Managed clients can run LiveUpdate manually only if the administrator configured the settings to allow it. See "To update the content immediately with LiveUpdate" on page 18.

To update the content on a schedule with LiveUpdate

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, modify the frequency of the updates, as needed.
6. Optionally enable and configure the randomization options and idle detection settings.

   These options improve the amount of time it takes LiveUpdate to update the client.
7. Click **OK**.

To update the content immediately with LiveUpdate

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

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

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 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. If the scan is still in progress, the dialog box may display a name such as ***Scan name* started on *Date Time***. If the scan is complete, the dialog box may display a name such as **Symantec Endpoint Protection Detection Results**. See "About scan results" on page 21.
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 28. ■ 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 26. ■ The client's trial license has expired. See "Responding to expired license messages" on page 27.

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:
	`Traffic has been blocked from this application: Application name`
	If the client is configured to block all traffic, these notifications appear frequently and generally require no action on your part. 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 26.
	■ The client terminates an application:
	`Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected. Symantec Endpoint Protection will terminate <application name> application`
	See "Preventing attacks on vulnerable applications" on page 91.
	■ The client detects a network attack against your computer:
	`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.`
	You do not need to do anything else other than read the messages.
	■ The security compliance check failed. Traffic may be blocked from going to and from your computer:
	`Security compliance scan failed.`
	See "Remediating your computer to pass the Host Integrity check" on page 71.

See "Symantec Endpoint Protection client status icons" on page 13.

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 turn on your computer. By default, Auto-Protect runs continuously on your computer.

When a scan runs, 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 96.

See "Responding to a virus or a risk detection" on page 22.

See "Pausing and delaying scans" on page 16.

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 might need to take action on a risk but choose not to take action right now. You can use the Quarantine or the Risk Log or Scan Log to act on the file later 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 previously configured actions for the particular type of risk that the scan detected.

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 tries to remove or repair any side effects of the infection. 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 of the infection. 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.
  If a restart is required, the removal or repair is not complete until you restart the computer.
- **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**.

See "How scans respond to a virus or risk detection" on page 41.

See "Viewing the logs" on page 102.

See "Managing scans on your computer" on page 30.

See "Managing quarantined files on your computer" on page 62.

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 Symantec's Insight technology, 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 *Drive*:\Users*username*\AppData\Local\Microsoft\Windows\Temporary Internet Files, *Drive*:\Users*username*\AppData\Local\Microsoft\Windows\INetCache, or *Drive*:\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 50.

See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 42.

See "Managing scans on your computer" on page 30.

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 65.

See "Responding to a virus or a risk detection" on page 22.

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**.

   On unmanaged computers and on some managed computers, you can also change the action on the application through the Status page. Next to Network and Host Exploit Mitigation, click **Options**, and then click **View Network Activity**, or click **View Application Settings**.

See "Allowing or blocking applications that are already running on the client" on page 86.

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 a trial license or a paid license. If the trial license has expired, the client does not update any content.

Table 2-2 Types of licenses

License type	Description

Trial license	If a trial license has expired, the top of the client's Status pane is red and displays the following message:
	
	`Trial License has expired.`
	`Click Details for more information.`
	
	When you click **Details**, the message indicates content downloads discontinue on a specific date, and to contact your administrator to purchase a paid license. The Status pane may also display some text that indicates the content is outdated.
	
	You can also view the license expiration date through the client interface. Click **Help > About**.

Paid license	If a paid license has expired, you should see no message regarding the expired status in the client's Status pane. The paid license expiration date does not display under **Help > About**. Content continues to update, such as Virus and Spyware definitions.

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

See “Types of alerts and notifications” on page 19.

See “Viewing the logs” on page 102.

