Symantec Endpoint Protection and Symantec Network Access Control Client Guide

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

Documentation version 12.01.00.00

Legal Notice

Copyright © 2011 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, Bloodhound, Confidence Online, Digital Immune System, LiveUpdate, Norton, Sygate, and TruScan are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

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

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

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

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

Symantec’s support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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

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

Additional enterprise services

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

Enterprise services that are available include the following:

Managed Services  
Managed Services remove the burden of managing and monitoring security devices and events, ensuring rapid response to real threats.

Consulting Services  
Symantec Consulting Services provide on-site technical expertise from Symantec and its trusted partners. Symantec Consulting Services offer a variety of prepackaged and customizable options that include assessment, design, implementation, monitoring, and management capabilities. Each is focused on establishing and maintaining the integrity and availability of your IT resources.

Education Services  
Education Services provide a full array of technical training, security education, security certification, and awareness communication programs.

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

www.symantec.com/business/services/

Select your country or language from the site index.
Getting started on the client

This chapter includes the following topics:

■ About the Symantec Endpoint Protection client
■ About the Symantec Network Access Control client
■ Getting started on the Status page
■ About alert icons on the Status page
■ Scanning your computer immediately
■ Where to get more information

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

<table>
<thead>
<tr>
<th>Layer</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus and Spyware Protection</td>
<td>This layer combats a wide range of threats, including spyware, worms, Trojan horses, rootkits, and adware. File System Auto-Protect continuously inspects all computer files for viruses and security risks. Internet Email Auto-Protect scans the incoming and outgoing email messages that use the POP3 or SMTP communications protocol over the Secure Sockets Layer (SSL). Microsoft Outlook Auto-Protect scans incoming and outgoing Outlook email messages. See “Managing scans on your computer” on page 51.</td>
</tr>
<tr>
<td>Proactive Threat Protection</td>
<td>Proactive threat technology includes SONAR, which offers real-time protection against zero-day attacks. SONAR can stop attacks even before traditional signature-based definitions detect a threat. SONAR uses heuristics as well as file reputation data to make decisions about applications or files. See “Managing SONAR on your client computer” on page 91.</td>
</tr>
<tr>
<td>Network Threat Protection</td>
<td>This layer comprises firewall and intrusion prevention protection. The rules-based firewall prevents unauthorized users from accessing your computer. The intrusion prevention system automatically detects and blocks network attacks. See “Managing firewall protection” on page 96.</td>
</tr>
</tbody>
</table>

Your administrator manages which types of protection the management server should download to your client computer. The client automatically downloads the virus definitions, IPS definitions, and the product updates to your computer. Users who travel with portable computers can get virus definitions and product updates directly from LiveUpdate. See “Updating the computer's protection” on page 33.

---

**About the Symantec Network Access Control client**

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

See “How Symantec Network Access Control works” on page 129.

Getting started on the Status page

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

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

<table>
<thead>
<tr>
<th>Click this option</th>
<th>To do these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Help</td>
<td>Access the main online Help and perform the following tasks on the client:</td>
</tr>
<tr>
<td></td>
<td>■ View information about your computer, the client, and the client's protection.</td>
</tr>
<tr>
<td></td>
<td>■ View information about the client's connection status with the management server. You can also try to connect to the server, if necessary.</td>
</tr>
<tr>
<td></td>
<td>■ Import and export security policies and communication settings on an unmanaged client.</td>
</tr>
<tr>
<td></td>
<td>■ View and export debugging logs and a troubleshooting file to help your administrator diagnose a problem with the client or the client's protection.</td>
</tr>
<tr>
<td></td>
<td>■ Download a support utility tool to diagnose common issues with the client.</td>
</tr>
</tbody>
</table>
### Table 1-2  
Client main window (continued)

<table>
<thead>
<tr>
<th>Click this option</th>
<th>To do these tasks</th>
</tr>
</thead>
</table>
| **Status**        | View whether the computer is protected and whether the computer’s license is current. The colors and alert icons in the Status page show you which technologies are enabled and protecting the client.  
See “About alert icons on the Status page” on page 15.  
You can:  
■ Enable or disable one or more protection technologies.  
   See “About enabling and disabling protection” on page 40.  
■ View whether you have the latest definitions files for Virus and Spyware Protection, Proactive Threat Protection, and Network Threat Protection.  
■ Run an active scan.  
   See “Scanning your computer immediately” on page 16.  
■ View the threat list and view the results of the last virus and spyware scan. |
| **Scan for Threats** | Access and perform the following tasks:  
■ Run an active scan or full scan immediately.  
   See “Scanning your computer immediately” on page 16.  
■ Create a scheduled, startup, or on-demand scan.  
   See “Scheduling a user-defined scan” on page 67.  
   See “Scheduling a scan to run on demand or when the computer starts up” on page 70. |
### Table 1-2

**Client main window (continued)**

<table>
<thead>
<tr>
<th>Click this option</th>
<th>To do these tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Change Settings</strong></td>
<td>Configure settings for the following protection technologies and features:</td>
</tr>
<tr>
<td></td>
<td>▪ Enable and configure Auto-Protect settings.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing virus and spyware scan settings” on page 75.</td>
</tr>
<tr>
<td></td>
<td>▪ Configure the firewall settings and the Intrusion Prevention System settings.</td>
</tr>
<tr>
<td></td>
<td>See “Managing firewall protection” on page 96.</td>
</tr>
<tr>
<td></td>
<td>▪ View and add exceptions to scans.</td>
</tr>
<tr>
<td></td>
<td>See “Excluding items from scans” on page 82.</td>
</tr>
<tr>
<td></td>
<td>▪ Display the notification area icon.</td>
</tr>
<tr>
<td></td>
<td>See “How to determine whether the client is connected and protected” on page 36.</td>
</tr>
<tr>
<td></td>
<td>▪ Configure the Tamper Protection settings.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling, disabling, and configuring Tamper Protection” on page 44.</td>
</tr>
<tr>
<td></td>
<td>▪ Create a schedule to download content and product updates to the client.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the content on a schedule” on page 35.</td>
</tr>
<tr>
<td></td>
<td>See “Managing your computer's protection” on page 32.</td>
</tr>
<tr>
<td><strong>View Quarantine</strong></td>
<td>View the viruses and security risks that the client has detected and quarantined. You can restore, delete, clean, export, and add files in the quarantine.</td>
</tr>
<tr>
<td></td>
<td>See “About quarantining files” on page 85.</td>
</tr>
<tr>
<td><strong>View Logs</strong></td>
<td>View any of the client logs.</td>
</tr>
<tr>
<td></td>
<td>See “Viewing the logs” on page 47.</td>
</tr>
<tr>
<td><strong>LiveUpdate</strong></td>
<td>Run LiveUpdate immediately. LiveUpdate downloads the latest content definitions and product updates from a management server that is located within your company's network.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the content immediately” on page 34.</td>
</tr>
</tbody>
</table>

### About alert icons on the Status page

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

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

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

See “Scheduling a scan to run on demand or when the computer starts up” on page 70.

See “Updating the computer’s protection” on page 33.

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

**To scan your computer immediately**

- Do one of the following actions:
  - In the client, on the Status page, next to Virus and Spyware Protection, click Options > Run Active Scan.
  - In the client, in the sidebar, click Scan for threats.
    Do one of the following actions:
    - Click Run Active Scan.

### Table 1-3  Status page alert icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Green Checkmark]</td>
<td>Shows that each protection is enabled.</td>
</tr>
</tbody>
</table>
| ![Warning Sign] | Warns you that the client computer virus definitions are out of date. To receive the most current virus definitions, you can run LiveUpdate immediately. The client computer might have 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.  
  - Host Integrity is not connected.  
  See “Updating the computer’s protection” on page 33. |
| ![Red X] | Shows that one or more protections are disabled or that the client has an expired license. To enable a protection, you click Fix or Fix All.  
  See “About enabling and disabling protection” on page 40. |
Click **Run Full Scan**.

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

You can view the scan progress unless your administrator disables the option. To view scan progress, click the message link that appears for the current scan: **scan in progress**.

See “About scan results” on page 23.

You can also pause or cancel the scan.

See “Pausing and delaying scans” on page 17.

**To scan your computer from Windows**

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

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

---

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

---

**Pausing and delaying scans**

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

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

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

---

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

---

See “Managing scans on your computer” on page 51.
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.

Where to get more information
The product includes several sources of information.
Table 1-4 displays the Web sites where you can get additional information to help you use the product.

<table>
<thead>
<tr>
<th>Types of information</th>
<th>Web address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public knowledge base</td>
<td></td>
</tr>
<tr>
<td>Releases and updates</td>
<td>Symantec Endpoint Protection:</td>
</tr>
<tr>
<td>Contact options</td>
<td>Symantec Network Access Control:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/business/support/overview.jsp?pid=52788">http://www.symantec.com/business/support/overview.jsp?pid=52788</a></td>
</tr>
<tr>
<td>Virus and other threat information and updates</td>
<td><a href="http://securityresponse.symantec.com">http://securityresponse.symantec.com</a></td>
</tr>
<tr>
<td>Product news and updates</td>
<td><a href="http://enterprisesecurity.symantec.com">http://enterprisesecurity.symantec.com</a></td>
</tr>
<tr>
<td>Types of information</td>
<td>Web address</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>Free online technical training</td>
<td><a href="http://go.symantec.com/education_septc">http://go.symantec.com/education_septc</a></td>
</tr>
<tr>
<td>Symantec Educational Services</td>
<td><a href="http://go.symantec.com/education_sep">http://go.symantec.com/education_sep</a></td>
</tr>
<tr>
<td>Symantec Connect forums:</td>
<td>Symantec Endpoint Protection:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/connect/security/forums/">http://www.symantec.com/connect/security/forums/</a></td>
</tr>
<tr>
<td></td>
<td>endpoint-protection-antivirus</td>
</tr>
<tr>
<td></td>
<td>Symantec Network Access Control:</td>
</tr>
<tr>
<td></td>
<td><a href="http://www.symantec.com/connect/security/forums/">http://www.symantec.com/connect/security/forums/</a></td>
</tr>
<tr>
<td></td>
<td>network-access-control</td>
</tr>
</tbody>
</table>
Where to get more information
Responding to alerts and notifications

This chapter includes the following topics:

- Types of alerts and notifications
- About scan results
- Responding to a virus or risk detection
- Responding to Download Insight messages that ask you to allow or block a file that you try to download
- Responding to messages that ask you to allow or block an application
- About expired license messages
- Responding to messages to update the client software

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

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
</table>
| <scan name> started on or Symantec Endpoint Protection Detection Results dialog box | If a scan detects a virus or a security risk, the scan results or Symantec Endpoint Protection Detection Results dialog box appears with details about the infection. The dialog box also displays the action that the scan performs on the risk. You usually do not need to take any further actions other than to review the activity and to close the dialog box. You can take action if necessary, however.  
See “About scan results” on page 23. <scan name> started on or Symantec Endpoint Protection Detection Results  |
| 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 30.  
■ 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 28.  
■ The client's evaluation license has expired.  
See “About expired license messages” on page 29. |
Table 2-1  Types of alerts and notifications (continued)

<table>
<thead>
<tr>
<th>Alert</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notification area icon messages</td>
<td>Notifications that appear above the notification area icon occur in the following situations:</td>
</tr>
<tr>
<td></td>
<td>■ The client blocks an application. For example, you might see the following notification:</td>
</tr>
<tr>
<td></td>
<td>Traffic has been blocked from this application: <em>(application name)</em></td>
</tr>
<tr>
<td></td>
<td>If the client is configured to block all traffic, these notifications appear frequently. If your client is configured to allow all traffic, these notifications do not appear.</td>
</tr>
<tr>
<td></td>
<td>■ The client detects a network attack against your computer. You might see the following type of notification:</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ The security compliance check failed. Traffic may be blocked from going to and from your computer</td>
</tr>
<tr>
<td></td>
<td>You do not need to do anything else other than to read the messages.</td>
</tr>
<tr>
<td></td>
<td>See “How to determine whether the client is connected and protected” on page 36.</td>
</tr>
</tbody>
</table>

About scan results

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

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

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

■ The names of the viruses or security risks
The names of the infected files

- The actions that the client performs on the risks

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

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

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

See “About managed clients and unmanaged clients” on page 37.

See “Responding to a virus or risk detection” on page 24.

See “Pausing and delaying scans” on page 17.

---

**Responding to a virus or 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.

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

See “Managing quarantined files on your client computer” on page 84.
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:

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Clean</strong></td>
<td>Removes the virus from the file. This option is only available for viruses.</td>
</tr>
<tr>
<td><strong>Exclude</strong></td>
<td>Excludes the file from being scanned again.</td>
</tr>
<tr>
<td><strong>Delete Permanently</strong></td>
<td>Deletes the infected file and all side effects. For security risks, use this action with caution. In some cases, if you delete security risks you might cause an application to lose functionality.</td>
</tr>
<tr>
<td><strong>Undo Action Taken</strong></td>
<td>Reverses the action taken.</td>
</tr>
<tr>
<td><strong>Move To Quarantine</strong></td>
<td>Places the infected files in the Quarantine. For security risks, the client also tries to remove or repair the side effects. In some cases, if the client quarantines a security risk, it might cause an application to lose functionality.</td>
</tr>
<tr>
<td><strong>Properties</strong></td>
<td>Displays the information about the virus or security risk.</td>
</tr>
</tbody>
</table>

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. In that case, a **Remove Risks Now** dialog box appears.

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

   ■ **Yes**
   
   The client removes the risk. The removal of the risk might require a restart. Information in the dialog box indicates whether or not a restart is required.

   ■ **No**
   
   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 65.
See “Viewing the logs” on page 47.
See “Managing scans on your computer” on page 51.

About removing a virus or risk from an infected file

If the client 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.

Table 2-2 describes the options in the results dialog box.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close</td>
<td>Closes the results dialog box if you do not need to take action on any of the risks. If you need to take action, one of the following notifications appears:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Remove Risk Required</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Restart Required</strong></td>
</tr>
<tr>
<td></td>
<td>Appears when a risk requires a restart.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Remove Risk and Restart Required</strong></td>
</tr>
<tr>
<td></td>
<td>Appears when a risk requires process termination and another risk requires a restart.</td>
</tr>
<tr>
<td>Remove Risks Now</td>
<td>Displays the Remove Risk dialog box. In the Remove Risk dialog box, you can select one of the following choices for each risk:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>Yes</strong></td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>No</strong></td>
</tr>
<tr>
<td></td>
<td>When you close the results dialog box, the Remove Risk dialog box appears. The dialog box reminds you that you still need to take action. However, the Remove Risk dialog box is suppressed until you restart your computer.</td>
</tr>
</tbody>
</table>
If a restart is required, the removal or repair is not complete until you restart the computer.

You might need to take action on a risk but choose not to take action right now. The risk can be removed or repaired at a later time in the following ways:

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

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

See “Responding to a virus or risk detection” on page 24.

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

When Download Insight notifications are enabled, you receive messages about the malicious and the unproven files that Download Insight detects when you try to download them.

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

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

Download Insight uses Insight, Symantec’s technology that 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.

See “Managing scans on your computer” on page 51.

See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 66.

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

1. In the Download Insight detection message, do one of the following actions:
   - Click **Remove this file from my computer**.
     Download Insight moves the file to the Quarantine. This option only appears for unproven files.
   - Click **Allow this file**.
     You might see a permission dialog that asks whether or not you are sure that you want to allow the file.
     If you choose to allow an unproven file that was not quarantined, the file runs automatically. If you choose to allow a quarantined file, the file does not automatically run. You can run the file from your temporary Internet folder.
     Typically the folder location is `\Documents and Settings\username\Local Settings\Temporary Internet Files`.