Responding to messages to update the client software

If there is a client software update available for you to download, 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?
```

The client software update may also install silently in the background. When the installation completes, you may see a message to notify you that you must restart the computer.

To respond to an 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**.
3. If a message appears to notify you that an upgrade completed, follow the on-screen instructions to restart. The installation completes once you restart the computer.

Chapter 3

Managing scans

This chapter includes the following topics:

- Changing SONAR settings
- Checking your computer's security compliance with a Host Integrity scan
- Enabling Tamper Protection

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.

Starting in 14, scans access the complete definitions set in the cloud.

See "How Windows clients receive definitions from the cloud" on page 43.

Table 3-1 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 34.
Update virus definitions	Make sure that you have the latest virus definitions installed on your computer. See "Updating the client content using LiveUpdate" on page 17.
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 Auto-Protect" on page 63.

Table 3-1 Managing scans *(continued)*

Task	Description
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 client computer immediately" on page 15. See "Scheduling a user-defined scan on the client" on page 46. 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 22. 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 16. On a managed client, the administrator might initiate a Power Eraser scan from the management console. Power Eraser is a powerful scan that detects difficult threats and sometimes requires a restart to complete. The administrator manually handles the remediation for the detections. You cannot run Power Eraser directly from the client, however, Power Eraser is available as part of the SymDiag support tool. If you download the SymHelp tool and run a Power Eraser scan directly on the client, the logs are not sent to the management console. You should make sure not to run Power Eraser locally with the SymHelp tool while the administrator runs Power Eraser from the management console; otherwise, you might negatively affect your computer's performance.

Table 3-1 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 effect 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 54. See "Scheduling a user-defined scan on the client" on page 46.
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**. ■ 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 54.

Table 3-1 Managing scans *(continued)*

Task	Description
Adjust scans to reduce false positives	Exclude a safe file or process from being scanned. See "Excluding items from scans" on page 60.
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 "Understanding submissions to Symantec that improve protection on your computer" on page 66.
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, the client eventually removes it. You can also take other actions on the file. See "Managing quarantined files on your computer" on page 62.

Table 3-2 displays additional scan settings that you can modify if you want to increase protection, improve performance, or reduce false positives.

Table 3-2 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 54.

Table 3-2 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 that ELAM affects your computer's performance. You might also 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 64.
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 50.
Manage SONAR	You can adjust the settings for SONAR. See "Managing SONAR on your computer" on page 69.

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 viruses, Trojans, worms, and other threats like security risks. Each threat has a recognizable pattern that is called a signature. The client uses a definition file that contains a collection of known signature information. The scan engine compares each file or component to the definitions file. If the scan engine finds a match, the file is infected or is malicious.
- The scan engine uses the definitions files to determine what kind of threat it is. The scan engine then takes action to remediate. The scan engine may clean, delete, or quarantine the item that it detects as a threat. The scan engine may also repair any side effects that result from the threat. The action it takes depends on the type of threat it detects.
  See "How scans respond to a virus or risk detection" on page 41.
- Starting in 14, on standard or embedded/VDI clients that are connected to the cloud, scans access the full set of definitions in the cloud.
  See "How Windows clients receive definitions from the cloud" on page 43.

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

Table 3-3 Computer components that the client scans

Component	Description
Selected files	The client scans individual files, based on the type of scan you select, or the type of scan that an administrator schedules. You can also a scan an individual file or folder from Windows. For most types of scans, you select the files that you want scanned.
Computer memory	The client scans 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 the hard drive. If a virus is in memory, the scan cannot clean it. 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.
Removable media	A common way for some threats to spread is through removable media, such as a USB drive. The client does not automatically scan removable media when you insert it, but you can scan it by right-clicking it from Windows.

See "Scanning your client computer immediately" on page 15.

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.

Figure 3-1 How viruses and security risks attack a computer

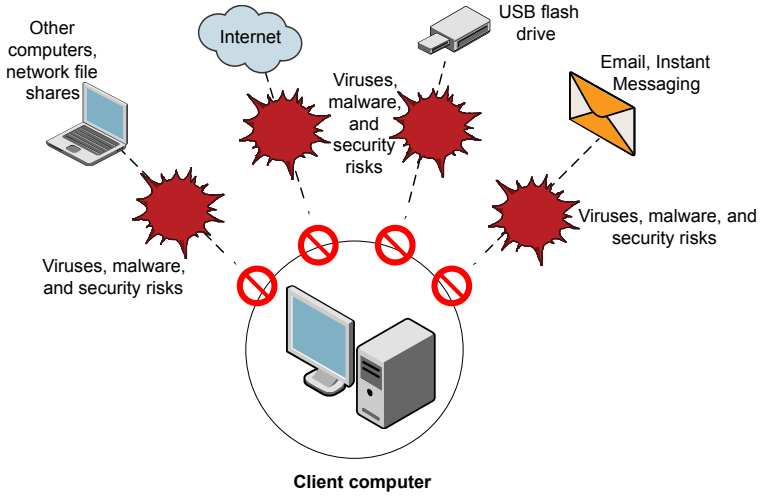

Table 3-4 lists the type of viruses and risks that can attack a computer.

Table 3-4 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.

Table 3-4 Viruses and security risks *(continued)*

Risk	Description
Adware	Programs that deliver advertising content.
Cookie	Messages that Web servers send to Web browsers for the purpose of identifying the computer or user
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.
Ransomware	A category of malware that sabotages documents and makes then unusable, but the computer user can still access the computer.
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.

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 41.

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.

Note: Starting in 14, scans access the complete definitions set in the cloud.

See "How Windows clients receive definitions from the cloud" on page 43.

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 affect computer performance.

Table 3-5 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. As of 14, on standard and embedded/VDI clients that are connected to the cloud, Auto-Protect also uses cloud definitions. See "About the types of Auto-Protect" on page 39.
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 Symantec Insight to make decisions about files" on page 42.

Table 3-5 Scan types *(continued)*

Scan type	Description
Administrator scans and user-defined scans	For managed clients, your administrator might create scheduled scans or run scans on demand. On 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. Starting in 14, on standard and embedded/VDI clients that are connected to the cloud, these scans use cloud definitions. 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 the scans that you start manually. You can run scans on demand from the **Scan for Threats** page. If the client detects a large number of viruses, spyware, or high-risk threats, an aggressive scan mode engages. The scan restarts and uses Insight lookups. See "How virus and spyware scans work" on page 34.
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 68.

See "Managing scans on your computer" on page 30.

About the types of Auto-Protect

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

Auto-Protect works on your supported email client only. It does not protect mail 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 3-6 Types of Auto-Protect

Type of Auto-Protect	Description
File System 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. Auto-Protect scans all files, even email attachments. If you do not enable Auto-Protect for email, your client computers are still protected when File System 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 writes 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.
Microsoft Outlook Auto-Protect	Downloads incoming Microsoft Outlook email attachments and scans for viruses and security risks when you read the message and open the attachment. Microsoft Outlook Auto-Protect supports Microsoft Outlook 98 through Outlook 2016, for the MAPI or Internet protocols. Microsoft Outlook Auto-Protect supports 32-bit and 64-bit systems. During installation, Symantec Endpoint Protection installs Microsoft Outlook Auto-Protect if your administrator included it in the package and Microsoft Outlook is already installed on the computer. 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:** You should not install Microsoft Outlook Auto-Protect on a Microsoft Exchange Server.

Table 3-6 Types of Auto-Protect *(continued)*

Type of Auto-Protect	Description
Internet Email Auto-Protect (Only available for client versions earlier than 14.2 RU1.)	Scans inbound Internet email body and email 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. Internet Email Auto-Protect supports 32-bit or 64-bit systems. 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. Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.
Lotus Notes Auto-Protect (Only available for client versions earlier than 14.2 RU1.)	Scans incoming Lotus Notes email attachments for viruses and security risks. Lotus Notes Auto-Protect supports Lotus Notes 7.x or later. During installation, Symantec Endpoint Protection installs Lotus Notes Auto-Protect if your administrator included it in the package and Lotus Notes is already installed on the computer.

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 3-7 How a scan responds to viruses and security risks

Threat type	Action
Virus	By default, when the client detects a virus, the client takes the following actions: ■ 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 "Managing quarantined files on your computer" on page 62. **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.

Table 3-7 How a scan responds to viruses and security risks *(continued)*

Threat type	Action
Security risk	By default, when the client detects a security risk, the client takes the following actions: ■ The client quarantines the infected file. ■ The client tries to remove or repair any changes that the security risk made. ■ The client the client cannot quarantine a security risk, it logs the risk and leaves it alone. In some instances, you might intentionally but unknowingly install an application that includes a security risk such as adware or spyware. If such a security risk is detected, the client takes the following action: ■ The client quarantines the risk immediately, if this action does not harm the computer or leave it in an unstable state. ■ Otherwise, the client waits until the application installation is complete before it quarantines the risk, and 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 Symantec Insight 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 is available to Symantec products in the cloud through Symantec Insight. Symantec Insight provides a file reputation database and the latest virus and spyware definitions.

Symantec products leverage Insight 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. Symantec Endpoint Protection must request or query Insight for information. The queries are called reputation lookups, cloud lookups, or Insight lookups.

Insight reputation ratings

Symantec Insight determines each file's level of risk or security rating. The rating is also known as the file's reputation.

Insight determines a file's security rating by examining the following characteristics of a 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

Insight lookups

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 requires reputation information to make detections. SONAR also uses reputation information to make detections.

You can change the Insight lookups setting. Go to **Change Settings > Client Management > Submissions**.

Starting in 14, on standard and embedded/VDI clients, the Insight lookups option also allows Auto-Protect and scheduled and manual scans to look up file reputation information as well as definitions in the cloud. Symantec recommends that you keep the option enabled.

Warning: Download Insight, SONAR, and virus and spyware scans use Insight lookups for threat detection. Symantec recommends that you always allow Insight lookups. Disabling lookups disables Download Insight and impairs the functionality of SONAR heuristics and virus and spyware scans.

File reputation submissions

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 and the latest definitions in the cloud. The more clients that submit information the more useful the reputation database becomes.

Symantec recommends that you keep client submissions for reputation detections enabled.

See “Managing Download Insight detections on your computer” on page 50.

See “Understanding submissions to Symantec that improve protection on your computer” on page 66.

How Windows clients receive definitions from the cloud

Starting in 14, Symantec Endpoint Protection standard and embedded/VDI clients provide real-time protection with definitions in the cloud. Earlier versions provided some cloud protection with various features, such as Download Insight. Now, all virus and spyware features use the cloud to evaluate files. Cloud content includes the entire set of virus and spyware definitions as well as the latest information that Symantec has about files and potential threats.

Clients support cloud-enabled content

Cloud-enabled content includes a reduced-sized set of definitions that provides full protection. When the client requires new definitions, the client downloads or looks up the definitions in the cloud for better performance and speed.

Your client type must support cloud-enabled content.

You can see your client type in **Help > Troubleshooting > Install Settings**.

Starting in 14, standard clients and embedded/VDI clients support cloud-enabled content.

All scans automatically use cloud lookups

Cloud lookups include queries to Symantec Insight for file reputation information and definition checking in the cloud.

- Scheduled and on-demand scans automatically perform cloud lookups.
- Auto-Protect also automatically performs cloud lookups. Auto-Protect now runs in user mode rather than kernel mode to reduce memory usage and provide better performance.

In addition to leveraging a smaller footprint with definitions on disk, the Intelligent Threat Cloud Service provides a 15-percent reduction in scan time.

Clients automatically send information about file reputation lookups to Symantec.

What are portal files?

Download Insight marks a file as a portal file when it examines a file that a user downloads from a supported portal. Scheduled and on-demand scans, Auto-Protect, and Download Insight evaluate the reputation of portal files using the sensitivity level that is set for Download Insight.

Note: Download Insight must be enabled to mark files as portal files.

Supported portals include: Internet Explorer, Firefox, Microsoft Outlook, Outlook Express, Google Chrome, Windows Live Messenger, and Yahoo Messenger. The portal list (or Auto-Protect portal list) is part of the Virus and Spyware Protection content that LiveUpdate downloads to the management server or the client.

Scans and Download Insight always evaluate non-portal files with a default internal sensitivity level that Symantec sets. The internal default detects only the most malicious files.

An example of cloud lookups in action

An example of the way the Intelligent Threat Cloud Service protects clients:

- You use Internet Explorer to try to download a file. Download Insight uses its sensitivity level and reputation information from Symantec Insight in the cloud to determine that the file is not harmful.

- Download Insight determines that the file's reputation is acceptable, allows the file to download, and marks the file as a portal file.
- Later, Symantec gets more information about the file from its extensive global intelligence network. Symantec determines that the file might be harmful and updates the Insight reputation database. Symantec might provide a late-breaking signature for the file in its definitions in the cloud.
- If you open the file or run a scan, Auto-Protect or the scan gets the latest information about the file from the cloud. Using the latest file reputation and the Download Insight sensitivity level, or using a late-breaking file signature, Auto-Protect or the scan now detects the file as potentially malicious

Required and recommended settings

By default, Symantec Endpoint Protection uses the cloud. If you disable any of these options, you limit or disable cloud protection.

- Auto-Protect
  Auto-Protect must be enabled. Auto-Protect is enabled by default.
- Download Insight
  Download Insight must be enabled so that it can examine file downloads, and so that file downloads are marked as portal files for future scans. If you disable Download Insight, all file downloads are treated as non-portal. Scans detect only the most malicious non-portal files.
  See "Managing Download Insight detections on your computer" on page 50.
- Insight lookups
  Insight lookups must be enabled. The Insight lookups option controls reputation lookups as well as cloud definition lookups. This option is enabled by default.

  Warning: If you disable Insight lookups, cloud protection is completely disabled.

- Submissions
  Symantec recommends that you share information with Symantec. Data you share with Symantec improves the performance of detection features. Information about the potential malware that might attack your computers helps improve the security landscape and address threats faster. Symantec makes every attempt to make the data pseudonymous to prevent the transmission of personally identifiable information.
  See "Understanding submissions to Symantec that improve protection on your computer" on page 66.

Scheduling a user-defined scan on the client

A scheduled scan on the Symantec Endpoint Protection client 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 client computer immediately" on page 15.