2. On unmanaged clients, if you allow a file, Symantec Endpoint Protection automatically creates an exception for the file on this computer. On managed clients, if your administrator lets you create exceptions, Symantec Endpoint Protection automatically creates an exception for the file on this computer.

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.
- The client switches users through Fast User Switching.

You might see the following type of message, which tells you when an application tries to access your computer:
IEXPLORE.EXE is attempting to access the network. Do you want to allow this program to access the network?

To respond to 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. Optionally, to learn more about the connection and the application, click **Detail >>**.

3. Do one of the following actions:
   - To allow the application to access the network, click **Yes**.
   - To block the application from accessing the network, click **No**.

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

See “Configuring application-specific settings” on page 112.

**About expired license messages**

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

<table>
<thead>
<tr>
<th>Table 2-3</th>
<th>Types of licenses</th>
</tr>
</thead>
<tbody>
<tr>
<td>License type</td>
<td>Description</td>
</tr>
<tr>
<td>Evaluation license</td>
<td>If an evaluation license has expired, the top of the client's Status pane is red and displays the following message:</td>
</tr>
<tr>
<td></td>
<td>Evaluation License has expired.</td>
</tr>
<tr>
<td></td>
<td>All content download will discontinue on date. Please contact your Administrator to purchase a full Symantec Endpoint Protection License.</td>
</tr>
<tr>
<td></td>
<td>You can also view the expiration date by clicking <strong>Help &gt; About</strong>.</td>
</tr>
<tr>
<td>Paid license</td>
<td>If a paid license has expired, the top of the client's Status pane is yellow and displays the following message:</td>
</tr>
<tr>
<td></td>
<td>Virus and Spyware Protection definitions are out of date.</td>
</tr>
</tbody>
</table>
For either type of license, you must contact your administrator to update or renew the license.

See “Types of alerts and notifications” on page 21.

See “Viewing the logs” on page 47.

Responding to messages to update the client software

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

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

To respond to an automatic update notification

1. Do one of the following actions:
   - To download the software immediately, click **Download Now**.
   - To be reminded after the specified time, click **Remind me later**.

2. If a message appears after the installation process begins for the updated software, click **OK**.
Making sure that your computer is protected

This chapter includes the following topics:

- Managing your computer's protection
- Updating the computer's protection
- How to determine whether the client is connected and protected
- About managed clients and unmanaged clients
- Checking whether the client is managed or unmanaged
- About enabling and disabling protection
- Enabling or disabling protection on the client computer
- Enabling or disabling Auto-Protect
- Enabling, disabling, and configuring Tamper Protection
- About the logs
- Viewing the logs
- Tracing logged events back to their source
- Exporting log data
Managing your computer's protection

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

- Your computer runs an unmanaged client.
  Once an unmanaged client is installed, only you have control over your computer’s protection. An unmanaged client is protected by default. But you may need to modify the computer’s protection settings.
  See “About managed clients and unmanaged clients” on page 37.

- You want to enable or disable one or more protection technologies.

- You want to verify that you have the latest virus definitions.

- You have heard of a recent virus and want to run a scan.

Table 3-1 displays the process to make sure that your computer is protected.

Table 3-1  Process for managing your computer’s protection

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respond to alerts or notifications</td>
<td>Respond to messages that appear, asking you for input. For example, a scan might detect a virus or security risk and display a scan results dialog box that asks you to act on the detection. See “Types of alerts and notifications” on page 21.</td>
</tr>
<tr>
<td>Check the protection status</td>
<td>Regularly check the Status page to determine that all the types of protections are enabled. See “Getting started on the Status page” on page 13. See “Enabling or disabling protection on the client computer” on page 41.</td>
</tr>
</tbody>
</table>
### Table 3-1

Process for managing your computer's protection *(continued)*

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Update virus definitions</strong></td>
<td>Check that the latest virus definitions are installed on your computer.</td>
</tr>
</tbody>
</table>
| *(Unmanaged client only)*         | - Check whether you have the latest protection updates. You can check the date and number of these definitions files on the client’s **Status** page, under each type of protection.  
  - Obtain the latest protection updates.  
  See “**Updating the computer's protection**” on page 33.                                                                                     |
| **Scan your computer**            | Run a scan to see if the computer or your email application has any viruses. By default, the client scans the computer when you turn it on, but you can scan the computer at any time.  
  See “**Scanning your computer immediately**” on page 16.                                                                                     |
| **Adjust protection settings**    | In most cases, the default settings provide adequate protection for your computer. If necessary, you can decrease or increase the following types of protection:  
  - Scheduling additional scans  
    See “**Managing scans on your computer**” on page 51.                                                                                     
  - Adding firewall rules *(unmanaged client only)*  
    See “**Managing firewall protection**” on page 96.                                                                                          |
| **View logs for detections or attacks** | Check the logs to see if your client has found a virus detection or network attack.  
  See “**Viewing the logs**” on page 47.                                                                                                       |
| **Update the security policy**    | Check that the client received the latest security policy. A security policy includes the most current protection technology settings for your client.  
  The security policy is updated automatically. To ensure that you have the latest policy, you can update it manually by right-clicking the client notification area icon and clicking **Update Policy**.  
  See “**How to determine whether the client is connected and protected**” on page 36.                                                        |
| *(Managed client only)*           |                                                                                                                                                                                                           |
Content updates are the files that keep your Symantec products current with the latest threat protection technology. LiveUpdate retrieves the new content files from a Symantec Internet site, and then replaces the old content files. The updates that you receive depend on which products are installed on your computer. How your computer receives the updates depends on whether your computer is managed or unmanaged, and on how your administrator has configured updates.

The following types of files are examples of content updates:

■ Virus definition files for Virus and Spyware Protection.
■ Heuristic signatures and commercial application lists for Proactive Threat Protection.
■ IPS definition files for Network Threat Protection.

See “About Network Threat Protection” on page 96.

LiveUpdate can also provide improvements to the installed client. These improvements are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. These improvements to the client are released on an as-needed basis. A client computer can receive these improvements directly from a LiveUpdate server. A managed client computer can also receive these improvement updates automatically from a management server at your company.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Update the content on a schedule</td>
<td>By default, LiveUpdate runs automatically at scheduled intervals.</td>
</tr>
<tr>
<td></td>
<td>On an unmanaged client, you can disable or change a LiveUpdate schedule.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the content on a schedule” on page 35.</td>
</tr>
<tr>
<td>Update the content immediately</td>
<td>Based on your security settings, you can run LiveUpdate immediately.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the content immediately” on page 34.</td>
</tr>
</tbody>
</table>

**Table 3-2** Ways to update content on your computer

**Updating the content immediately**

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

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

See “Updating the content on a schedule” on page 35.
See “Updating the computer's protection” on page 33.

To update your protection immediately
- In the client, in the sidebar, click LiveUpdate.

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

Updating the content on a schedule

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

See “Updating the content immediately” on page 34.

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

To update your protection on a schedule

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

The time settings depend on what you select from the Frequency group box. The availability of the other options on this dialog box also depends on the frequency that you select.

6 In the Retry Window group box, check Keep trying for, and then specify the time interval during which the client tries to run LiveUpdate again.

7 In the Randomization Options group box, check Randomize the start time to be + or - 9in hours), and then specify the number of hours or days.

This option sets a range of time before or after the scheduled time for the update to start.
8 In the **Idle Detection** group box, check **Delay scheduled LiveUpdates until the system is idle.** Overdue sessions will eventually run unconditionally.

You can also configure options for proxy server connection to an internal LiveUpdate server. See the online help for information about the options.

9 Click **OK**.

### How to determine whether the client is connected and protected

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

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Yellow Shield" /></td>
<td>The client runs with no problems. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain yellow shield.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow Shield with Green Dot" /></td>
<td>The client runs with no problems. It is connected to and communicates with the server. All components of the security policy protect the computer. The icon is a yellow shield with a green dot.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow Shield with Light Yellow Dot" /></td>
<td>The client has a minor problem. For example, the virus definitions may be out of date. The icon is a yellow shield and a light yellow dot that contains a black exclamation mark.</td>
</tr>
<tr>
<td><img src="image" alt="Yellow Shield with White Dot and Red Outline" /></td>
<td>The client does not run, has a major problem, or has at least one protection technology disabled. For example, Network Threat Protection may be disabled. The icon is a yellow shield with a white dot outlined in red and a red line across the dot.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🛠️</td>
<td>The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It is either offline or unmanaged. Unmanaged clients are not connected to a management server. The icon is a plain gold key.</td>
</tr>
<tr>
<td>🛠️</td>
<td>The client runs with no problems and has both passed the Host Integrity check and updated the security policy. It communicates with the server. The icon is a gold key with a green dot.</td>
</tr>
<tr>
<td>🛠️</td>
<td>The client has either failed the Host Integrity check or not updated the security policy. The icon is a gold key with a red dot that contains a white &quot;x.&quot;</td>
</tr>
</tbody>
</table>

See “Hiding and displaying the notification area icon” on page 37.

Hiding and displaying the notification area icon

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

See “How to determine whether the client is connected and protected” on page 36.

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

To hide or display the notification area icon

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

About 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 3-5 Differences between a managed client and an unmanaged client

<table>
<thead>
<tr>
<th>Client type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Managed client  | A managed client communicates with a management server in your network. The administrator configures the protection and the default settings, and the management server downloads the settings to the client. If the administrator makes a change to the protection, the change is almost immediately downloaded to the client. Administrators can change the level at which you interact with the client in the following ways:achsen:

- The administrator manages the client completely. You are not required to configure the client. All the settings are locked or unavailable, but you can view information about what the client does on your computer.
- The administrator manages the client, but you can change some client settings and perform some tasks. For example, you may be able to run your own scans and manually retrieve client updates and protection updates.
- The availability of the client settings, as well as the values of the settings themselves, can change periodically. For example, a setting might change when your administrator updates the policy that controls your client’s protection.
- The administrator manages the client, but you can change all the client settings and perform all the protection tasks.                                                                                                                                 |

| Unmanaged client | An unmanaged client does not communicate with a management server and an administrator does not manage the client. An unmanaged client can be one of the following types:

- A standalone computer that is not connected to a network, such as a home computer or a laptop. The computer must include a Symantec Endpoint Protection installation that uses either the default option settings or administrator-preset settings.
- A remote computer that connects to the corporate network that must meet security requirements before it connects.

The client has default settings when it is first installed. After the client is installed, you can change all the client settings and perform all the protection tasks.                                                                                                                                                                                                                                                                 |

See “Checking whether the client is managed or unmanaged” on page 39.

Table 3-6 describes the differences in the user interface between a managed and unmanaged client.
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 a unmanaged client than on a managed client.

See “About managed clients and unmanaged clients” on page 37.

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 is Self-managed.
4 Click Close.
About enabling and disabling protection

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

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

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

Table 3-7 describes the reasons why you might want to disable each protection technology.

<table>
<thead>
<tr>
<th>Protection technology</th>
<th>Purpose for disabling the protection technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virus and Spyware Protection</td>
<td>If you disable this protection, you disable Auto-Protect only. The scheduled or startup scans still run if you or your administrator has configured them to do so. You might enable or disable Auto-Protect for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>■ Auto-Protect might block you from opening a document. For example, if you open a Microsoft Word that has a macro, Auto-Protect may not allow you to open it. If you know the document is safe, you can disable Auto-Protect.</td>
</tr>
<tr>
<td></td>
<td>■ Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, you might get a warning when you install new computer applications. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect.</td>
</tr>
<tr>
<td></td>
<td>■ Auto-Protect may interfere with Windows driver replacement.</td>
</tr>
<tr>
<td></td>
<td>■ Auto-Protect might slow down the client computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you disable Auto-Protect, you also disable Download Insight, even if Download Insight is enabled. SONAR also cannot detect heuristic threats. SONAR detection of host file and system changes continues to function.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling or disabling Auto-Protect” on page 42.</td>
</tr>
<tr>
<td></td>
<td>If Auto-Protect causes a problem with an application, it is better to create an exception than to permanently disable the protection.</td>
</tr>
<tr>
<td></td>
<td>See “Excluding items from scans” on page 82.</td>
</tr>
</tbody>
</table>
Table 3-7 Purpose for disabling a protection technology (continued)

<table>
<thead>
<tr>
<th>Protection technology</th>
<th>Purpose for disabling the protection technology</th>
</tr>
</thead>
</table>
| Proactive Threat Protection | You might want to disable Proactive Threat Protection for the following reasons:  
  ■ You see too many warnings about the threats that you know are not threats.  
  ■ Proactive Threat Protection might slow down the client computer.  
  See “Enabling or disabling protection on the client computer” on page 41. |
| Network Threat Protection   | You might want to disable Network Threat Protection for the following reasons:  
  ■ You install an application that might cause the firewall to block it.  
  ■ A firewall rule or firewall setting blocks an application due to an administrator's mistake.  
  ■ The firewall or the intrusion prevention system causes network connectivity-related issues.  
  ■ The firewall might slow down the client computer.  
  ■ You cannot open an application.  
  See “Enabling or disabling intrusion prevention” on page 126.  
  See “Enabling or disabling protection on the client computer” on page 41.  
  If you are not sure that Network Threat Protection causes the problem, you might need to disable all the protection technologies.  
  On a managed client, your administrator might lock Network Threat Protection completely so that you cannot enable or disable it. |
| Tamper Protection           | Typically you should keep Tamper Protection enabled.  
  You might want to disable Tamper Protection temporarily to make sure that you do not get false positive detections.  
  See “Enabling, disabling, and configuring Tamper Protection” on page 44. |

**Enabling or disabling protection on the client computer**

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

■ The status bar at the top of the Status page is red.

■ The client's icon appears with a universal no sign, a red circle with a diagonal slash. The client icon appears as a full shield in the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon does not appear.
See “How to determine whether the client is connected and protected” on page 36.

On a managed client, your administrator can enable any protection at any time. You can also disable Auto-Protect, Proactive Threat Protection, or Network Threat Protection for troubleshooting purposes. On a managed client, your administrator might lock a protection so that you cannot disable it.

See “About enabling and disabling protection” on page 40.

See “Enabling or disabling Auto-Protect” on page 42.

To enable protection technologies from the Status page

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

To enable or disable protection technologies from the taskbar

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

To enable or disable Proactive Threat Protection or Network Threat Protection

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

Enabling or disabling Auto-Protect

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

When you right-click the icon, a check mark appears next to Enable Auto-Protect when Auto-Protect for files and processes is enabled.

See “About alert icons on the Status page” on page 15.

See “About enabling and disabling protection” on page 40.
**Note:** 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.

If you have not changed the default option settings, Auto-Protect loads when you start your computer to guard against viruses and security risks. Auto-Protect checks programs for viruses and security risks as they run. It also monitors your computer for any activity that might indicate the presence of a virus or security risk. When a virus, virus-like activity (an event that can be the work of a virus), or a security risk is detected, Auto-Protect alerts you.

**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.

To **enable or disable Auto-Protect for the file system**

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

To **enable or disable Auto-Protect for email**

1. In the client, in the sidebar, click Change settings.
2. Next to Virus and Spyware Protection, click Configure Settings.
3. Do one of the following actions:
   - On the Internet Email Auto-Protect tab, check or uncheck Enable Internet Email Auto-Protect.
   - On the Outlook Auto-Protect tab, check or uncheck Enable Microsoft Outlook Auto-Protect.
   - On the Notes Auto-Protect tab, check or uncheck Enable Lotus Notes Auto-Protect.
4. Click OK.
Enabling, disabling, and configuring Tamper Protection

Tamper Protection provides real-time protection for Symantec applications that run on servers and clients. It prevents non-Symantec processes such as worms, Trojan horses, viruses, and security risks, from affecting Symantec resources.