See "Managing scans on your computer" on page 30.

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.

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 49.

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**.

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 client computer immediately" on page 15.

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 the client" on page 46.

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 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 3-8 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 then scans the file when the user opens or runs the file. See "How Symantec Endpoint Protection uses Symantec Insight to make decisions about files" on page 42.
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 "Understanding submissions to Symantec that improve protection on your computer" on page 66.

Table 3-8 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 24.
Create exceptions for specific files or web domains	You can create an exception for an application that you 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, the Symantec Endpoint Protection client allows any file that a user downloads from one of the trusted sites. Download Insight only recognizes those trusted sites that you or your administrator have explicitly configured. See "Excluding items from scans" on page 60.

Table 3-8 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. The message only appears 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** to always allow these detections and not notify you. 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 53.
Control what information you submit about reputation detections to Symantec	By default, all managed clients send information about reputation detections to Symantec. Symantec recommends that you keep submissions enabled for reputation detections. The information helps Symantec address threats. See "Understanding submissions to Symantec that improve protection on your computer" on page 66.

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.

Note: Auto-Protect must be enabled in order for Download Insight to function. If Auto-Protect is disabled, Download Insight does not function even if Download Insight is enabled.

See "Managing Download Insight detections on your computer" on page 50.

To customize 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: With only basic Virus and Spyware Protection installed, the malicious file sensitivity is automatically set to level 1, and you cannot change the setting.

   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: *x* or fewer users**, where *x* is by default 5. You can select another value from the drop-down list.
   - **Files known by users for: *x* or fewer days**, where *x* is by default 2. You can enter any value

     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.
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.

You can customize a user-defined scan, global scan settings, and Auto-Protect.

- To customize a user-defined scan
- To change global scan settings
- To customize Auto-Protect

See "Managing scans on your computer" on page 30.

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 specify fewer file types to scan, click **Selected extensions**, and then click **Extensions**.

  Note: User-defined scans always scan container files unless you disable the compressed file option on the scheduled scan under **Advanced Scanning Options**, 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 65.

- To configure advanced options for compressed files, backups, and tuning, click **Advanced**.

  You can 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 In the client, in the sidebar, click **Change settings**, and the next to Virus and Spyware Protection, click **Configure Settings**.

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

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 54.

See "Customizing Download Insight settings" on page 53.

See "Changing SONAR settings" on page 70.

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

To configure actions for malware and security risk detections

1. In the client, in the sidebar, click **Change settings**.
2. Next to Virus and Spyware Protection, click **Configure Settings**, and then on any Auto-Protect tab, click **Actions**.
3. Click **Actions**.
4. In the **Scan Actions** dialog box, select the category **Malware** or **Security Risks**.

   You can also select a subcategory. 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 For a category or a subcategory, 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 the **Malware** category.

Note: This setting is only available as a first action for the **Malware** category. 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 the detected virus and is no longer susceptible to the spread of that virus into other areas of your computer.

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 the 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 malware, this action moves the infected file from its original location to the Quarantine. This setting is the default second action for malware.
- For security risks, this action 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 the 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 was taken appears in the **Notification** dialog box. The information also appears in the event log. This setting is the default second action for security risks. 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 and places an entry in the risk history to keep a record of it. Use this option to take manual control of how the client handles malware or security risks. **Note:** Malware may be able to spread to other parts of your computer or to other computers on the network until you take further action. 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. 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 files and other items 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. 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.

Table 3-9 Exception types

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

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.

See "Excluding items from scans" on page 60.

Excluding items from scans

You can exclude items from being scanned applications and files that you know are safe. You can also exclude some items to improve the computer's performance.

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.

You can exclude items from security risk scans, exclude folders from SONAR scans, and exclude an application from all scans.

- To exclude items from security risk scans
- To exclude a folder from SONAR
- To exclude an application that makes a DNS or a host file change
- To change how all scans handle an application

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.
     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**.

If you run an application that writes many temp files to a folder, you might want to exclude the folder from Auto-Protect. Auto-Protect scans files as they are written so you can increase computer performance by limiting the exception to scheduled and on-demand scans.

You might want to exclude the folders that are not often used or that contain archived or packed files from scheduled and on-demand scans. For example, scheduled or on-demand scans of deeply archived files that are not often used might decrease computer performance. Auto-Protect still protects the folder by scanning only when any files are accessed or written to the folder.

- 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 domain name or IP address that you want to exclude from Download Insight and SONAR detection. You can specify a URL, but the exception uses only the domain name portion of a URL. If you specify a URL, you can pre-pend the URL with either HTTP or HTTPS (case-insensitive), but the exception applies to both. The exception allows you to download files from any location in the domain.
  For Download Insight, 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 the **Internet Options > Security > Automatically detect intranet network** option discovers.

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 exclude an application that makes a DNS or a host file change

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 **DNS or Host File Change Exception > Application**

4 Select the application that you want to exclude, and then click **OK**.

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 30.

See "About excluding items from scans" on page 58.

Managing quarantined files on your computer

About quarantined files

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. When the client moves an infected file to the quarantine, it encrypts the file. Since the file is encrypted, you do not have access to the quarantined file. A file in the quarantine 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.

After your computer is updated with new virus definitions, the client automatically rescans 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.
- For security risks, scans move infected files to the quarantine and repair any side effects of the security risk.
- Download Insight and SONAR can also quarantine files.

See "How scans respond to a virus or risk detection" on page 41.

Managing files in the quarantine

Because the quarantine handles the infected files on your computer, you can leave the files in the quarantine. However, there are some actions that you may want to perform on a file in the quarantine. For example, if a file was quarantined in error, you can restore the file from the quarantine. Or, if you need to conserve space on your computer, you can reduce the time before the quarantine automatically deletes its contents.

To manage files in the quarantine

1. In the client, in the sidebar, click **View Quarantine**.
2. In the **View Quarantine** window, select the file in the list of quarantined items.
3. Click one of the options and follow any on-screen instructions.

See "Managing scans on your computer" on page 30.

Enabling Auto-Protect

You should keep Auto-Protect enabled 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 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 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 **Outlook Auto-Protect** tab, check **Enable Microsoft Outlook Auto-Protect**. Microsoft Outlook Auto-Protect is automatically installed on the computers that run Outlook.
   - For versions earlier than 14.2 RU1, on the **Internet Email Auto-Protect** tab, check **Enable Internet Email Auto-Protect**.
     Internet Email Auto-Protect is not supported on server operating systems.
   - For versions earlier than 14.2 RU1, on the **Notes Auto-Protect** tab, check **Enable Lotus Notes Auto-Protect**.
4. Click **OK**.

See "About the types of Auto-Protect" on page 39.

See "How to determine whether the client computer is protected using the Status page icons" on page 14.

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 the client 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 and later, and Windows Server 2012 and later. The Windows early launch anti-malware driver must be enabled for this option to take effect.

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 Help tool. You can obtain the Symantec Help tool through the Symantec Endpoint Protection client's **Help** button.

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**.
4. If you want to log the detections only, under **When a potentially malicious driver is detected**, 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 30.

See "Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)" on page 100.

See "Excluding items from scans" on page 60.

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 25.

Understanding submissions to Symantec that improve protection on your computer

By default, the client periodically sends pseudonymous detection, network, and configuration information to Symantec. Symantec 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. Symantec recommends that you submit as much information as possible.

Symantec makes every attempt to pseudonymize any information the client sends.

The pseudonymous information the client sends to Symantec benefits you by:

- Increasing the security of your network
- Optimizing product performance

In some cases, however, you might want to prevent the client from submitting some information. You can disable submission of network information only rather than disabling all types of client submissions.

Note: Symantec recommends that you always keep client submissions enabled. Disabling submissions might interfere with faster resolution of false positive detections on the applications that are used exclusively in your organization. Without information about the malware in your organization, product response and Symantec response to threats might take longer.

The data that Symantec telemetry collects may include pseudonymous elements that are not directly identifiable. Symantec neither needs nor seeks to use telemetry data to identify any individual user.

To modify submissions to Symantec

1. Select **Change Settings** > **Client Management**.
2. On the **Submissions** tab, check **Send pseudonymous data to Symantec to receive enhanced threat protection intelligence**. This option lets Symantec Endpoint Protection submit information about the threats that are found on your computer as well as information about your network and configuration.

   Symantec recommends that you keep this option enabled.
3. Select **More options** if you want to choose the types of information to submit.
4. Click **OK**.

You can also manually submit a file to Symantec from the Quarantine.

See “Managing quarantined files on your computer” on page 62.

For more information about privacy, see the following document:

Privacy statement

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 3-10 shows the protection status reporting in WSC.

Table 3-10 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)
Symantec Endpoint Protection is installed and ccSvcHst is turned off manually	OFF (red)

Table 3-11 shows the Symantec Endpoint Protection firewall status reporting in WSC.

Table 3-11 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, Memory Exploit Mitigation, 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.

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.

Note: SONAR does not inject code into applications on computers that run Symantec Endpoint Protection earlier than 12.1.2. If you use Symantec Endpoint Protection Manager 12.1.2 or later to manage clients, a SONAR file exception in an Exceptions policy is ignored on those 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.

See "Managing SONAR on your computer" on page 69.

See "Excluding items from scans" on page 60.

Managing SONAR on your computer

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

Table 3-12 Managing SONAR on your 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 "Enabling protection on the client computer" on page 98.
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 "Customizing Download Insight settings" on page 53.
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 70.
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 60.

Table 3-12 Managing SONAR on your 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 60.
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 "Understanding submissions to Symantec that improve protection on your computer" on page 66.

See "Managing scans on your computer" on page 30.

See "About the types of scans" on page 38.

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.

   You can also change the notification settings and whether or not SONAR makes detections on remote computers (network drives).
4. 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.

   You can enable or disable **Suspicious Behavior Detection** only when SONAR is disabled.

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

6 Click **OK**.

See "Managing SONAR on your computer" on page 69.

Checking your computer's security compliance with a Host Integrity scan

A Host Integrity scan verifies that your computer meets certain security requirements before it connects to the network. For example, the Host Integrity check may verify whether the operating system has the latest security patch. If your computer does not meet a security requirement, the client may remediate your computer to make sure that it passes the Host Integrity check. To remediate, the check automatically downloads and installs the necessary software. Your administrator may send a message to have you remediate your computer.

The Host Integrity check runs when you start your computer and continues until the network connection ends. You can also run a Host Integrity check manually.

Your administrator may have also configured the Host Integrity check to pass even if a specific requirement fails. You can view the results of the Host Integrity checks in the client's Security log.

To check your computer's security compliance with a Host Integrity scan

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

2 In the **Scan for threats** dialog box, click **Run Host Integrity Scan**.

3 Click **OK**.

If a compliance failure prevents access to the network, you should regain access when you update your computer to meet compliance requirements.

The scan results appear in the Security log.

See "Remediating your computer to pass the Host Integrity check" on page 71.

See "Viewing the logs" on page 102.

Remediating your computer to pass the Host Integrity check

If the client does not meet a Host Integrity policy requirement, 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 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.

See "Checking your computer's security compliance with a Host Integrity scan" on page 71.

Enabling 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.

To enable 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, make sure that **Protect Symantec security software from being tampered with or shut down** is checked.
4. 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**.
5. Click **OK**.

Chapter 4

Managing the firewall, intrusion prevention, and application hardening

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 4-1 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 4-1 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 75.
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 76. You can also configure a firewall rule to allow applications to access the network or prevent the applications from accessing the network. See "Allowing or blocking applications that are already running on the client" on page 86.
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 firewall settings" on page 82.