You can configure the software to block or log attempts to modify Symantec resources.

If Tamper Protection is enabled, you can choose the action that it takes when it detects an attempt to tamper with Symantec software. You can also have Tamper Protection display a message to notify you of tamper attempts. If you want to customize the message, you can use the predefined variables that Tamper Protection fills in with the appropriate information.

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

For information about the predefined variables, see the Help on the Tamper Protection tab.

See “About enabling and disabling protection” on page 40.

To enable or disable Tamper Protection

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

To configure Tamper Protection

1. In the client, in the sidebar, click Change settings.
2. Next to Client Management, click Configure Settings.
3. On the Tamper Protection tab, in the Action to take if an application attempts to tamper with or shut down Symantec security software list box, click Block it and log the event or Log the event only.
4. If you want to be notified when Tamper Protection detects suspicious behavior, check Display a notification message when tampering is detected.

If you enable these notification messages, you may receive notifications about Windows processes as well as Symantec processes.
5 To customize the message that appears, update the text in the message field.
6 Click OK.

About the logs

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

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

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

For more information about a log, you can press F1 to view the help for that log. Table 3-8 describes the event types that each log displays.

Table 3-8  

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Log</td>
<td>Contains entries about the scans that have run on your computer over time.</td>
</tr>
<tr>
<td>Risk Log</td>
<td>Contains entries about viruses and security risks, such as adware and spyware, that have infected your computer. Security risks include a link to the Symantec Security Response Web page that provides additional information. See “Quarantining a file from the Risk or Scan Log” on page 86.</td>
</tr>
<tr>
<td>Virus and Spyware Protection System Log</td>
<td>Contains the information about system activities on your computer that are related to viruses and security risks. This information includes configuration changes, errors, and definitions file information.</td>
</tr>
<tr>
<td>Threat Log</td>
<td>Contains the information about the threats that SONAR detected on your computer. SONAR detects any files that act suspiciously. SONAR also detects system changes.</td>
</tr>
<tr>
<td>Log</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Proactive Threat Protection System Log</td>
<td>Contains information about system activities on your computer that are related to SONAR.</td>
</tr>
<tr>
<td>Traffic Log</td>
<td>Contains the events that concern firewall traffic and intrusion prevention attacks. The log contains information about the connections that your computer makes through the network. The Network Threat Protection logs can help you to detect potentially threatening activity such as port scanning. They can also be used to trace traffic back to its source. You can also use Network Protection logs to help troubleshoot connectivity problems or possible network attacks. The logs can tell you when your computer has been blocked from the network and help you to determine why your access has been blocked.</td>
</tr>
<tr>
<td>Packet Log</td>
<td>Contains the information about the packets of data that enter or leave through the ports on your computer. By default, the Packet log is disabled. On a managed client, you cannot enable the Packet log. On an unmanaged client, you can enable the Packet Log. See “Enabling the Packet Log” on page 47.</td>
</tr>
<tr>
<td>Control Log</td>
<td>The Control Log contains information about the Windows registry keys, files, and DLLs that an application accesses, as well as the applications that your computer runs.</td>
</tr>
<tr>
<td>Security Log</td>
<td>Contains the information about the activities that could 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.</td>
</tr>
<tr>
<td>Client Management System Log</td>
<td>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; The status of a client serving as a group update provider.</td>
</tr>
<tr>
<td>Tamper Protection Log</td>
<td>Contains entries about the attempts to tamper with the Symantec applications on your computer. These entries contain information about the attempts that Tamper Protection detected or detected and thwarted.</td>
</tr>
</tbody>
</table>
### Table 3-8 Client logs (continued)

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Debug Logs</td>
<td>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.</td>
</tr>
</tbody>
</table>

See “Viewing the logs” on page 47.

### Viewing the logs

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

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

**To view a log**

1. In the main window, in the sidebar, click View Logs.
2. Click View Logs next to one of the following items:
   - Virus and Spyware Protection
   - Proactive Threat Protection
   - Network Threat Protection
   - Client Management
   - Network Access Control
   
   Some items might not appear depending on your installation.
3. In the drop-down menu, select the log that you want to view.

See “About the logs” on page 45.

### Enabling the Packet Log

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

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

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

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

3. Check Enable Packet Log.

4. Click OK.

Tracing logged events back to their source

You can trace some events back to pinpoint the source of data from a logged event. A back trace shows the exact steps, or hops, that incoming traffic made. A hop is a transition point such as a router, which a packet travels through as it goes from computer to computer on the Internet. A back trace follows a data packet backwards, by discovering which routers the data took to reach your computer.

For some log entries, you can trace a data packet that was used in an attack attempt. Each router that a data packet passes through has an IP address. You can view the IP address and other details. The information that is displayed does not guarantee that you have discovered who the hacker truly is. The final hop’s IP address lists the owner of the router that the hackers have connected through, and not necessarily the hackers themselves.

You can back trace some logged events in the Security Log and the Traffic Log.

To back trace a logged event

1. In the client, in the sidebar, click View logs.

2. To the right of Network Threat Protection or Client Management, click View Logs. Then, click the log that contains the entry that you want to trace.

3. In the log view window, select the row of the entry that you want to trace.

4. Click Action, and then click BackTrace.

5. In the Back Trace Information dialog box, click Who is > > to view detailed information on each hop.

A drop panel displays detailed information about the owner of the IP address from which the traffic event originated. You can use Ctrl-C and Ctrl-V to cut and paste the information in the panel into an email message to your administrator.
6  Click **Who is <<** again to hide the information.
7  When you are finished, click **OK**.

### Exporting log data

You can export the information in some logs into a file with comma-separated values (.csv) or into an Access Database (*.mdb) format. The .csv format is a common file format that most spreadsheet and database programs use to import data. After you import the data into another program, you can use the data to create presentations, graphs, or to combine with other information. You can export the information in the Network Threat Protection logs and the Client Management logs into tab-delimited text files.

See “About the logs” on page 45.

---

**Note:** If you run the client software on Windows Server 2008 Server Core, you cannot export log data to an .mdb file. The .mdb format requires some Microsoft applications that are not available on Server Core.

You can export the following logs to a .csv or .mdb file:

- Virus and Spyware System Log
- Virus and Spyware Risk Log
- Virus and Spyware Scan Log
- Proactive Threat Protection System Log
- Proactive Threat Protection Threat Log
- Tamper Protection Log

**Note:** If you filter the log data in any way and then export it, you only export the data that you have currently filtered. This restriction is not true for the logs that you export to a tab-delimited text file. All the data in those logs is exported.

You can export the following logs to a tab-delimited .txt file:

- Client Management Control Log
- Client Management Security Log
- Client Management System Log
- Network Threat Protection Packet Log
Network Threat Protection Traffic Log

Note: In addition to a tab-delimited text file, you can also export the data from the Packet Log into network monitor format or NetXray format.

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

To export data to a .csv file
1 In the client, in the sidebar, click View logs.

2 Beside either Virus and Spyware Protection or Proactive Threat Protection, click View Logs.

3 Click the name of the log you want.

4 In the log window, make sure that the data that you want to save appears, and then click Export.

5 In the Save in drop-down list, browse to the directory where you want the file to be saved.

6 In the File name text box, type a name for the file.

7 Click Save.

8 Click OK.

To export Network Threat Protection log data or Client Management log data to text file
1 In the client, in the sidebar, click View logs.

2 To the right of Network Threat Protection or Client Management, click View Logs.

3 Click the name of the log you want to export data from.

4 Click File > Export.

   If you selected the Packet Log, you can click Export to network monitor format or Export to Netxray format instead.

5 In the Save in drop-down list, browse to the directory where you want the file to be saved.

6 In the File name text box, type a name for the file.

7 Click Save.

8 Click File > Exit.
Managing scans

This chapter includes the following topics:

- Managing scans on your computer
- How virus and spyware scans work
- Scheduling a user-defined scan
- Scheduling a scan to run on demand or when the computer starts up
- Managing Download Insight detections on your computer
- Customizing Download Insight settings
- Customizing virus and spyware scan settings
- Configuring actions for malware and security risk detections
- About excluding items from scans
- Excluding items from scans
- Managing quarantined files on your client computer
- About submitting information about detections to Symantec Security Response
- Submitting information about detections to Symantec Security Response
- About the client and the Windows Security Center
- Managing SONAR on your client computer

Managing scans on your computer

By default, a managed client runs an active scan every day at 12:30 P.M. An unmanaged client installs with a preset active scan that is disabled.
If you have an unmanaged client, you can manage your own scans. On a managed client, you might be able to configure your own scans, if your administrator made these settings available.

### Table 4-1  Managing scans

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read about how scans work</td>
<td>Review the types of scans and the types of viruses and security risks. See “How virus and spyware scans work” on page 57.</td>
</tr>
<tr>
<td>Update virus definitions</td>
<td>Make sure that you have the latest virus definitions installed on your computer. See “Updating the computer’s protection” on page 33.</td>
</tr>
<tr>
<td>Check that Auto-Protect is enabled</td>
<td>Auto-Protect is enabled by default. You should always keep Auto-Protect enabled. If you disable Auto-Protect, you also disable Download Insight and you prevent SONAR from making heuristic detections. See “Enabling or disabling Auto-Protect” on page 42.</td>
</tr>
<tr>
<td>Scan your computer</td>
<td>Regularly scan your computer for viruses and security risks. Ensure that scans run regularly by checking the last scan date. See “Scanning your computer immediately” on page 16. See “Scheduling a user-defined scan” on page 67.</td>
</tr>
</tbody>
</table>
Whenever an on-demand, scheduled, startup, or user-defined scan runs, by default Symantec Endpoint Protection displays a scan progress dialog box to report progress. In addition, Auto-Protect can display a results dialog whenever it detects a virus or security risk. You can disable these notifications.

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.

In managed networks, 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 “Pausing and delaying scans” on page 17.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pause or delay scans</td>
<td>Whenever an on-demand, scheduled, startup, or user-defined scan runs, by default Symantec Endpoint Protection displays a scan progress dialog box to report progress. In addition, Auto-Protect can display a results dialog whenever it detects a virus or security risk. You can disable these notifications.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>In managed networks, 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.</td>
</tr>
<tr>
<td></td>
<td>When a scan resumes, it starts from where the scan stopped.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you pause a scan while the client scans a compressed file, the client might take several minutes to respond to the pause request.</td>
</tr>
<tr>
<td></td>
<td>See “Pausing and delaying scans” on page 17.</td>
</tr>
</tbody>
</table>

| Interact with scan results   | 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.                                                      |
|                              | In a managed network, the scan progress dialog box might not appear for administrator-initiated scans. Your administrator may choose not to display results when the client detects a virus or security risk. In some cases, your administrator might let you view the scan results but not to pause or resume a scan. |
|                              | **Note:** The language of the operating system might not be able to interpret some characters in the virus names that appear in the scan results dialog box. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some unicode virus names might contain double-byte characters. On the computers that run the client on an English operating system, these characters appear as question marks. |
|                              | See “Responding to a virus or risk detection” on page 24.                                                                                                                                                  |
Table 4-1  Managing scans (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Adjust scans to improve your computer</td>
<td>By default, Symantec Endpoint Protection provides a high level of security while it minimizes the affect on your computer performance. You can customize settings to increase the computer performance even more.</td>
</tr>
<tr>
<td>performance</td>
<td>For scheduled and on-demand scans you can change the following options:</td>
</tr>
<tr>
<td></td>
<td>■ Scan tuning</td>
</tr>
<tr>
<td></td>
<td>Set the scan tuning to <strong>Best Application Performance</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ Compressed files</td>
</tr>
<tr>
<td></td>
<td>Change the number of levels to scan compressed files.</td>
</tr>
<tr>
<td></td>
<td>■ Resumable scans</td>
</tr>
<tr>
<td></td>
<td>You can specify a maximum time for a scan to run. The scan resumes when the computer is idle.</td>
</tr>
<tr>
<td></td>
<td>■ Randomized scans</td>
</tr>
<tr>
<td></td>
<td>You can specify that a scan randomizes its start time within a specific time interval.</td>
</tr>
<tr>
<td></td>
<td>You might also want to disable startup scans or change the schedule for your scheduled scans.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing virus and spyware scan settings” on page 75.</td>
</tr>
<tr>
<td></td>
<td>See “Scheduling a user-defined scan” on page 67.</td>
</tr>
</tbody>
</table>
### 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 run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to **Scan until finished**.

- **Insight Lookup**
  Insight Lookup uses the latest definition set to scan and make decisions about files. It also uses Symantec’s reputation technology. You should make sure that Insight Lookup is enabled. Insight Lookup settings are similar to the settings for Download Insight.

You can also 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 75.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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 run until the specified time interval expires and then resume when the client computer is idle. You can set the scan duration to **Scan until finished**.  
- **Insight Lookup**
  Insight Lookup uses the latest definition set to scan and make decisions about files. It also uses Symantec’s reputation technology. You should make sure that Insight Lookup is enabled. Insight Lookup settings are similar to the settings for Download Insight. You can also 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.  
<p>|</p>
<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Modify Auto-Protect settings to improve your</td>
<td>For Auto-Protect, you might want to change the following options:</td>
</tr>
</tbody>
</table>
| computer performance or increase protection    |  ■ 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 75.                                                                                                                                              |
| Manage Download Insight detections             | Download Insight inspects files that you try to download through Web browsers and text messaging clients and other portals. Download Insight uses reputation information from Symantec Insight to make decisions about files.                                                                 |
|                                                | See “Managing Download Insight detections on your computer” on page 71.                                                                                                                                  |
| Manage SONAR                                   | SONAR is part of Proactive Threat Protection.                                                                                                                                                             |
|                                                | See “Managing SONAR on your client computer” on page 91.                                                                                                                                                 |
| Identify scan exceptions                       | Exclude a safe file or process from being scanned.                                                                                                                                                       |
|                                                | See “Excluding items from scans” on page 82.                                                                                                                                                              |
### How virus and spyware scans work

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

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

See “How scans respond to a virus or risk detection” on page 65.

Table 4-2 describes the components that the client scans on your computer.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Selected files</td>
<td>The client scans individual files. For most types of scans, you select the files that you want scanned. The client software uses pattern-based scanning to search for traces of viruses within files. The traces of viruses are called patterns or signatures. Each file is compared to the innocuous signatures that are contained in a virus definitions file, as a way of identifying specific viruses. If a virus is found, by default the client tries to clean the virus from the file. If the file cannot be cleaned, the client quarantines the file to prevent further infection of your computer. The client also uses pattern-based scanning to search for signs of security risks within files and Windows registry keys. If a security risk is found, by default the client quarantines the infected files and repairs the risk's effects. If the client cannot quarantine the files, it logs the attempt.</td>
</tr>
<tr>
<td>Computer memory</td>
<td>The client searches the computer's memory. Any file virus, boot sector virus, or macro virus may be memory-resident. Viruses that are memory-resident have copied themselves into a computer's memory. In memory, a virus can hide until a trigger event occurs. Then the virus can spread to a floppy disk in the disk drive, or to the hard drive. If a virus is in memory, it cannot be cleaned. However, you can remove a virus from memory by restarting your computer when prompted.</td>
</tr>
<tr>
<td>Boot sector</td>
<td>The client checks the computer's boot sector for boot viruses. Two items are checked: the partition tables and the master boot record.</td>
</tr>
<tr>
<td>Floppy drive</td>
<td>A common way for a virus to spread is through the floppy disks. A floppy disk might remain in a disk drive when you start up or turn off your computer. When a scan starts, the client searches the boot sector and partition tables of a floppy disk that is located in the disk drive. When you turn off your computer, you are prompted to remove the disk to prevent possible infection.</td>
</tr>
</tbody>
</table>
About the types of scans

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

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

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

See “Managing scans on your computer” on page 51.