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 101. See "Enabling the Packet log" on page 103.
Allow or block 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 "Blocking traffic when the screensaver is active or the firewall does not run" on page 87. ■ You can automatically allow or block, or ask you to allow or block access to the network by an application that runs on your computer. You can also configure See "Allowing or blocking applications from accessing the network" on page 86. See "Allowing or blocking applications that are already running on the client" on page 86.

Table 4-1 Managing firewall protection *(continued)*

Task	Description
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 protection on the client computer" on page 98.

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 unit 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 include the following information about the data:

- The originating computer
- The intended recipient or 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 73.

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 4-2 describes what you need to know to manage firewall rules.

Table 4-2 Managing firewall rules

Task	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 78. ■ That the client uses stateful inspection, which keeps track of the state of the network connections See "How the firewall uses stateful inspection" on page 79. ■ The firewall components that make up the firewall rule See "The elements of a firewall rule on the client" on page 76.
Add a new firewall rule	You can perform the following tasks to manage firewall rules: ■ Add your own rules to the rules that Symantec Endpoint Protection installs by default See "Adding firewall rules on the client" on page 80. ■ Customize a rule by changing any of the firewall rule criteria ■ Export and import firewall rules from another firewall policy See "Exporting or importing firewall rules on the client" on page 81. ■ Copy and paste firewall rules

The elements of a firewall rule on the client

When a computer attempts to connect to another computer, the Symantec Endpoint Protection firewall compares the connection type with the firewall 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 packet triggers a firewall rule, the firewall evaluates no further firewall rules. If the packet triggers no rule, the firewall automatically blocks the packet and does not log the event.

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 4-3 describes the criteria that you use to define a firewall rule.

Table 4-3 Firewall rule criteria

Condition	Description
Triggers	■ 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 criteria 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.

Table 4-3 Firewall rule criteria *(continued)*

Condition	Description
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.
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, the traffic that the rule specifies can access your network. If the firewall blocks traffic, the traffic that the rule specifies cannot access your network.

See "How the firewall uses stateful inspection" on page 79.

See "Adding firewall rules on the client" on page 80.

See "Managing firewall rules" on page 76.

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

Table 4-4 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 "How a firewall works" on page 75.

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.

The state table that maintains the connection information may be periodically cleared. For example, it is cleared when a Firewall policy update is processed or if Symantec Endpoint Protection services are restarted.

See "How a firewall works" on page 75.

See "Managing firewall rules" on page 76.

Adding firewall rules on the client

When you add or change a firewall rule on the Symantec Endpoint Protection client, 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 website.

Firewall rules are automatically enabled when you create them.

Note: You can add or change firewall rules on unmanaged clients, or if the administrator grants client control to managed clients.

To add a firewall rule

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, click **Add** to open a blank rule.

   Note: For managed clients, this action launches the rule creation wizard. The following steps describe configuring a blank rule.

   ---

4. On the **General** tab of the blank rule, 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:
   - **General**
   - **Hosts**
   - **Ports and Protocols**
   - **Applications**
   - **Scheduling**

For example, you may want to select to which network adapters this rule applies, to which hosts this rule applies, the time period during which the rule is active or inactive, or to log the packet traffic.

Note: Use caution when you write to the Packet log, because a potentially large amount of data is logged.

See "The elements of a firewall rule on the client" on page 76.

6 Click **OK**.

Rules are enabled automatically. You must enable rules so that the firewall can process them.

7 To change the order of the rules click the up or down arrow.

8 Click **OK**.

Exporting or importing firewall rules on the client

You can share the rules with another Symantec Endpoint Protection 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 on the client

1 In the client, in the sidebar, click **Status**.

2 Beside **Network and Host Exploit Mitigation**, 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 on the client

1 In the client, in the sidebar, click **Status**.

2 Beside **Network and Host Exploit Mitigation**, 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 file in .sar format that contains the rules you want to import.

5 Click **Open**.

6 Click **OK**.

See "Adding firewall rules on the client" on page 80.

Enabling 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 4-5 describes the types of firewall settings that you can configure to further customize your firewall protection.

Table 4-5 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 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. See "Enabling network file and printer sharing with the Symantec Endpoint Protection client installed" on page 83.

Table 4-5 Firewall settings *(continued)*

Category	Description
Attack detection and blocking	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.
Inbound traffic control	You can configure the client to block inbound traffic and outbound traffic in the following situations: ■ When your computer's screensaver is activated. ■ When the firewall does not run. ■ When you want to block all inbound traffic and outbound traffic at any time. See "Blocking traffic when the screensaver is active or the firewall does not run" on page 87.

To enable firewall settings

1. In the client, click **Change Settings**.
2. Beside **Network and Host Exploit Mitigation**, 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 76.

See "Adding firewall rules on the client" on page 80.

Enabling network file and printer sharing with the Symantec Endpoint Protection client installed

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 4-6 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. See "To automatically enable network file and printer sharing and browsing" on page 84.
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. See "To manually enable network file and printer sharing and browsing" on page 84. See "To manually enable other computers to browse files on the client computer" on page 85.

To automatically enable network file and printer sharing and browsing

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options** > **Change Settings**.
3. On the **Microsoft Windows Networking** tab, click either one of the following settings:
   - To browse other computers and printers in the network, click **Browse files and printers on the network**.
   - To enable other computers to browse files on your computer, click **Share my files and printers with others on the network**.
4. Click **OK**.

To manually enable network file and printer sharing and browsing

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options** > **Change Settings** > **Configure Firewall Rules**.

Note: You can only see this setting if your administrator made this setting available or if you are running an unmanaged client.

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 the following:

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 the following:

88

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

137, 138

13 Click **OK**.

To manually enable other computers to browse files on the client computer

1 In the client, in the sidebar, click **Status**.

2 Beside **Network and Host Exploit Mitigation**, click **Configure Settings**

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 the following:

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 the following:

88, 137, 138

12 Click **OK**.

See “Enabling firewall settings” on page 82.

Allowing or blocking applications from accessing the network

You can configure Symantec Endpoint Protection to allow or block the application, or to ask you first whether to allow or block the application. This action creates a firewall rule that specifies whether a running application on your computer may access the network. These rules are called application-based firewall rules. For example, you can block Internet Explorer from accessing any websites from your computer.