Table 4-3  Scan types

<table>
<thead>
<tr>
<th>Scan type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto-Protect     | Auto-Protect continuously inspects files and email data as they are written to or read from a computer. Auto-Protect automatically neutralizes or eliminates detected viruses and security risks.  
                 | Auto-Protect also protects some email that you might send or receive.  
                 | See “About the types of Auto-Protect” on page 60.                                                                                       |
| 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 reputation information to make decisions about files. The reputation scoring of files is determined by a Symantec technology called Insight. Insight uses not only the source of a file but also its context. Insight provides a security rating that Download Insight uses to make decisions about the files.  
                 | Download Insight functions as part of Auto-Protect and requires Auto-Protect to be enabled. If you disable Auto-Protect but enable Download Insight, Download Insight cannot function.  
                 | See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 66.                                   |
Table 4-3  Scan types (continued)

<table>
<thead>
<tr>
<th>Scan type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrator scans and user-defined scans</td>
<td>For managed clients, your administrator might create scheduled scans or run scans on demand. For unmanaged clients, or managed clients for which scan settings are unlocked, you can create and run your own scans. Administrator or user-defined scans detect viruses and security risks by examining all files and processes on the client computer. These types of scans can also inspect memory and load points. The following types of administrator or user-defined scans are available:</td>
</tr>
<tr>
<td>■ Scheduled scans</td>
<td>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 directories.</td>
</tr>
<tr>
<td>■ Startup scans and triggered scans</td>
<td>Startup scans run when the users log on to the computers. Triggered scans run when new virus definitions are downloaded to computers.</td>
</tr>
<tr>
<td>■ On-demand scans</td>
<td>On-demand scans are scans that you start manually. You can run scans on demand from the Scan for Threats page.</td>
</tr>
<tr>
<td>SONAR</td>
<td>SONAR 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. Like proactive threat scans, SONAR detects keyloggers, spyware, and any other application that might be malicious or potentially malicious.</td>
</tr>
</tbody>
</table>

About the types of Auto-Protect

Auto-Protect scans files as well as certain types of email and email attachments. If your client computer runs other email security products, such as Symantec Mail Security, you might not need to enable Auto-Protect for email. Auto-Protect works on your supported email client only. It does not protect email servers.
Note: If a virus is detected as you open email, your email may take several seconds to open while Auto-Protect completes its scan.

Table 4-4  Types of Auto-Protect

<table>
<thead>
<tr>
<th>Type of Auto-Protect</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auto-Protect</td>
<td>Continuously scans files as they are read from or written to your computer. Auto-Protect is enabled by default for the file system. It loads at computer startup. It inspects all files for viruses and security risks, and blocks the security risks from being installed. It can optionally scan files by file extension, scan files on remote computers, and scan floppies for boot viruses. It can optionally back up files before it attempts to repair the files, and terminate processes and stop services. You can configure Auto-Protect to scan only selected file extensions. When Auto-Protect scans the selected extensions, it can also determine a file's type even if a virus changes the file's extension. If you do not run Auto-Protect for email, your client computers are still protected when Auto-Protect is enabled. Most email applications save attachments to a temporary directory when users launch email attachments. Auto-Protect scans the file as it is written to the temporary directory 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.</td>
</tr>
<tr>
<td>Internet Email Auto-Protect</td>
<td>Scans internet email (POP3 or SMTP) and attachments for viruses and security risks; also performs outbound email heuristics scanning. By default, Internet Email Auto-Protect supports encrypted passwords and email over POP3 and SMTP connections. If you use POP3 or SMTP with Secure Sockets Layer (SSL), then the client detects secure connections but does not scan encrypted messages. <strong>Note</strong>: For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems. Internet email scanning also is not supported for 64-bit computers. Email scanning does not support IMAP, AOL, or HTTP-based email such as Hotmail or Yahoo! Mail.</td>
</tr>
</tbody>
</table>
### Table 4-4 Types of Auto-Protect (continued)

<table>
<thead>
<tr>
<th>Type of Auto-Protect</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Microsoft Outlook Auto-Protect** | Scans Microsoft Outlook email (MAPI and Internet) and attachments for viruses and security risks  
If Microsoft Outlook is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Microsoft Outlook Auto-Protect.  
If you use Microsoft Outlook over MAPI or Microsoft Exchange client and you have Auto-Protect enabled for email, attachments are immediately downloaded. The attachments are scanned when you open the attachment. If you download a large attachment over a slow connection, mail performance is affected. You may want to disable this feature if you regularly receive large attachments.  
**Note:** On a Microsoft Exchange server, you should not install Microsoft Outlook Auto-Protect. |
| **Lotus Notes Auto-Protect**  | Scans Lotus Notes email and attachments for viruses and security risks  
Supported for Lotus Notes 4.5x, 4.6, 5.0, and 6.x  
If Lotus Notes is already installed on the computer when you perform a client software installation, the client software detects the email application. The client automatically installs Lotus Notes Auto-Protect. |

### About viruses and security risks

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

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

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

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

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

See “How scans respond to a virus or risk detection” on page 65.

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

Table 4-5 lists the type of viruses and risks that can attack a computer
Table 4-5  Viruses and security risks

<table>
<thead>
<tr>
<th>Risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Viruses</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>The following types of threats are included in the virus category:</td>
</tr>
<tr>
<td></td>
<td>■ Malicious Internet bots</td>
</tr>
<tr>
<td></td>
<td>Programs that run automated tasks over the Internet. Bots can be used to automate attacks on computers or to collect information from Web sites.</td>
</tr>
<tr>
<td></td>
<td>■ Worms</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ Trojan horses</td>
</tr>
<tr>
<td></td>
<td>Programs that hide themselves in something benign, such as a game or utility.</td>
</tr>
<tr>
<td></td>
<td>■ Blended threats</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>■ Rootkits</td>
</tr>
<tr>
<td></td>
<td>Programs that hide themselves from a computer's operating system.</td>
</tr>
<tr>
<td>Adware</td>
<td>Programs that deliver advertising content.</td>
</tr>
<tr>
<td>Dialers</td>
<td>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.</td>
</tr>
<tr>
<td>Hacking tools</td>
<td>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.</td>
</tr>
<tr>
<td>Risk</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Joke programs</td>
<td>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 it.</td>
</tr>
<tr>
<td>Misleading applications</td>
<td>Applications that intentionally misrepresent the security status of a computer. These applications typically masquerade as security notifications about fake infections that must be removed.</td>
</tr>
<tr>
<td>Parental control programs</td>
<td>Programs that monitor or limit computer usage. The programs can run undetected and typically transmit monitoring information to another computer.</td>
</tr>
<tr>
<td>Remote access programs</td>
<td>Programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user’s computer.</td>
</tr>
<tr>
<td>Security assessment tool</td>
<td>Programs that are used to gather information for unauthorized access to a computer.</td>
</tr>
<tr>
<td>Spyware</td>
<td>Stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.</td>
</tr>
<tr>
<td>Trackware</td>
<td>Stand-alone or appended applications that trace a user's path on the Internet and send information to the controller or hacker's system.</td>
</tr>
</tbody>
</table>

**How scans respond to a virus or risk detection**

When viruses and security risks infect files, the client responds to the threat types in different ways. For each threat type, the client uses a first action, and then applies a second action if the first action fails.
Table 4-6 How a scan responds to viruses and security risks

<table>
<thead>
<tr>
<th>Threat type</th>
<th>Action</th>
</tr>
</thead>
</table>
| Virus             | By default, when the client detects a virus, the client:  
|                   | ■ Tries first to clean the virus from the infected file.  
|                   | ■ If the client cleans the file, the client completely removes the risk from your computer.  
|                   | ■ If the client cannot clean the file, it logs the failure and moves the infected file to the Quarantine.  
|                   | See “About quarantining files” on page 85.                                                                                           |
| Security risk     | By default, when the client detects a security risk:  
|                   | ■ It quarantines the infected file.  
|                   | ■ It tries to remove or repair any changes that the security risk made.  
|                   | ■ If the client cannot quarantine a security risk, it logs the risk and leaves it alone.  
|                   | In some instances, you might unknowingly install an application that includes a security risk such as adware or spyware. If Symantec has determined that quarantining the risk does not harm the computer, then the client quarantines the risk. If the client quarantines the risk immediately, its action might leave the computer in an unstable state. Instead, the client waits until the application installation is complete before it quarantines the risk. It then repairs the risk's effects. |

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

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

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

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

Insight determines a file's security rating by examining the following characteristics of the file and its context:
Scanning features in Symantec Endpoint Protection leverage Insight to make decisions about files and applications. Virus and Spyware Protection includes a feature that is called Download Insight. Download Insight relies on reputation information to make detections. If you disable Insight lookups, Download Insight runs but cannot make detections. Other protection features, such as Insight Lookup and SONAR, use reputation information to make detections; however, those features can use other technologies to make detections.

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

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

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

See “Managing Download Insight detections on your computer” on page 71.
See “Submitting information about detections to Symantec Security Response” on page 89.

Scheduling a user-defined scan

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

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

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

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

See “Scanning your computer immediately” on page 16.

See “Managing scans on your computer” on page 51.

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

To schedule a user-defined scan

1. In the client, in the sidebar, click Scan for threats.
2. Click Create a New Scan.
3. In the Create New Scan - What To Scan dialog box, select one of the following types of scans to schedule:
   - **Active Scan**: Scans the areas of the computer that viruses and security risks most commonly infect.
     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 impact your computer performance.
   - **Custom Scan**: Scans the selected areas of the computer for viruses and security risks.
4. Click Next.
5 If you selected **Custom Scan**, check the appropriate check boxes to specify where to scan, and then click **Next**.

The symbols have the following descriptions:

- The file, drive, or folder is not selected. If the item is a drive or folder, the folders and files in it are also not selected.
- The individual file or folder is selected.
- The individual folder or drive is selected. All items within the folder or drive are also selected.
- The individual folder or drive is not selected, but one or more items within the folder or drive are selected.

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

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

7 Click **Next**.

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

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

See “**Scheduling a scan to run on demand or when the computer starts up**” on page 70.
In the Create New Scan - Schedule dialog box, under Scan Schedule, specify the frequency and when to scan, and then click Next.

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

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

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

For example, call the scan: Friday morning

Click Finish.

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

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

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

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

See “Scanning your computer immediately” on page 16.

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

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

1 In the client, in the sidebar, click Scan for threats.
2 Click Create a New Scan.
3 Specify what to scan and any scan options for the scheduled scan.
   See “Scheduling a user-defined scan” on page 67.
4 In the Create New Scan - When to Run dialog box, do one of the following actions:
   - Click At startup.
■ Click On demand.

5 Click Next.

6 In the Create New Scan - Scan Name dialog box, type a name and description for the scan. For example, call the scan: MyScan1

7 Click Finish.

Managing Download Insight detections on your computer

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

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

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

Download Insight determines that a downloaded file might be a risk based on evidence about the file's reputation. Download Insight does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or SONAR scans the file when the user opens or runs the file.

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

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn how Download Insight uses reputation data to make decisions about files</td>
<td>Download Insight uses reputation information exclusively when it makes decisions about downloaded files. It does not use signatures or heuristics to make decisions. If Download Insight allows a file, Auto-Protect or SONAR scans the file when the user opens or runs the file. See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 66.</td>
</tr>
</tbody>
</table>
### Table 4-7 Managing Download Insight detections on your computer (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Respond to Download Insight detections</td>
<td>You might see notifications when Download Insight makes a detection. For managed clients, your administrator might choose 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 27.</td>
</tr>
</tbody>
</table>
| Create exceptions for specific files or Web domains | You can create an exception for an application that your users download. You can also create an exception for a specific Web domain that you believe is trustworthy.                                                                                           By default, Download Insight does not examine any files that users download from a trusted Internet or intranet site. Trusted sites are configured on the Windows Control Panel > Trusted Internet Sites > Security tab. When the
Automatically trust any file downloaded from an intranet site option is enabled, Symantec Endpoint Protection allows any file that a user downloads from one of the trusted sites. Download Insight recognizes only explicitly configured trusted sites. Wildcards are allowed, but non-routable IP address ranges are not supported. For example, Download Insight cannot recognize 10.*.*.* as a trusted site. Download Insight also does not support the sites that are discovered by the Internet Options > Security > Automatically detect intranet network option. See “Excluding items from scans” on page 82. |
<p>| Make sure that Insight lookups are enabled  | Download Insight requires reputation data to make decisions about files. If you disable Insight lookups, Download Insight runs but cannot make detections. Insight lookups are enabled by default. See “Submitting information about detections to Symantec Security Response” on page 89.                                                                                                                                                                                                                     |</p>
<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customize Download Insight settings</td>
<td>You might want to customize Download Insight settings for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ 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.</td>
</tr>
<tr>
<td></td>
<td>■ Get alerts about Download Insight detections. When Download Insight detects a file that it considers malicious, it displays a message on the client computer if the action is set to Quarantine. You can undo the quarantine action. When Download Insight detects a file that it considers unproven, it displays a message on the client computer if you set the action for unproven files to Prompt or Quarantine. When the action is set to Prompt, you can allow or block the file. When the action is Quarantine, you can undo the quarantine action. You can turn off user notifications so that you do not have a choice when Download Insight detects a file that it considers unproven. If you keep notifications enabled, you can set the action for unproven files to Ignore so that these detections are always allowed and you are not notified. When notification 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.</td>
</tr>
<tr>
<td></td>
<td>See “Customizing Download Insight settings” on page 74.</td>
</tr>
<tr>
<td>Submit information about reputation</td>
<td>By default, clients send information about reputation detections to Symantec. Symantec recommends that you enable submissions for reputation detections. The information helps Symantec address threats.</td>
</tr>
<tr>
<td>detections to Symantec</td>
<td>See “Submitting information about detections to Symantec Security Response” on page 89.</td>
</tr>
</tbody>
</table>
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 notifications that Download Insight displays on client computers when it makes a detection.

See “Managing Download Insight detections on your computer” on page 71.

Customizing Download Insight settings

1. In the client, in the sidebar, click Change Settings.
2. Next to Virus and Spyware Protection, click Configure Settings.
3. On the Download Insight tab, make sure that Enable Download Insight to detect potential risks in downloaded files based on file reputation is checked.
   If Auto-Protect is disabled, Download Insight cannot function even if it is enabled.
4. Move the slider to change the malicious file sensitivity.

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

   If you set the level higher, Download Insight detects more files as malicious and fewer files as unproven. Higher settings, however, return more false positives.

5. Check or uncheck the following options to use as additional criteria for examining unproven files:
   - **Files with fewer than x users**
   - **Files known by users for less than x days**
     When unproven files meet this criteria, Download Insight detects the files as malicious.

6. Make sure that Automatically trust any file downloaded from an intranet website is checked.
   This option also applies to Insight Lookup detections.

7. Click Actions.

8. Under Malicious Files, specify a first action and a second action.

9. Under Unproven Files, specify the action.
10  Click OK.

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

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

12  Click OK.

Customizing virus and spyware scan settings

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

See “Managing scans on your computer” on page 51.

To customize a user-defined scan

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

2  In the Scan for threats page, right-click a scan and click Edit.

3  On the Scan Options tab, do any of the following tasks:

   ■ To change Insight Lookup settings, click Insight Lookup.
     Insight Lookup settings are similar to Download Insight settings.
     See “Customizing Download Insight settings” on page 74.

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

   ■ To specify which a first and second action that the client takes on an infected file, click Actions.

   ■ To specify notification options, click Notifications.

   ■ To configure advanced options for compressed files, backups, and tuning, click Advanced.
     You might want to change the tuning options to improve your client computer performance.

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

4  Click OK.

To change global scan settings

1  Do one of the following actions:

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

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

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

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

5. Click **OK**.

**To customize Auto-Protect**

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

2. Next to Virus and Spyware Protection, click **Configure Settings**.

3. On any Auto-Protect tab, do the following tasks:
   - To specify fewer file types to scan, click **Selected**, and then click **Extensions**.
   - To specify which a first and 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 padlock 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 75.
See “Customizing Download Insight settings” on page 74.
See “Changing SONAR settings” on page 94.

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

To configure actions for malware and security risk detections

1 In the client, in the sidebar, click Change settings or Scan for Threats.

2 Do one of the following actions:

   ■ Next to Virus and Spyware Protection, click Configure Settings, and then on any Auto-Protect tab, click Actions.

   ■ Select a scan and then right-click and select Edit, and then click Scan Options.

3 Click Actions.

4 In the Scan Actions dialog box, in the tree, select the category or subcategory under Malware or Security Risks.

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

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

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

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

Note: There might be a single subcategory under a category, depending on how Symantec currently classifies risks. For example, under Malware, there might be a single subcategory called Viruses.
Check Override actions configured for Security Risks, and then set the actions for that subcategory only.
Select a first and second action from the following options:

**Clean risk**
- Removes the virus from the infected file. This setting is the default first action for viruses.

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

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

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

  By default, the client backs up the file.

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

  Some infected files cannot be cleaned.

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

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

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

  Quarantine contains a record of all the actions that were performed. You can return the computer to the state that existed before the client removed the risk.
Delete risk  Deletes the infected file from your computer’s hard drive. If the client cannot delete a file, information about the action that the client performed appears in the Notification dialog box. The information also appears in the Event Log.

Use this action only if you can replace the file with a backup copy that is free of viruses or security risks. When the client deletes a risk, it deletes the risk permanently. The infected file cannot be recovered from the Recycle Bin.

**Note:** Use this action with caution when you configure actions for security risks. In some cases, deleting security risks can cause applications to lose functionality.

Leave alone (log only)  Leaves the file as is.

If you use this action for viruses, the virus remains in the infected files. The virus can spread to other parts of your computer. An entry is placed in the Risk History to keep a record of the infected file.

You can use Leave alone (log only) as a second action for both malware and security risks.

Do not select this action when you perform large-scale, automated scans, such as scheduled scans. You might want to use this action if you intend to view the scan results and take an additional action later. An additional action might be to move the file to the Quarantine.

For security risks, this action leaves the infected file as is and places an entry in the Risk History to keep a record of the risk. Use this option to take manual control of how the client handles a security risk. This setting is the default second action for security risks.

Your administrator might send a customized message that explains how to respond.

7 Repeat steps these steps for each category for which you want to set specific actions, and then click **OK**.

8 If you selected a security risk category, you can select custom actions for one or more specific instances of that security risk category. You can exclude a security risk from scanning. For example, you might want to exclude a piece of adware that you need to use in your work.

9 Click **OK**.
About excluding items from scans

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

For managed clients, your administrator may have created exceptions for your scans. If you create an exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence. Your administrator can also prevent you from configuring any or all types of exceptions.

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

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

See “Excluding items from scans” on page 82.
Excluding items from scans

Exceptions are known security risks, files, folders, file extensions, Web domains, or applications that you want to exclude from scans. If you have scanned your computer and know that certain files are safe, you can exclude them. In some cases, exceptions can reduce scan time and increase system performance. 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.

Security risk exceptions apply across all security risk scans. Application exceptions apply to all security risk scans as well. SONAR folder exceptions apply only to SONAR.

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

See “Managing scans on your computer” on page 51.

See “About excluding items from scans” on page 81.

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

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

To exclude items from security risk scans

1  In the client, in the sidebar, click Change settings.
2  Next to Exceptions, click Configure Settings.
3  In the Exceptions dialog box, under User-defined Exceptions, click Add > Security Risk Exceptions.
4  Select one of the following exception types:
   ■  Known Risks
   ■  File
   ■  Folder
   ■  Extensions
   ■  Web Domain
5  Do one of the following actions:
For known risks, check the security risks that you want to exclude from scans.
If you want to log an event when the security risk is detected and ignored, check **Log when the security risk is detected**.

- For files or folders, select the file or folder that you want to exclude, and then click **Add**.
  For folders, check or uncheck **Include subfolders**.

- For extensions, type the extension that you want to exclude.
  You can only include one extension name in the text box. If you type multiple extensions, the client treats the entry as a single extension name.

- For domains, enter a Web site that you want to exclude from Download Insight detection.

6 Click **OK**.
7 In the **Exceptions** dialog box, click **Close**.

**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 **Add**.
  If you select a file instead of a folder, the client uses the parent folder for the exception.
5 In the **Exceptions** dialog box, click **Close**.

**To change how all scans handle an application**
1 In the client, in the sidebar, click **Change settings**.
2 Next to **Exceptions**, click **Configure Settings**.
3 In the **Exceptions** dialog box, under **User-defined Exceptions**, click **Add > Application Exception**.
4 Select the filename of the application
5 In the **Action** drop-down box, select **Ignore**, **Log Only**, **Quarantine**, or **Terminate**.
6 Click **Add**.
7 In the **Exceptions** dialog box, click **Close**.
Managing quarantined files on your client computer

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

See “About quarantining files” on page 85.

### Table 4-9  Managing quarantined files on your client computer

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restore a quarantined file to its original location</td>
<td>Occasionally, a clean file does not have a location to which to be returned. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. You must release the file and specify a location.</td>
</tr>
<tr>
<td>Manually quarantine an item</td>
<td>You can manually quarantine a file by adding it to the Quarantine or by selecting the file from the virus and spyware or SONAR logs. See “Quarantining a file from the Risk or Scan Log” on page 86.</td>
</tr>
<tr>
<td>Permanently delete files from the Quarantine</td>
<td>You can manually delete the files that you no longer need from the Quarantine. You can also set up a time period by which files are deleted automatically. Note: Your administrator may specify a maximum number of days that items are allowed to stay in the Quarantine. Items are automatically deleted from the Quarantine after that time limit.</td>
</tr>
<tr>
<td>Rescan files in the Quarantine after you receive new definitions</td>
<td>When you update definitions, files in the Quarantine might get scanned, cleaned, and restored automatically. For some files, the Repair Wizard appears. Follow the on-screen instructions to complete the rescan and repair. You can also rescan virus-infected files in the Quarantine manually.</td>
</tr>
<tr>
<td>Export Quarantine information</td>
<td>You can export the contents of the Quarantine to either a comma-delimited (.csv) file or a Microsoft Access Database (.mdb) file.</td>
</tr>
</tbody>
</table>
### Table 4-9  
Managing quarantined files on your client computer (continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Submit infected files in the Quarantine to Symantec Security Response | After items in the Quarantine are rescanned, you might want to submit a file that is still infected to Symantec Security Response for further analysis. 
See “Manually submitting a potentially infected file to Symantec Security Response for analysis” on page 86. |
| Clear backup items | Before trying to clean or repair items, the client makes backup copies of infected items by default. After the client successfully cleans a virus, you should manually delete the item from the Quarantine because the backup is still infected. |
| Automatically delete files from the Quarantine | You can set up the client to automatically remove items from the Quarantine after a specified time interval. You can also specify that the client removes items when the folder where the items are stored reaches a certain size. This configuration prevents the buildup of files that you may forget to remove manually from these areas. 
See “Automatically deleting files from the Quarantine” on page 87. |

---

### About quarantining files

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

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

Viruses can be quarantined. Boot viruses reside in the boot sector or partition tables of a computer; these items cannot be moved to the Quarantine. Sometimes the client detects an unknown virus that cannot be eliminated with the current set of virus definitions. If you have a file that you believe is infected but scans do not detect an infection, you should quarantine the file.
Note: The language of the operating system on which you run the client might not be able to interpret some characters in risk names. If the operating system cannot interpret the characters, the characters appear as question marks in notifications. For example, some unicode risk names might contain double-byte characters. On those computers that run the client on an English operating system, these characters appear as question marks.

See “Managing quarantined files on your client computer” on page 84.

Quarantining a file from the Risk or Scan Log

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

See “About quarantining files” on page 85.

To quarantine a file from the Risk Log or Scan Log

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

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

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

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

See “Managing quarantined files on your client computer” on page 84.
To submit a file to Symantec Security Response from the Quarantine

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

Automatically deleting files from the Quarantine

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

See “Managing quarantined files on your client computer” on page 84.

To automatically delete files from the Quarantine

1. In the client, in the sidebar, click View Quarantine.
2. Click Purge Options.
3. In the Purge Options dialog box, select one of the following tabs:
   - Quarantine Items
   - Backup Items
   - Repaired Items
4. Check or uncheck Length of time stored exceeds to enable or disable the ability of the client to delete the files after the configured time expires.
5. If you check the Length of time stored exceeds check box, type or click an arrow to enter the amount of time.
6. Select the unit of time from the drop-down list. The default is 30 days.
7. If you check the Total folder size exceeds check box, type in the maximum folder size to allow, in megabytes. The default is 50 megabytes.
   
   If you check both check boxes, all files that are older than the time that you have set are deleted first. If the size of the folder still exceeds the limit that you set, the client deletes the oldest files individually. The client deletes the oldest files until the folder size does not exceed the limit.
8. Repeat steps 4 through 7 for any of the other tabs.
9. Click OK.
About submitting information about detections to Symantec Security Response

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

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

See “About the Symantec Endpoint Protection client” on page 11.

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

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

■ Antivirus detections
  Information about virus and spyware scan detections.

■ Antivirus advanced heuristic detections
  Information about potential threats detected by Bloodhound and other virus and spyware scan heuristics.
  These detections are silent detections that do not appear in the Risk log.
  Information about these detections is used for statistical analysis.

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

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

You can also manually submit a sample to Response from the Quarantine.

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

See “How Symantec Endpoint Protection uses reputation data to make decisions about files” on page 66.

See “About the files and applications that SONAR detects” on page 93.
Submitting information about detections to Symantec Security Response

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

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

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

See “Managing quarantined files on your client computer” on page 84.


To configure submissions to Symantec Security Response

1 Select Change Settings > Client Management.

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

Symantec recommends that you keep this option enabled.

3 Select the types of information to submit:

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

- Antivirus detections
  Information about virus and spyware scan detections.

- Antivirus advanced heuristic detections
  Information about the potential threats that are detected by Bloodhound and other virus and spyware scan heuristics.
These detections are silent detections that do not appear in the Risk log. Information about these detections is used for statistical analysis.

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

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

4 Enable **Allow Insight lookups for threat detection** to allow Symantec Endpoint Protection to use Symantec’s reputation database to make decisions about threats.

Insight lookups are enabled by default. Symantec recommends that you allow Insight lookups. Disabling this feature disables the Download Insight and may impair the functionality of SONAR and Insight Lookup.

However, you can disable this option if you do not want to allow Symantec to query Symantec Insight.

### About the client and the Windows Security Center

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

Table 4-10 shows the protection status reporting in WSC.

**Table 4-10**  
WSC protection status reporting

<table>
<thead>
<tr>
<th>Symantec product condition</th>
<th>Protection status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection is not installed</td>
<td>NOT FOUND (red)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed with full protection</td>
<td>ON (green)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed, and virus and security risk definitions are out of date</td>
<td>OUT OF DATE (red)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed and Auto-Protect for the file system is not enabled</td>
<td>OFF (red)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed, Auto-Protect for the file system is not enabled, and virus and security risk definitions are out of date</td>
<td>OFF (red)</td>
</tr>
</tbody>
</table>
Table 4-10  WSC protection status reporting (continued)

<table>
<thead>
<tr>
<th>Symantec product condition</th>
<th>Protection status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection is installed and Rtvscan is turned off manually</td>
<td>OFF (red)</td>
</tr>
</tbody>
</table>

Table 4-11 shows the Symantec Endpoint Protection firewall status reporting in WSC.

Table 4-11  WSC firewall status reporting

<table>
<thead>
<tr>
<th>Symantec product condition</th>
<th>Firewall status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec firewall is not installed</td>
<td>NOT FOUND (red)</td>
</tr>
<tr>
<td>Symantec firewall is installed and enabled</td>
<td>ON (green)</td>
</tr>
<tr>
<td>Symantec firewall is installed but not enabled</td>
<td>OFF (red)</td>
</tr>
<tr>
<td>Symantec firewall is not installed or enabled, but a third-party firewall is installed and enabled</td>
<td>ON (green)</td>
</tr>
</tbody>
</table>

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

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

Managing SONAR on your client computer

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

See “Managing scans on your computer” on page 51.

See “About the types of scans” on page 59.
### Table 4-12  Managing SONAR on your client computer

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make sure that SONAR is enabled</td>
<td>For the best protection on your client computer, SONAR should be enabled. SONAR is enabled by default. You enable SONAR by enabling Proactive Threat Protection. See “About enabling and disabling protection” on page 40.</td>
</tr>
<tr>
<td>Make sure that Insight lookups are enabled</td>
<td>SONAR uses reputation data in addition to heuristics to make detections. If you disable Insight lookups (reputation queries), SONAR makes detections by using heuristics only. The rate of false positives might increase, and the protection that SONAR provides is limited. See “Submitting information about detections to Symantec Security Response” on page 89.</td>
</tr>
<tr>
<td>Change SONAR settings</td>
<td>You can enable or disable SONAR. You can also change the detection action for some types of threats that SONAR detects. You might want to change the detection action to reduce false positive detections. See “Changing SONAR settings” on page 94.</td>
</tr>
<tr>
<td>Create exceptions for applications that you know are safe</td>
<td>SONAR might detect the files or the applications that you want to run on your computer. You can create exceptions for the applications or folders. You can also create an exception from the Quarantine. See “Excluding items from scans” on page 82.</td>
</tr>
</tbody>
</table>
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 complement your existing Virus and Spyware Protection, intrusion prevention, and firewall protection.

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

See “Managing SONAR on your client computer” on page 91.

See “About the files and applications that SONAR detects” on page 93.

About the files and applications that SONAR detects

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.

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:

<table>
<thead>
<tr>
<th>Heuristic threats</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>System changes</td>
<td>SONAR detects applications or the files that try to modify DNS settings or a host file on a client computer.</td>
</tr>
</tbody>
</table>
Some good trusted files might be associated with suspicious behavior. SONAR detects these files as suspicious behavior events. For example, a well-known document sharing application might create executable files.

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

See “Managing SONAR on your client computer” on page 91.

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.

See “Managing SONAR on your client computer” on page 91.