Table 4-7 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 applications from accessing the network

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > View Network Activity**
3. In the **Network Activity** dialog box, right-click the running application or service, and then select the action that you want the client to take on that application.

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

   See "Allowing or blocking applications that are already running on the client" on page 86.
4. Click **Close**.

Allowing or blocking applications that are already running on the client

You can configure the conditions for when and how applications that already run on the client computer are allowed or blocked. For example, you can specify that a video game application

can access the network only during specific hours. Application-based firewall rules are also called application settings.

See "Allowing or blocking applications from accessing the network" on page 86.

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.

To allow or block applications that are already running on the client

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, click **Options > View Application Settings**.
3. In the **View Application Settings** dialog box, you can change the action by right-clicking the application and clicking **Allow**, **Ask**, or **Block**.
4. To change other options about the application-based rule, click **Configure**.
5. In the **Configure Application Settings** dialog box, configure the restrictions or exceptions for this application.

   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.

   For more information about these settings, click **Help**.
6. Click **OK** to accept the configuration changes.
7. To remove the rule that you put on the application, click the application name, and then click **Remove**. 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.

   To remove all application-based firewall rules, **Remove All**.
8. Click **OK** to close the **View Application Settings** dialog box.

See "Adding firewall rules on the client" on page 80.

Blocking 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 screensaver is activated	You can configure your computer to block all the inbound and the outbound network neighborhood traffic when your computer's screensaver is activated. As soon as the screensaver turns off, your computer returns to the previously assigned security level. See "To block traffic when the screensaver is activated" on page 88.
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. See "To block traffic when the firewall does not run" on page 88.
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. See "To block all traffic at any time" on page 89.

You can allow all traffic by disabling Network Threat Protection.

See "Enabling protection on the client computer" on page 98.

To block traffic when the screensaver is activated

1. In the client, in the sidebar, click **Change Settings**.
2. Beside **Network and Host Exploit Mitigation**, click **Configure Settings**.
3. On the **Microsoft Windows Networking** tab, 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 and Host Exploit Mitigation**, click **Configure Settings**
3. On the **Firewall** tab under **Traffic Settings**, click **Block all traffic until the firewall starts and after the firewall stops**.

   If you disable **Allow initial DHCP and NetBIOS traffic**, the initial traffic that enables network connectivity is blocked.
4. Click **OK**.

To block all traffic at any time

1. In the client, in the sidebar, click **Status**.
2. Beside **Network and Host Exploit Mitigation**, 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 firewall settings" on page 82.

Configuring intrusion prevention

By default, intrusion prevention runs on your computer. 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 is the second layer of defense after the firewall to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

Note: Intrusion prevention and the firewall are part of Network Threat Protection. Network Threat Protection and Memory Exploit Mitigation are part of Network and Host Exploit Mitigation.

To manage intrusion prevention:

1. Make sure that the latest IPS signatures are downloaded.

   By default, the latest signatures are downloaded to the client. However you might want to download the signatures manually immediately.

   See "Updating the client content using LiveUpdate" on page 17.

2. Keep intrusion prevention enabled.

   You should keep intrusion prevention enabled at all times. 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 "Viewing the logs" on page 102.

   See "Enabling the Packet log" on page 103.

3. If you think the detection is a false positive, notify your administrator.

   Do not assume that unexpected events are false positives.

Best Practice for Responding to Suspected IPS False Positives in Symantec Endpoint Protection

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

Enabling intrusion prevention

Intrusion prevention includes two types:

- 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.
- Browser intrusion prevention
  Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers. For the latest information about the browsers that browser intrusion prevention protects, see: Supported browser versions for browser intrusion prevention.

You can also enable or disable notifications when the client detects a network attack.

See: To enable intrusion prevention notifications

To enable intrusion prevention

1. In the client, in the sidebar, click **Change Settings**.
2. Beside **Network and Host Exploit Mitigation**, click **Configure Settings**.
3. On the **Intrusion Prevention** tab, make sure that the following options are checked:
   - **Enable Network Intrusion Prevention**
   - **Enable Browser Intrusion Prevention**
     You can also configure browser intrusion prevention to only log detections, but not block them. You should only use this configuration on a temporary basis as it decreases your computer's protection. For example, you would configure log-only mode while you troubleshoot blocked traffic. After you review the Security log to identify and exclude the signatures that block traffic, you disable log-only mode.
4. Click **OK**.

To enable intrusion prevention notifications

1. In the client, in the sidebar, click **Change Settings**.
2. Beside Network and Host Exploit Mitigation, click **Configure Settings**.

3 On the **Notifications** tab, make sure that **Display Intrusion Prevention and Memory Exploit Mitigation notifications** is checked.

4 Click **OK**.

Preventing attacks on vulnerable applications

Memory Exploit Mitigation (MEM) stops attacks on the commonly used applications that run on your Windows computer. When the client detects an exploit attempt, it displays one or both of the following messages.

- `Symantec Endpoint Protection: Attack: Structured Exception Handler Overwrite detected`

  The client blocks the exploit without terminating the application.

- `Symantec Endpoint Protection will terminate your application`

  The client terminates the application from running.

If the application keeps terminating, perform the following steps:

1. Notify your administrator.
2. Determine whether a true exploit attacked the application, or the detection was a false positive.
   - If an exploit attacked the application, check whether there is a patched version or a newer release of the infected application that fixes the current vulnerability. After you or your administrator installs the patched application, rerun it on the client computer to see if Memory Exploit Mitigation still terminates the application.
   - If the detection is a false positive, temporarily disable Memory Exploit Mitigation. Notify your administrator or Symantec Security Response about the false detection. Keep Memory Exploit Mitigation disabled until Symantec fixes the problem. Then reenable Memory Exploit Mitigation.

To determine whether a detection was a false positive

1 In the Security log, check that Memory Exploit Mitigation did terminate the application.

For example, you might see the following event: `Attack: Blocked Structured Exception Handler Overwrite attack against C:\Program Files (x86)\Adobe\Reader 9.0\Reader\AcroRd32.exe`

See "Viewing the logs" on page 102.

2 Disable Memory Exploit Mitigation.

3 Rerun the application.

- If the application runs correctly, the detection was a false positive.

- If the application behavior is abnormal, such as it brings up another application, the detection was a true positive.

On managed clients, your administrator may prevent you from disabling Memory Exploit Mitigation.

To disable and reenable Memory Exploit Mitigation

1. On the **Status** page next to **Network and Host Exploit Mitigation**, click **Options**.
2. In the drop-down menu, do one of the following tasks:
   - Click **Disable Memory Exploit Mitigation** or **Enable Memory Exploit Mitigation**.
   - Click **Change Settings** > **Memory Exploit Mitigation** tab, and check or uncheck **Enable Memory Exploit Mitigation**.

Chapter 5

Managing the client

This chapter includes the following topics:

Managing the client

By default, your client computer is protected and you should not need to configure the client. However, you may want to modify 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.