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

To change SONAR settings

1 In the client, in the sidebar, click Change settings.
2 Next to Proactive Threat Protection, click Configure Settings
3 On the SONAR tab, change the actions for high risk or low risk heuristic threats.
   You can enable aggressive mode for low risk detections. This setting increases SONAR sensitivity to low risk detections. It might increase the false positive detections.
4 Optionally, change the notification settings.
5 On the Suspicious Behavior Detection tab, change the action for high risk or low risk detections. SONAR makes these detections when trusted files are associated with suspicious behavior.
6 On the System Change Events tab, change the scan action for detections of changes to the DNS server settings or a host file.
7 Click OK.
Managing the firewall and intrusion prevention

This chapter includes the following topics:

- About Network Threat Protection
- Managing firewall protection
- Configuring firewall settings
- About allowing or blocking applications
- Viewing network activity
- About client firewall rules
- About the firewall rule, firewall setting, and intrusion prevention processing order
- Changing the order of firewall rules
- How the firewall uses stateful inspection
- The elements of a firewall rule
- Setting up firewall rules
- Managing intrusion prevention
- How intrusion prevention works
- Enabling or disabling intrusion prevention
- Configuring intrusion prevention notifications
About Network Threat Protection

The Symantec Endpoint Protection client provides Network Threat Protection, which monitors the information that comes in and out of your computer and blocks network attack attempts.

Table 5-1 describes the Symantec Endpoint Protection features that you can use to manage Network Threat Protection.

Table 5-1   Network Threat Protection features

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
</table>
| Firewall                       | The firewall protects unauthorized users from accessing your computer and the networks that connect to the Internet. The firewall detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic. The firewall allows or blocks inbound and outbound traffic.  
See “How a firewall works” on page 98.  
See “Managing firewall protection” on page 96. |
| Intrusion Prevention System    | The Intrusion Prevention System (IPS) automatically detects and blocks network attacks. The IPS scans every packet that enters and exits a computer for attack signatures.  
The IPS relies on an extensive list of attack signatures to detect and block suspicious network activity. Symantec supplies the known threat list, which you can update on the client by using Symantec LiveUpdate. The Symantec IPS engine and corresponding set of IPS signatures are installed on the client by default.  
See “How intrusion prevention works” on page 125.  
See “Managing intrusion prevention” on page 124. |

Managing firewall protection

By default, the firewall allows all incoming network traffic and outgoing network traffic. You can configure the firewall to allow or block specific types of traffic.

Your administrator determines the level of interaction that you have with the client by permitting your ability to configure firewall rules and settings. Your administrator can restrict your use such that you can only interact with the client when it notifies you of new network connections and possible problems. Or your administrator can permit you full access to the user interface.
Table 5-2 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>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read about how the firewall works</td>
<td>Learn how the firewall protects your computer from network attacks. See “How a firewall works” on page 98.</td>
</tr>
<tr>
<td>Configure firewall settings</td>
<td>In addition to creating firewall rules, you can also enable and configure firewall settings to further enhance your firewall protection. See “Configuring firewall settings” on page 99.</td>
</tr>
<tr>
<td>View firewall logs</td>
<td>You can regularly check the firewall protection status on your computer to determine the following:</td>
</tr>
<tr>
<td></td>
<td>■ The firewall rules that you created work correctly.</td>
</tr>
<tr>
<td></td>
<td>■ The client blocked any network attacks.</td>
</tr>
<tr>
<td></td>
<td>■ The client blocked any applications that you expected to run.</td>
</tr>
<tr>
<td></td>
<td>You can use the Traffic Log and the Packet Log to check the firewall protection status.</td>
</tr>
<tr>
<td></td>
<td>See “About the logs” on page 45.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> By default, the Packet log is disabled on managed clients.</td>
</tr>
<tr>
<td>Configure application settings</td>
<td>You can enhance protection for your computer by customizing application settings. An application is a software program designed to help the user perform a task. For example, Microsoft Internet Explorer is an application. You can configure firewall settings to control the applications that can access the network. See “About allowing or blocking applications” on page 110.</td>
</tr>
<tr>
<td>Monitor network activity</td>
<td>You can view information about inbound traffic and outbound traffic from the client. You can also view a list of applications and services that have run since the client service started. See “Viewing network activity” on page 114.</td>
</tr>
</tbody>
</table>
**Table 5-2  Managing firewall protection (continued)**

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
</table>
| Add and customize firewall rules  | In addition to enabling firewall settings, you can modify the default firewall rules to further customize your firewall protection. You can also create new 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 “[About client firewall rules](#)” on page 115.  
See “[Setting up firewall rules](#)” on page 121.  
See “[Enabling and disabling firewall rules](#)” on page 123. |
| Enable or disable the firewall     | You can disable Network Threat Protection temporarily for troubleshooting purposes. For example, you might need to disable it so that you can open a certain application.  
See “[Enabling or disabling protection on the client computer](#)” on page 41. |

See “[About Network Threat Protection](#)” on page 96.

**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 computers
- Warns you of connection attempts from other computers
- Warns you of connection attempts by the applications on your computer that connect to other computers

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

Packets contain information about the following:

- Sending computers
- Intended recipients
How the packet data is processed

Ports that receive the packets

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

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

See “About Network Threat Protection” on page 96.

See “Managing firewall protection” on page 96.

## Configuring firewall settings

Table 5-3 describes the types of firewall settings that you can configure to further customize your firewall protection.

Your administrator has not given you the appropriate permissions to configure these settings if they do not appear in the user interface or cannot be modified. Modification of firewall settings is optional and can be done in any order.

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Traffic and stealth Web browsing</td>
<td>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. See “Enabling traffic settings and stealth Web browsing settings” on page 100.</td>
</tr>
</tbody>
</table>
Table 5-3  Firewall settings (continued)

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
</table>
| 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.  
  See “Automatically allowing communications for essential network services” on page 105. |
| Network file and print sharing         | You can enable the client to either share its files or to browse for shared files and printers on your local network. To prevent network-based attacks, you can disable network file and printer sharing.  
  See “Enabling network file and printer sharing” on page 106. |
| Block an attacking computer           | When the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an active response. 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.  
  See “Blocking and unblocking an attacking computer” on page 108. |

See “About client firewall rules” on page 115.

See “Setting up firewall rules” on page 121.

Enabling traffic settings and stealth Web browsing settings

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.
After the firewall has completed certain operations, control is passed to a number of components. Each component is designed to perform a different type of packet analysis.

To enable traffic settings and stealth Web browsing settings

1. In the client, in the sidebar, click Change settings.
3. On the Firewall tab, under Traffic Settings, check the boxes for the features that you want to enable as follows:

   Enable NetBIOS protection
   - Blocks the NetBIOS traffic from an external gateway.
   - You can use Network Neighborhood file and printer sharing on a LAN and protect a computer from NetBIOS exploits from any external network. This option blocks the NetBIOS packets that originate from the IP addresses that are not part of the defined ICANN internal ranges. ICANN internal ranges include 10.x.x.x, 172.16.x.x, 192.168.x.x, and 169.254.x.x, with the exception of the 169.254.0.x and 169.254.255.x subnets. The NetBIOS packets include UDP 88, UDP 137, UDP 138, TCP 135, TCP 139, TCP 445, and TCP 1026.
   - Note: The NetBIOS protection can cause a problem with Microsoft Outlook if the client computer connects to a Microsoft Exchange Server that is on a different subnet. You can create a firewall rule that specifically allows access to that server.

   Allow token ring traffic
   - Allows the client computers that connect through a token ring adapter to access the network, regardless of the firewall rules on the client.
   - If you disable this setting, any traffic that comes from the computers that connect through a token ring adapter cannot access the corporate network. The firewall does not filter token ring traffic. It either allows all token ring traffic or blocks all token ring traffic.
Enable anti-MAC spoofing | Allows the inbound and the outbound ARP (address resolution protocol) traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the Security log.

Some hackers use MAC spoofing to try to hijack a communication session between two computers. Media Access Control (MAC) addresses are the hardware addresses that identify the computers, the servers, the routers, and so forth. When computer A wants to communicate with computer B, it may send an ARP packet to the computer.

Anti-MAC spoofing protects a computer from letting another computer reset a MAC address table. If a computer sends an ARP REQUEST message, the client allows the corresponding ARP RESPOND message within a period of 10 seconds. All client rejects all unsolicited ARP RESPOND messages.

Enable network application monitoring | Allows the client to monitor changes to the network applications that run on the client computer.

Network applications send and receive traffic. The client detects whether an application's content changes.

Block all traffic until the firewall starts and after the firewall stops | Blocks all inbound traffic to and outbound traffic from the client computer when the firewall does not run for any reason.

The computer is not protected when either of the following events occur:

- After the client computer turns on and before the firewall service starts
- After the firewall service and client computer stop

This time frame is a small security hole that can allow unauthorized communication. This setting prevents unauthorized applications from communicating with other computers.

Note: When Network Threat Protection is disabled, the client ignores this setting.
Enable denial of service detection

When this setting is enabled, Symantec Endpoint Protection identifies known attacks based on multiple packets, regardless of the port number or type of Internet protocol.

The inability to provide this type of detection is a limitation of a signature-based intrusion detection and prevention system.

Enable port scan detection

When this setting is enabled, Symantec Endpoint Protection monitors all incoming packets that any security rule blocks. If a rule blocks several different packets on different ports in a short period of time, Symantec Endpoint Protection creates a Security log entry.

Port scan detection does not block any packets. You must create a security policy to block traffic when a port scan occurs.

4 Under Unmatched IP Traffic Settings, check the boxes for the features that you want to enable.

These options control the incoming IP traffic and outgoing IP traffic that does not match any firewall rules. IP traffic includes the data packets that flow through IP networks and that use the TCP, UDP, and ICMP protocols. Applications, mail exchanges, file transfers, ping programs, and Web transmissions are types of IP traffic.

You can enable one or more of the following IP traffic settings:

Allow IP traffic

Allows any incoming traffic and outgoing traffic, unless a firewall rule states otherwise. For example, if you add a firewall rule that blocks VPN traffic, the firewall allows all other traffic except for the VPN traffic.

Allow only application traffic

Allows the traffic to and from applications and blocks the traffic that is not associated with any application. For example, the firewall allows Internet Explorer but blocks VPN traffic, unless a rule states otherwise.

Prompt before allowing application traffic

Displays a message that asks you whether to allow or block an application. For example, you may want to choose whether or not to block media files. Or, you may want to hide broadcasts from the NTOSKRNL.DLL process. The NTOSKRNL.DLL process can be an indication of spyware, because spyware often downloads and installs the NTOSKRNL.DLL process.
5 Under **Stealth Settings**, check the boxes for the features that you want to enable as follows:

**Enable TCP resequencing**

Prevents an intruder from forging or spoofing an individual’s IP address.

Hackers use IP spoofs to hijack a communication session between two computers, such as computer A and B. A hacker can send a data packet that causes computer A to drop the communication. Then the hacker can pretend to be computer A and communicate with and attack computer B. To protect the computer, TCP resequencing randomizes TCP sequence numbers.

**Note:** OS fingerprint masquerading works best when TCP resequencing is enabled.

**Warning:** TCP resequencing changes the TCP sequencing number when the client service runs. The sequencing number is different when the service runs and when the service does not run. Therefore, the network connections are terminated when you stop or start the firewall service. TCP/IP packets use a sequence of session numbers to communicate with other computers. When the client does not run, the client computer uses the Windows number scheme. When the client runs and TCP resequencing is enabled, the client uses a different number scheme. If the client service suddenly stops, the number scheme reverts back to the Window number scheme and Windows then drops the traffic packets. Furthermore, TCP resequencing may have a compatibility issue with certain NICs that causes the client to block all inbound traffic and outbound traffic.
Enable stealth mode Web browsing

Detects the HTTP traffic from a Web browser on any port and removes the following information: the browser name and version number, the operating system, and the reference Web page. It stops Web sites from knowing which operating system and browser the computer uses. It does not detect HTTPS (SSL) traffic.

**Warning:** Stealthmode Web browsing may cause some Web sites not to function properly. Some Web servers build a Web page that is based on information about the Web browser. Because this option removes the browser information, some Web pages may not appear properly or at all. Stealth mode Web browsing removes the browser signature, called the HTTP_USER_AGENT, from the HTTP request header and replaces it with a generic signature.

Enable OS fingerprint masquerading

Prevents the detection of the operating system of a client computer. The client changes the TTL and identification value of TCP/IP packets to prevent the identification of an operating system.

**Note:** OS fingerprint masquerading works best when TCP resequencing is enabled.

**Warning:** TCP resequencing may have a compatibility issue with certain NICs that causes the client to block all inbound traffic and outbound traffic.

6 Click **OK**.

See “**Configuring firewall settings**” on page 99.

See “**Blocking traffic**” on page 109.

**Automatically allowing communications for essential network services**

Symantec Endpoint Protection provides built-in the 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.
Built-in rules filters allow the packet if a request was made. They do not block packets. The firewall rules allow or block packets.

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

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

3. On the **Firewall** tab under **Built-in Rules** check one or more of the following options:
   - Enable Smart DHCP
   - Enable Smart DNS
   - Enable Smart WINS

4. Click **OK**.

See “**Enabling traffic settings and stealth Web browsing settings**” on page 100.

See “**Configuring firewall settings**” on page 99.

Enabling network file and printer sharing

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

You can enable network file and print sharing in the following ways:

- **Automatically enable the network file and printer sharing settings on the Microsoft Windows Networking tab.**
  
  If a firewall rule blocks this traffic, the firewall rule takes priority over the settings.

  To automatically enable network file and print sharing

- **Manually enable network file and printer sharing by adding firewall rules.**
  
  You can add the firewall rules if you want more flexibility than what the settings provide. For example, when you create a rule, you can specify a particular host rather than all hosts. The firewall rules allow access to the ports to browse and share files and printers.

  You can create one set of firewall rules so that the client can share its files. You create a second set of firewall rules so that the client can browse for other files and printers.

  To manually enable clients to browse for files and printers

  To manually enable other computers to browse files on the client
To automatically enable network file and print sharing

1. In the client, in the sidebar, click Change settings.
3. On the Microsoft Windows Networking tab under Settings, click the drop-down menu and select the adapter for which these settings apply.
4. To browse other computers and printers in the network, click Browse files and printers on the network.
5. To enable other computers to browse files on your computer, click Share my files and printers with others on the network.
6. Click OK.

To manually enable clients to browse for files and printers

1. In the client, in the sidebar, click Status.
2. Beside NetworkThreat Protection, click Options > Configure Firewall Rules.
3. In the Configure Firewall Rules dialog box, click Add.
4. On the General tab, type a name for the rule and click Allow this traffic.
5. On the Ports and Protocols tab, in the Protocol drop-down list, click TCP.
7. Click OK.

8. In the Configure Firewall Rules dialog box, click Add.
9. On the General tab, type a name for the rule and click Allow this traffic.
10. On the Ports and Protocols tab, in the Protocol drop-down list, click UDP.
11. In the Remote ports drop-down list, type 88.
12. In the Local ports drop-down list, type 137, 138.
13. Click OK.

To manually enable other computers to browse files on the client

1. In the client, in the sidebar, click Status.
2. Beside NetworkThreat Protection, click Options > Configure Firewall Rules.
3. In the Configure Firewall Rules dialog box, click Add.
4. On the General tab, type a name for the rule and click Allow this traffic.
5. On the Ports and Protocols tab, in the Protocol drop-down list, click TCP.
6. In the Local ports drop-down list, type 88, 135, 139, 445.
7 Click OK.
8 In the Configure Firewall Rules dialog box, click Add.
9 On the General tab, type a name for the rule and click Allow this traffic.
10 On the Ports and Protocols tab, in the Protocol drop-down list, click UDP.
11 In the Local ports drop-down list, type 88, 137, 138.
12 Click OK.

See “Configuring firewall settings” on page 99.

Blocking and unblocking an attacking computer

When the Symantec Endpoint Protection client detects a network attack, it can automatically block the connection to ensure that the client computer is safe. The client activates an active response, which automatically blocks all communication to and from the IP address of the attacking computer for a set period of time. The IP address of the attacking computer is blocked for a single location.

You can view the IP address of the attacking computer in the security log. You can also unblock an attack by stopping the active response in the security log.

If you do not want to wait the default amount of time to unblock the IP address, you can unblock it immediately.

To block an attacking computer

1 In the client, in the sidebar, click Change settings.
2 Beside Network Threat Protection, click Configure Settings.
3 On the Firewall tab under Active Response Settings, check Number of seconds to automatically block an attacker's IP address, and then enter the number of seconds..

   Enter a number from one second to 999,999 seconds. The default time is 600 seconds (10 minutes).
4 Click OK.

To unblock an attacking computer

1 In the client, in the sidebar, click View logs.
3 In the **Security Log**, select the row that contains **Active Response** in the **Event Type** column, and then click **Action > Stop Active Response**.

To unblock the blocked IP addresses, click **Action > Stop All Active Response**. If you unblock an active response, the **Event Type** column displays "Active Response canceled." If the active response times out, the **Event Type** column displays "Active Response disengaged."

4 In the message box that appears, click **OK**.

5 Click **File > Exit**.

See “**Blocking traffic**” on page 109.

See “**Configuring firewall settings**” on page 99.

**Blocking traffic**

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

<table>
<thead>
<tr>
<th>When your computer’s screen saver is activated.</th>
<th>You can configure your computer to block all the inbound and the outbound network neighborhood traffic when your computer’s screen saver is activated. As soon as the screen saver turns off, your computer returns to the previously assigned security level.</th>
</tr>
</thead>
<tbody>
<tr>
<td>When the firewall does not run.</td>
<td>The computer is unprotected after the client computer starts and before the firewall service starts or after the firewall service stops and the computer turns off. This time frame is a small security hole that can allow unauthorized communication.</td>
</tr>
<tr>
<td>When you want to block all inbound traffic and outbound traffic at any time.</td>
<td>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. <strong>Note:</strong> Your administrator may have configured this option to be unavailable. You cannot block traffic on an unmanaged client.</td>
</tr>
</tbody>
</table>

You can allow all traffic by disabling Network Threat Protection.

See “**Enabling or disabling protection on the client computer**” on page 41.
To block traffic when the screen saver is activated
1  In the client, in the sidebar, click Change settings.
2  Beside Network Threat Protection, click Configure Settings.
3  On the Microsoft Windows Networking tab under Screen Saver Mode, click Block Microsoft Windows Networking traffic while the screen saver runs.
4  Click OK.

To block traffic when the firewall does not run
1  In the client, in the sidebar, click Change settings.
2  Beside Network Threat Protection, click Configure Settings.
3  On the Firewall tab under Traffic Settings, click Block all traffic until the firewall starts and after the firewall stops.
4  Optionally click Allow initial DHCP and NetBIOS traffic.
5  Click OK.

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

See “Blocking and unblocking an attacking computer” on page 108.
See “Configuring firewall settings” on page 99.

About allowing or blocking applications

An application is a software program that you use to accomplish certain tasks. For example, Internet Explorer and iTunes are applications. You can customize the client to control certain applications to protect your network from attacks.

The following describes the tasks you can perform to customize firewall protection for your applications. All of these tasks are optional and can be performed in any order:

■ You can enable the client to allow or block an application from accessing the network.
   See “Allowing or blocking applications from accessing the network” on page 111.
You can configure the settings for an application that has run since the client service starts or has asked for permission to access the network. You can also configure restrictions such as the IP addresses and the ports that the application can use. You can view and change the action that the client takes for each application that tries to gain access through your network connection. By configuring the settings for a specific application, you create an application-based firewall rule. See “Configuring application-specific settings” on page 112.

You can remove the application's restrictions, such as the time of day that the firewall blocks an application. 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. You can also stop an application or service from running until the application tries to access your computer again, such as when you restart the computer. See “Removing the restrictions from an application” on page 113.

See “Managing firewall protection” on page 96.

Allowing or blocking applications from accessing the network

You can enable the client to allow or block an application from accessing the network.

Table 5-4 describes the actions that the client takes on network traffic.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>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.</td>
</tr>
<tr>
<td>Block</td>
<td>Blocks the inbound traffic and the outbound traffic from accessing the network or an Internet connection.</td>
</tr>
<tr>
<td>Ask</td>
<td>Asks you whether you want the application to access the network the next time you attempt to run the application.</td>
</tr>
<tr>
<td>Terminate</td>
<td>Stops the process.</td>
</tr>
</tbody>
</table>
To allow or block an application from accessing the network

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


3. In the Network Activity dialog box, in the Running Applications field, right-click the application or service, and then click the option that you want.

4. Click Close.

See “Viewing network activity” on page 114.

See “Blocking traffic” on page 109.

See “About allowing or blocking applications” on page 110.

Configuring application-specific settings

You can configure the settings for an application that has run since the client service starts or has asked for permission to access the network.

You can configure restrictions such as the IP addresses and the ports that the application can use. You can view and change the action that the client takes for each application that tries to gain access through your network connection. By configuring the settings for a specific application, you create an application-based firewall rule.

Note: If there is a conflict between a firewall rule and an application-specific setting, 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 the schedule for a specific video application.

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

To configure application-specific settings

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

2. Beside Network Threat Protection, click Options > View Application Settings.

3. In the View Application Settings dialog box, select the application you want to configure, and then click Configure.

4. In the Configure Application Settings dialog box, in the Trusted IPs for the application box, type an IP address or an IP range.

5. In the Remote server ports or Local ports group boxes, select a TCP or a UDP port.
6 To specify the direction of the traffic, click one or both of the following items:

- To allow outbound traffic: Click **Allow outgoing connections**.
- To allow inbound traffic: Click **Allow incoming connections**.

7 To apply the rule when the screen saver runs, click **Allow while screen saver is activated**.

8 To set up a schedule when the restrictions are or are not in effect, click **Enable scheduling**.

9 Select one of the following items:

- To specify the time when the restrictions are in effect: Click **During the period below**.
- To specify the time when the restrictions are not in effect: Click **Excluding the period below**.

10 Set up the schedule.

11 Click **OK**.

12 In the **View Application Settings** dialog box, to change the action, right-click the application, and then click **Allow** or **Block**.

13 Click **OK**.

**To stop an application or service**

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

2 Beside Network Threat Protection, click **Options > View Network Activity**.

3 In the **Running Applications** field, right-click the application, and then click **Terminate**.

4 To confirm, click **Yes**, and then click **Close**.

See “Adding a firewall rule” on page 122.

See “Viewing network activity” on page 114.

See “About allowing or blocking applications” on page 110.

---

**Removing the restrictions from an application**

You can remove the application's restrictions, such as the time of day that the firewall blocks an application. 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.

You can stop an application or service from running until the application tries to access your computer again, such as when you restart the computer.

**To remove the restrictions from an application**

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options** > **View Application Settings**.
3. In the **View Application Settings** dialog box, do one of the following actions:
   - To remove an application from the list, select the application, and then click **Remove**.
   - To remove all applications from the list, click **Remove All**.
4. Click **Yes**.
5. Click **OK**.

See “**Configuring application-specific settings**” on page 112.

See “**About allowing or blocking applications**” on page 110.

---

### Viewing network activity

You can view information about inbound traffic and outbound traffic from your computer. You can also view a list of applications and services that have run since the client service started.

**Note:** The client does not detect network traffic from Personal Digital Assistant (PDA) devices.

You can display the network traffic as either broadcast traffic or unicast traffic. Broadcast traffic is the network traffic that is sent to every computer in a particular subnet, and is not directed specifically to your computer. Unicast traffic is the traffic that is directed specifically to your computer.

**To view network activity history**

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options** > **View Network Activity**.
3. Click **Close**.
To show or hide Windows services and broadcast traffic

1. In the client, in the sidebar, click Status.
3. In the Network Activity dialog box, right-click Running Applications and do any of the following actions:
   - To show or hide Windows services: Check or uncheck Show Windows Services.
   - To display broadcast traffic: Check Show Broadcast Traffic.
   - To display unicast traffic: Uncheck Show Broadcast Traffic.
4. Click Close.

To change the way the application information displays

1. In the client, in the sidebar, click Status.
3. In the Running Applications field, right-click the application, and then click the view that you want to see. For example, you can click Details.
4. Click Close.

See “Configuring application-specific settings” on page 112.
See “Allowing or blocking applications from accessing the network” on page 111.
See “Blocking traffic” on page 109.
See “Managing firewall protection” on page 96.

About client firewall rules

Table 5-5 describes what you should know about client firewall rules.
### Table 5-5  
Topics about client firewall rules

<table>
<thead>
<tr>
<th>Topic</th>
<th>Description</th>
</tr>
</thead>
</table>
| Understand how firewall rules, settings, and intrusion prevention   | You can be more successful in creating effective firewall rules if you understand how the rules, firewall settings, and intrusion prevention settings are processed. Understanding how the rules and settings are processed lets you order your firewall rules accordingly.  
See “About the firewall rule, firewall setting, and intrusion prevention processing order” on page 116.  
See “Changing the order of firewall rules” on page 117.                                                                 | settings are processed.                                                                                                                                                                                                                                                                                                                                 |
| rules, settings, and intrusion prevention settings are processed      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Learn about how the client uses stateful inspection so that you     | Symantec Endpoint Protection uses stateful inspection. This means that for the traffic that is initiated in one direction, you do not need a rule to permit the return traffic. Understanding how stateful inspection works eliminates the need for creating rules.  
See “How the firewall uses stateful inspection” on page 118.                                                                 | do not have to create specific rules                                                                                                                                                                                                                                                                                                                                 |
| do not have to create specific rules                                |                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Know the elements of a firewall rule                               | To create effective firewall rules, you should understand the components that make up a rule.  
See “The elements of a firewall rule” on page 119.                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                           |

See “Managing firewall protection” on page 96.

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

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

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

The best practices for creating a rule base include the following order of rules:
1st  Rules that block all traffic.
2nd  Rules that allow all traffic.
3rd  Rules that allow or block specific computers.
4th  Rules that allow or block specific applications, network services, and ports.

Table 5-6 shows the order in which the firewall processes the rules, firewall settings, and intrusion prevention settings.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>First</td>
<td>Custom IPS signatures</td>
</tr>
<tr>
<td>Second</td>
<td>Intrusion Prevention settings, traffic settings, and stealth settings</td>
</tr>
<tr>
<td>Third</td>
<td>Built-in rules</td>
</tr>
<tr>
<td>Fourth</td>
<td>Firewall rules</td>
</tr>
<tr>
<td>Fifth</td>
<td>Port scan checks</td>
</tr>
<tr>
<td>Sixth</td>
<td>IPS signatures that are downloaded through LiveUpdate</td>
</tr>
</tbody>
</table>

See “Changing the order of firewall rules” on page 117.
See “How a firewall works” on page 98.
See “How intrusion prevention works” on page 125.
See “About client firewall rules” on page 115.

### Changing the order of firewall rules

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

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

**To change the order of a firewall rule**

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options > Configure Firewall Rules**.
3 In the **Configure Firewall Rules** dialog box, select the rule that you want to move.

4 Do one of the following actions:
   - To have the firewall process this rule before the rule above it, click the up arrow.
   - To have the firewall process this rule after the rule below it, click the down arrow.

5 When you finish moving rules, click **OK**.

See “About the firewall rule, firewall setting, and intrusion prevention processing order” on page 116.

See “About client firewall rules” on page 115.

---

**How the firewall uses stateful inspection**

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

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

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

Stateful inspection supports all rules that direct TCP traffic.

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

See “How a firewall works” on page 98.

See “About client firewall rules” on page 115.

The elements of a firewall rule

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

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

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

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

Table 5-7 describes the criteria that you use to define a firewall rule.
The firewall rule triggers are as follows:

- **Applications**
  When the application is the only trigger you define in an allow traffic rule, the firewall allows the application to perform any network operation. The application is the significant value, not the network operations that the application performs. For example, suppose you allow Internet Explorer and define no other triggers. Users can access the remote sites that use HTTP, HTTPS, FTP, Gopher, and any other protocol that the Web browser supports. You can define additional triggers to describe the particular network protocols and hosts with which communication is allowed.

- **Hosts**
  The local host is always the local client computer and the remote host is always a remote computer that is positioned elsewhere on the network. This expression of the host relationship is independent of the direction of traffic. When you define host triggers, you specify the host on the remote side of the described network connection.

- **Protocols**
  A protocol trigger identifies one or more network protocols that are significant in relation to the described traffic. The local host computer always owns the local port, and the remote computer always owns the remote port. This expression of the port relationship is independent of the direction of traffic.

- **Network adapters**
  If you define a network adapter trigger, the rule is relevant only to the traffic that is transmitted or received by using the specified type of adapter. You can specify either any adapter or the one that is currently associated with the client computer.

You can combine the trigger definitions to form more complex rules, such as to identify a particular protocol in relation to a specific destination address. When the firewall evaluates the rule, all the triggers must be true for a positive match to occur. If any one trigger is not true in relation to the current packet, the firewall cannot apply the rule.

### Table 5-7: Firewall rule conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Triggers</td>
<td>The firewall rule triggers are as follows:</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Managing the firewall and intrusion prevention

The elements of a firewall rule
Table 5-7  
Firewall rule conditions (continued)

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

See “How the firewall uses stateful inspection” on page 118.

See “Adding a firewall rule” on page 122.

See “About client firewall rules” on page 115.

Setting up firewall rules

Table 5-8 describes how to set up new firewall rules.
Table 5-8  How to setup firewall rules

<table>
<thead>
<tr>
<th>Step</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Add a new firewall rule</td>
<td>Symantec Endpoint Protection installs with default firewall rules. But you can create your own rules.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Adding a firewall rule” on page 122.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Another way that you can add a firewall rule is to export existing firewall rules from another Firewall policy. You can then import the firewall rules and settings so that you do not have to re-create them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>See “Exporting and importing firewall rules” on page 123.</td>
</tr>
<tr>
<td>2</td>
<td>(Optional) Customize the firewall rule</td>
<td>After you create a new rule, or if you want to customize a default rule, you can modify any of the firewall rule criteria.</td>
</tr>
<tr>
<td></td>
<td>criteria</td>
<td>See “The elements of a firewall rule” on page 119.</td>
</tr>
</tbody>
</table>

See “About client firewall rules” on page 115.

See “Enabling and disabling firewall rules” on page 123.

Adding a firewall rule

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

Firewall rules are automatically enabled when you create them.

**To add a firewall rule**

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, click **Add**.
4. On the **General** tab, type a name for the rule, and then click either **Block this traffic** or **Allow this traffic**.
5. To define the triggers for the rule, click on each tab and configure it as needed.
6. To define the time period when the rule is active or inactive, on the **Scheduling** tab, click **Enable Scheduling**, and then set up a schedule.
7. When you finish making changes, click **OK**.
8. Click **OK**.

See “The elements of a firewall rule” on page 119.
Exporting and importing firewall rules

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

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

To export firewall rules
1. In the client, in the sidebar, click Status.
2. Beside Network Threat Protection, click Options > Configure Firewall Rules.
3. In the Configure Firewall Rules dialog box, select the rules you want to export.
4. Right-click the rules, and then click Export Selected Rules.
5. In the Export dialog box, type a file name, and then click Save.
6. Click OK.

To import firewall rules
1. In the client, in the sidebar, click Status.
2. Beside Network Threat Protection, click Options > Configure Firewall Rules.
3. In the Configure Firewall Rules dialog box, right-click the firewall rules list, and then click Import Rule.
4. In the Import dialog box, locate the .sar file that contains the rules you want to import.
5. Click Open.
6. Click OK.