  See "About managed clients and unmanaged clients" on page 96.
  See "Checking whether the client is managed or unmanaged" on page 97.
- You want to enable or disable one or more protection technologies.
  See "Enabling protection on the client computer" on page 98.
- You want to verify that you have the latest virus definitions and security content.
- You have heard of a recent virus or security threat and want to run a scan.

Table 5-1 Tasks to configure the client

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 19.
Check the protection status	Regularly check the **Status** page to determine that all the types of protections are enabled. See "Enabling protection on the client computer" on page 98. See "Symantec Endpoint Protection client status icons" on page 13.
Update virus definitions and security content	Check that the computer has the latest virus definitions and security content. ■ Check whether you have the latest protection updates. You can check the date and number of these definitions files on the client's **Status** page, under each type of protection. ■ Obtain the latest protection updates. See "Updating the client content using LiveUpdate" on page 17. 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 client computer immediately" on page 15.
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 30. ■ Add firewall rules (unmanaged client only) See "Managing firewall protection" on page 73.
Run a compliance check	Check whether your computer is compliant with your company's security policy. See "Checking your computer's security compliance with a Host Integrity scan" on page 71.

Table 5-1 Tasks to configure the client *(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 102.
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. See "Symantec Endpoint Protection client status icons" on page 13. The security policy is updated automatically. However, to ensure that you have the latest policy, you can update it manually. See "Updating client policies" on page 95.

Updating client policies

You can update the policies on the Symantec Endpoint Protection client computer if you do not think you have the latest. 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.

You can only manually update the policy on the client computer. If policy settings prevent you from opening the user interface or the notification area icon, you may not be able to manually update the policy.

No command exists in Symantec Endpoint Protection Manager to manually prompt the client to update policies. The client checks in for policy updates based on its update method of pull mode or push mode.

To update the client policy on the client from the Windows taskbar

1. In the Windows taskbar, in the notification area, right-click the Symantec Endpoint Protection icon.
2. Click **Update Policy**.

To update the client policy from the client user interface

1. In the client, click **Help > Troubleshooting**.
2. In the **Troubleshooting** dialog box, in the left column, click **Management**.
3. On the **Management** panel, under **Policy Profile**, click one of the following:
   - Click **Update** to update the policy directly from the management console.

- Click **Import** to import the policy with one that was exported from the management console. Follow the prompt to select the policy file to import.

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 5-2 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. The management server notifies the client, and the client downloads the settings. Depending on the management server's communication settings, if the administrator makes a change to the protection, the client downloads the change almost immediately. 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 administrator manages the client, but you can change all the client settings and perform all the protection tasks. 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.
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 includes a Symantec Endpoint Protection client 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. However, Host Integrity is not supported on an unmanaged client. 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 5-3 describes the differences in the user interface between a managed and unmanaged client.

Table 5-3 Differences between a managed client and an unmanaged client by feature area

Feature area	Centrally managed client	Unmanaged 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.
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 and Host Exploit Mitigation 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 97.

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 96.

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**.

Hiding and displaying the notification area icon on the Symantec Endpoint Protection client

You can hide the Symantec Endpoint Protection notification area icon (also called the system tray icon) if necessary. For example, you can hide it if you need more space on the Windows taskbar.

See "Symantec Endpoint Protection client status icons" on page 13.

To hide or display the notification area icon on the client

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

---

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

2 On the **Change Settings** page, click **Configure Settings** next to **Client Management**.

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**.

Enabling protection on the client computer

You should keep all types of protection enabled on your computer at all times, especially Auto-Protect.

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 "Symantec Endpoint Protection client status icons" on page 13.

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.

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 protection technologies from the taskbar

- On the Windows desktop, in the notification area, right-click the client icon, and then click **Enable Symantec Endpoint Protection**.

To enable protection technologies from within the client

- In the client, on the **Status** page, beside ***protection type* Protection**, click **Options > Enable *protection type* Protection**.

To enable the firewall

1. On the client, at the top of the **Status** page, next to **Network and Host Exploit Mitigation**, click **Options** > **Change Settings**.
2. On the **Firewall** tab, check **Enable Firewall**.
3. Click **OK**.

See "Enabling Auto-Protect" on page 63.

Chapter 6

Troubleshooting the client

This chapter includes the following topics:

Troubleshooting computer issues with the Symantec Diagnostic Tool (SymDiag)

You can download a utility to diagnose common issues you encounter with installing and using 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 Diagnostic Tool (SymDiag)

1. Do one of the following tasks:
   - See: Download the Symantec Diagnostic Tool (SymDiag) to detect Symantec product issues
   - In either the Symantec Endpoint Protection Manager or the client, click **Help > Download Symantec Diagnostic Tool**
2. Follow the on-screen instructions.

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 6-1 Client logs

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.
Debug Log	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.
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 unless your administrator allows it. On an unmanaged client, you can enable the packet log. See "Enabling the Packet log" on page 103.
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 webpage that provides additional information. See "Managing quarantined files on your computer" on page 62.
Scan Log	Contains the entries about the scans that have run on your computer over time.
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. The Security log also displays the results of a Host Integrity check.

Table 6-1 Client logs *(continued)*

Log	Description
System Log	■ Virus and Spyware Protection: Contains the information about system activities on your computer that are related to viruses and to security risks. This information includes configuration changes, errors, and definitions file information. ■ Proactive Threat Protection: Contains the information about system activities on your computer that are related to SONAR. ■ Client Management: 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.
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.
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. With Risk Tracer enabled, the Network and Host Exploit Mitigation 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. For more information, see What is Risk Tracer?

See "Viewing the logs" on page 102.

Viewing the logs

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

To view a log

1. In the client, in the sidebar, click **View Logs**.
2. Click a **View Logs** button, and in the drop-down menu, select the log that you want to view.

   Some protection technologies might not appear, depending on your installation.

See "About the logs" on page 101.

Enabling the Packet log

All Network and Host Exploit Mitigation 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 101.

To enable the Packet log

1. In the client, on the **Status** page, beside **Network and Host Exploit Mitigation**, click **Options**, and then click **Change Settings**.
2. Click **Logs**.
3. Check **Enable Packet Log**.
4. Click **OK**.

Index

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W