See “Adding a firewall rule” on page 122.

Enabling and disabling firewall rules

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

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

1. In the client, in the sidebar, click **Status**.
2. Beside **Network Threat Protection**, click **Options > Configure Firewall Rules**.
3. In the **Configure Firewall Rules** dialog box, in the Rule Name column, check or uncheck the check box beside the rule that you want to enable or disable.
4. Click **OK**.

See “Adding a firewall rule” on page 122.

### Managing intrusion prevention

You manage intrusion prevention as part of Network Threat Protection.

<table>
<thead>
<tr>
<th>Table 5-9</th>
<th>Managing intrusion prevention</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Learn about intrusion prevention</td>
<td>Learn how intrusion prevention detects and blocks network and browser attacks. See “How intrusion prevention works” on page 125.</td>
</tr>
<tr>
<td>Download the latest IPS signatures</td>
<td>By default, the latest signatures are downloaded to the client. However you might want to download the signatures immediately. See “Updating the computer’s protection” on page 33.</td>
</tr>
</tbody>
</table>
### Table 5-9 Managing intrusion prevention (continued)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Enable or disable network intrusion prevention or browser intrusion prevention | You might want to disable intrusion prevention for troubleshooting purposes or if client computers detect excessive false positives. Typically, you should not disable intrusion prevention. You can enable or disable the following types of intrusion prevention:  
  - Network intrusion prevention  
  - Browser intrusion prevention  
  See “Enabling or disabling intrusion prevention” on page 126. You can also enable or disable intrusion prevention when you enable or disable Network Threat Protection.  
  See “About enabling and disabling protection” on page 40. |
| Configure intrusion prevention notifications | You can configure notifications to appear when Symantec Endpoint Protection detects a network or browser intrusion.  
  See “Configuring intrusion prevention notifications” on page 127. |

### How intrusion prevention works

Intrusion prevention is part of Network Threat Protection.

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

See “Managing intrusion prevention” on page 124.

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 or browser attacks. Intrusion prevention uses signatures to detect attacks on operating system components and the application layer.

Intrusion prevention provides two types of protection.
Network intrusion prevention

Network intrusion prevention uses signatures to identify attacks on client computers. For known attacks, intrusion prevention automatically discards the packets that match the signatures.

You cannot create custom signatures on the client. But you can import custom signatures that you or your administrator created in Symantec Endpoint Protection Manager.

Browser intrusion prevention

Browser intrusion prevention monitors attacks on Internet Explorer and Firefox. Browser intrusion prevention is not supported on any other browsers.

This type of intrusion prevention uses attack signatures as well as heuristics to identify attacks on browsers.

For some browser attacks, intrusion prevention requires that the client terminate the browser. A notification appears on the client computer.

Enabling or disabling intrusion prevention

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

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

See “Managing intrusion prevention” on page 124.

You can enable or disable two types of intrusion prevention:

- Network intrusion prevention
- Browser intrusion prevention

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

See “About enabling and disabling protection” on page 40.
To enable or disable intrusion prevention settings

1. In the client, in the sidebar, click Change settings.
3. On the Intrusion Prevention tab, check or uncheck either of the following settings:
   - Enable Network Intrusion Prevention
   - Enable Browser Intrusion Prevention
   For more information on the settings, click Help.
4. Click OK.

Configuring intrusion prevention notifications

You can configure notifications to appear when the client detects a network attack on your computer or when the client blocks an application from accessing your computer. You can set the length of time that these notifications appear and whether the notification occurs with an audio announcement.

You must enable the intrusion prevention system for the intrusion prevention notifications to appear.

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

See “Managing intrusion prevention” on page 124.

To configure intrusion prevention notifications

1. In the client, in the sidebar, click Change settings.
3. In the Network Threat Protection Settings dialog box, click Notifications.
4. Check Display Intrusion Prevention notifications.
5. To hear a beep when the notification appears, check Use sound when notifying users.
6. Click OK.
Managing the firewall and intrusion prevention

Configuring intrusion prevention notifications
Managing Symantec Network Access Control

This chapter includes the following topics:

- How Symantec Network Access Control works
- How the client works with an Enforcer
- Running a Host Integrity check
- Remediating your computer
- Configuring the client for 802.1x authentication
- Viewing the Symantec Network Access Control logs

How Symantec Network Access Control works

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

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

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>The client continuously evaluates its compliance.</td>
<td>You turn on the client computer. The client runs a Host Integrity check that compares the computer's configuration with the Host Integrity policy that was downloaded from the management server. The Host Integrity check evaluates your computer for compliance with the Host Integrity policy for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check how recently its virus definitions have been updated, and which were the latest patches applied to the operating system.</td>
</tr>
<tr>
<td>A Symantec Enforcer authenticates the client computer and either grants the computer network access or blocks and quarantines non-compliant computers.</td>
<td>If the computer meets all the policy's requirements, the Host Integrity check passes. The Enforcer grants full network access to computers that pass the Host Integrity check. If the computer does not meet the policy's requirements, the Host Integrity check fails. When a Host Integrity check fails, the client or a Symantec Enforcer blocks or quarantines your computer until you remediate your computer. Quarantined computers have limited or no access to the network. See &quot;How the client works with an Enforcer&quot; on page 131.</td>
</tr>
<tr>
<td>Your administrator may have set up the policy so that a Host Integrity check passes even if a specific requirement fails.</td>
<td>The client may display a notification every time the Host Integrity check passes. See “Types of alerts and notifications” on page 21.</td>
</tr>
<tr>
<td>The client remediates non-compliant computers.</td>
<td>If the client finds that a Host Integrity policy requirement is not met, it installs or requests you to install the required software. After your computer is remediated, it tries to access the network again. If the computer is fully compliant, the network grants the computer network access. See “Remediating your computer” on page 132.</td>
</tr>
<tr>
<td>The client proactively monitors compliance.</td>
<td>The client actively monitors the compliance state for all client computers. If at any time the computer’s compliance status changes, so do the network access privileges of the computer.</td>
</tr>
</tbody>
</table>
You can view more information about the Host Integrity check results in the security log.

How the client works with an Enforcer

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

See “How Symantec Network Access Control works” on page 129.

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

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

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

See “Configuring the client for 802.1x authentication” on page 132.

Running a Host Integrity check

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

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

2. Next to Network Access Control, click **Options > Check Compliance**.

3. If a message appears that confirms that the Host Integrity check ran, click **OK**.

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

Remediating your computer

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

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

To remediate your computer

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

Configuring the client for 802.1x authentication

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

The 802.1x authentication process includes the following steps:
An unauthenticated client or third-party supplicant sends the user information and compliance information to a managed 802.1x network switch.

The network switch relays the information to the LAN Enforcer. The LAN Enforcer sends the user information to the authentication server for authentication. The RADIUS server is the authentication server.

If the client fails the user-level authentication or is not in compliance with the Host Integrity policy, the Enforcer may block network access. The Enforcer places the non-compliant client computer in a quarantine network where the computer can be remediated.

After the client remediates the computer and brings it into compliance, the 802.1x protocol reauthenticates the computer and grants the computer access to the network.

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

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

### Table 6-2  802.1x authentication options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-party supplicant</td>
<td>Uses a third-party 802.1x supplicant. The LAN Enforcer works with a RADIUS server and third-party 802.1x supplicants to perform user authentication. The 802.1x supplicant prompts you for user information. The LAN Enforcer passes that user information to the RADIUS server for user-level authentication. The client sends the client profile and the Host Integrity status to the Enforcer so that the Enforcer authenticates the computer. <strong>Note:</strong> If you want to use the Symantec Network Access Control client with a third-party supplicant, then the Network Threat Protection module of the Symantec Endpoint Protection client must be installed.</td>
</tr>
</tbody>
</table>
Table 6-2 802.1x authentication options (continued)

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

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

**To configure the client to use a third-party supplicant**

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

4. Click **OK**.

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

   See “**Adding a firewall rule**” on page 122.

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

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

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

2. Beside Network Access Control, click **Options > Change Settings > 802.1x Settings**.

3. In the **Network Access Control Settings** dialog box, click **Enable 802.1x authentication**.

4. Click **Use client as an 802.1x supplicant**.

5. Do one of the following actions:
   - To select transparent mode, check **Use Symantec Transparent Mode**.
   - To configure a built-in supplicant, click **Allows you to choose the authentication protocol**.
     You then need to choose the authentication protocol for your network connection.

6. Click **OK**.

**To choose an authentication protocol**

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

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

2. In the **Local Area Connection Status** dialog box, click **Properties**.

3. In the **Local Area Connection Properties** dialog box, click the **Authentication** tab.

4. On the **Authentication** tab, click the **EAP type** drop-down list, and select one of the following authentication protocols:
Smart Card or other Certificate
- Protected EAP (PEAP)
- Symantec NAC Transparent Mode

Make sure that the Enable IEEE 802.1x authentication for this network check box is checked.

5. Click OK.
6. Click Close.

Reauthenticating your computer

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

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

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

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

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

To reauthenticate your computer
1. Right-click the notification area icon.
2. Click Re-authentication....
3. In the Re-authenticate dialog box, type your user name and password.
4. Click OK.
Viewing the Symantec Network Access Control logs

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

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

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

You can export the log data from these logs.

**To view Symantec Network Access Control logs**

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

See “About the logs” on page 45.
Viewing the Symantec Network Access Control logs
Symbols
64-bit computers 17
802.1x authentication
about 132
configuring 134

A
active response
about 108
active scans
running 68
adware 64
alerts
icons 15
responding to 21
allow traffic 112
firewall rules 122
responding to messages 28
anti-MAC spoofing
enabling 100
applications 110
allowing or blocking 112, 122
excluding from scans 82
Auto-Protect
Download Insight 40
enabling or disabling 40, 42
for Internet email 60
for Lotus Notes 62
for Microsoft Outlook 60
for the file system 42
groupware email clients 60

B
blended threats 64
block an attacking computer 108
block traffic 109, 112
firewall rules 122
responding to messages 28
bots 64
broadcast traffic
showing 114
browser intrusion prevention
about 125

C
Change settings page 15
clean viruses 24, 66
clients
disabling protection on 40
how to protect computers 32
managed vs. unmanaged 37, 39
computers
how to protect computers 32
scanning 51
updating protection on 33
Control Log 46
custom scans
running 68

D
Debug Log 47
definitions
about 57
updating 33–35
delete viruses 24
dialers 64
disable
Auto-Protect 40, 42
Network Threat Protection 41–42
Proactive Threat Protection 41–42
Download Insight
customizing 74
interaction with Auto-Protect 40
managing detections 71
reputation data 66
responding to notifications 27
driver-level protection
enabling 100
email
  excluding Inbox file from scans 81
e-mail scanning. See Auto-Protect
enable
  Auto-Protect 42
  Network Threat Protection 42
  Proactive Threat Protection 42
enforcement
  about 131
exceptions
  about 81–82
creating 82
files
  acting on a detection 24
  excluding from scans 82
  sharing 106
  submitting to Symantec Security Response 86
firewall
  applications 110
  defined 96
  enabling or disabling 42
  managing 96
  settings 99
  stateful inspection 118
firewall rules 117
  about 119
  adding 122
  enabling and disabling 123
  exporting 123
  importing 123
  processing order
    about 116
    changing 117
  setting up 121
folders
  excluding from scans 82
full scans
  running 68
hack tools 64
Help option 13
Host Integrity check
  running 131
icons
  on Status page 15
    padlock 39
    shield 36
infected files
  acting on 23
Insight 66
Insight Lookup
  trusted intranet sites 74
Internet bots 64
intrusion prevention. See IPS
  enabling or disabling 127
  how it works 125
  managing 124
  notifications for 127
IPS
  about 96
  updating definitions 33–34
joke programs 65
licenses
  responding to messages about 29
LiveUpdate
  command 15
  creating a schedule for 35
  overview 33
  running immediately 34
logs
  about 45
  back tracing entries 48
  enabling the Packet Log 47
  export formats 49–50
  exporting data 49
  exporting filtered log entries 49
  network access control 137
  viewing 47
malware
  configuring actions for detections of 76
managed clients
  about 37
  checking for 39
  managing protection 32
messages
  intrusion prevention 127
  responding to 21, 28–30
misleading applications 65

N
NetBIOS protection
  enabling 100
network access control
  about 12, 129
  enforcement 131
  remediating the computer 132
network activity
  displaying 114
network intrusion prevention
  about 125
Network Threat Protection
  about 12, 96
  enabling or disabling 41–42
  logs 46
  managing 96
notification area icon
  about 36
  hiding and displaying 37
notifications
  Download Insight 27
  intrusion prevention 127
  responding to 21

O
on-demand scans
  creating 70
  running 16
options
  unavailable 38

P
Packet Log 46
  enabling 47
parental control programs 65
print sharing 106
Proactive Threat Protection
  about 12
  enabling or disabling 41–42
protection
  enabling or disabling 40
  how to 32
  updating 33–35

Q
Quarantine
  deleting files 87
  managing files in 84
  manually quarantine a file 86
  moving files to 85
  submitting files to Symantec Security Response 86
  viewing infected files 85
quarantining viruses 24

R
reauthentication 136
remote access programs 65
reputation data 66
right-click scanning 16
risk
  removing from infected file 26
Risk Log 45
  quarantining a file 86
rootkits 64

S
scan exceptions. See exceptions
Scan for threats page 14
Scan Log 45
  quarantining a file 86
scans
  about 59
  adjusting settings 75
  components that they scan 57
  configuring exceptions 75
  delaying 17
  excluding items from 82
  how they work 57
  interpreting results 23
  managing 51
  notification actions 75
  on-demand and startup 70
  pausing 17
  remediation actions 75
  responding to a detection 24
  running 16
  scheduled 67
  snooze options 18
  types of 59
  user-defined 75
scheduled scans
creating 67
multiple 68
security assessment tool 65
Security Log 46
security risks
configuring actions for detections of 76
excluding from scans 82
how the client detects 57
how the client responds 59
how the client responds to a detection 66
server
connecting to 36
managed clients 38
settings
intrusion prevention 127
share files and printers 106
shield icon 36
Smart DHCP 105
Smart DNS 105
Smart WINS 105
SONAR
about 12, 93
about detections 93
changing settings 94
logs 46
managing 91
spyware 65
standalone clients 37
startup scans
creating 70
stateful inspection 118
Status page 14
alert icons 15
troubleshooting 13
stealth mode Web browsing
enabling 100
submissions 88–89
Symantec Security Response
submitting files to 86
System Log
Client Management 46
Proactive Threat Protection 46
Virus and Spyware Protection 45
system tray icon 36

Tamper Protection (continued)
disabling 41
enabling and disabling 44
Tamper Protection Log 46
Threat Log 45
threats
blended 64
token ring traffic
enabling 100
trackware 65
traffic
allowing or blocking 112
blocking 109
displaying 114
Traffic and stealth settings 100
Traffic Log 46
Trojan horses 64
troubleshooting
from the Status page 13

U
unblock an attacking computer 108
unmanaged clients
about 37
checking for 39
managing protection 32
update
definitions 33–35

V
View quarantine page 15
virus
removing from infected file 26
Virus and Spyware Protection
about 12
System Log 45
virus definitions
about 57
updating 33–35
viruses 64
classifying 76
detection 57
response 59
response to a detection 66
unrecognized 86
W
Web domain
   excluding from scans  82
Windows Security Center
   seeing antivirus status from  90
   seeing firewall status from  91
Windows services
   showing  114
worms  64