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

For Microsoft Windows
Client Guide for Symantec Endpoint Protection and Symantec Network Access Control

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 11.00.06.00.00

Legal Notice

Copyright © 2010 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 Maintenance Programs, you can visit our Web site at the following URL:

www.symantec.com/business/support/

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 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.
Technical Support ................................................................................................................. 4

Section 1     Getting started on the client .......................................................... 13

Chapter 1     Introducing the client ................................................................. 15
About the client ........................................................................................................ 15
About the Symantec Endpoint Protection client ........................................ 16
  About Antivirus and Antispyware Protection ........................................ 16
  About Proactive Threat Protection .................................................. 17
  About Network Threat Protection ................................................. 18
About the Symantec Network Access Control client ................................. 18

Chapter 2     Responding to the client ............................................................... 19
About client interaction ................................................................................ 19
Acting on infected files ...................................................................................... 20
  About the damage that viruses cause ............................................. 21
About notifications and alerts ....................................................................... 22
  Responding to application-related notifications ................................ 22
  Responding to security alerts ......................................................... 25
  Responding to Network Access Control notifications ....................... 25

Chapter 3     Managing the client ................................................................ 27
About centrally managed clients and self-managed clients ................. 28
Converting a self-managed client to a centrally managed client .......... 29
Updating the computer's protection ......................................................... 30
  Updating the content immediately ................................................ 31
  Updating the content on a schedule ............................................... 32
About security policies ................................................................................. 32
Updating the policy file manually ............................................................. 33
Verifying that policies have been updated .................................................. 33
Scanning your computer immediately ....................................................... 34
Pausing and delaying scans .......................................................................... 34
Enabling and disabling protection technologies ....................................... 35
  Enabling or disabling Auto-Protect .................................................. 38
### Section 2
Managing protection on the Symantec Endpoint Protection client

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Managing Antivirus and Antispyware Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>page 49</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enabling or disabling Network Threat Protection</td>
<td>39</td>
</tr>
<tr>
<td>Enabling or disabling Proactive Threat Protection</td>
<td>39</td>
</tr>
<tr>
<td>About Tamper Protection</td>
<td>40</td>
</tr>
<tr>
<td>Enabling, disabling, and configuring Tamper Protection</td>
<td>41</td>
</tr>
<tr>
<td>Testing the security of your computer</td>
<td>42</td>
</tr>
<tr>
<td>About locations</td>
<td>42</td>
</tr>
<tr>
<td>Changing locations</td>
<td>43</td>
</tr>
<tr>
<td>About the notification area icon</td>
<td>44</td>
</tr>
<tr>
<td>Hiding and displaying the notification area icon</td>
<td>45</td>
</tr>
<tr>
<td>About preventing an administrator from restarting your computer</td>
<td>45</td>
</tr>
<tr>
<td>About viruses and security risks</td>
<td>50</td>
</tr>
<tr>
<td>How the client responds to viruses and security risks</td>
<td>53</td>
</tr>
<tr>
<td>About antivirus and antispyware settings</td>
<td>54</td>
</tr>
<tr>
<td>About scanning files</td>
<td>54</td>
</tr>
<tr>
<td>If your email application uses a single Inbox file</td>
<td>54</td>
</tr>
<tr>
<td>About scanning by extension</td>
<td>55</td>
</tr>
<tr>
<td>About scanning all file types</td>
<td>55</td>
</tr>
<tr>
<td>About preventing macro virus infections</td>
<td>56</td>
</tr>
<tr>
<td>When the client detects a virus or security risk</td>
<td>56</td>
</tr>
<tr>
<td>About Auto-Protect</td>
<td>57</td>
</tr>
<tr>
<td>About Auto-Protect and security risks</td>
<td>57</td>
</tr>
<tr>
<td>About Auto-Protect and email scanning</td>
<td>58</td>
</tr>
<tr>
<td>Disabling Auto-Protect handling of encrypted email connections</td>
<td>59</td>
</tr>
<tr>
<td>Viewing Auto-Protect scan statistics</td>
<td>60</td>
</tr>
<tr>
<td>Viewing the risk list</td>
<td>60</td>
</tr>
<tr>
<td>Configuring Auto-Protect to determine file types</td>
<td>60</td>
</tr>
<tr>
<td>Disabling and enabling Auto-Protect security risk scanning and blocking</td>
<td>61</td>
</tr>
<tr>
<td>Configuring network scanning setting</td>
<td>62</td>
</tr>
<tr>
<td>Working with antivirus and antispyware scans</td>
<td>64</td>
</tr>
<tr>
<td>How antivirus and antispyware scans work</td>
<td>64</td>
</tr>
<tr>
<td>About definitions files</td>
<td>66</td>
</tr>
<tr>
<td>About scanning compressed files</td>
<td>66</td>
</tr>
</tbody>
</table>
Scheduling a user-defined scan ....................................................... 66
Scheduling a scan to run on demand or when the computer starts up ................................................................................. 69
Editing and deleting startup, user-defined, and scheduled scans ........... 70
Interpreting scan results ................................................................................... 71
About interacting with scan results or Auto-Protect results ........... 71
Configuring actions for viruses and security risks ......................... 73
Tips for assigning second actions for viruses ........................................... 75
Tips for assigning second actions for security risks ...................... 76
About risk impact ratings ........................................................................... 77
Configuring notifications for viruses and security risks .................. 78
About excluding items from being scanned ....................................... 80
Excluding items from being scanned .......................................................... 81
About handling quarantined files .............................................................. 82
About infected files in the Quarantine ......................................................... 83
About handling infected files in the Quarantine .................................. 83
About handling files infected by security risks ..................................... 84
Managing the quarantine ........................................................................... 84
Viewing files and file details in the Quarantine ....................................... 85
Rescanning files in the Quarantine for viruses ...................................... 85
When a repaired file cannot be returned to its original location .......... 86
Clearing backup items ................................................................................. 86
Deleting files from the Quarantine ............................................................ 86
Automatically deleting files from the Quarantine ................................. 87
Submitting a potentially infected file to Symantec Security Response for analysis ........................................................... 88
Submitting information about scan detections to Symantec Security Response ................................................................. 88
About the client and the Windows Security Center ............................... 89

Chapter 5

Managing Proactive Threat Protection ........................................ 91
About TruScan proactive threat scans ................................................. 91
Processes and applications that TruScan proactive threat scans examine ................................................................. 92
About exceptions for TruScan proactive threat scans ....................... 93
About TruScan proactive threat scan detections .............................. 93
About acting on false positives ............................................................... 94
Configuring how often to run TruScan proactive threat scans .......... 95
Managing TruScan proactive threat detections ................................. 95
Setting the action for the detection of commercial applications ............. 96
Specifying actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers ........................................... 97
Specifying the types of processes that TruScan proactive threat scans detect ................................................................. 98
Configuring notifications for TruScan proactive threat scan detections ........................................................................ 99
Submitting information about TruScan proactive threat scans to Symantec Security Response ........................................ 99
Excluding a process from TruScan proactive threat scans ......................................................................................... 100

Chapter 6 Managing Network Threat Protection .............................. 103

About managing Network Threat Protection ............................... 104
Managing firewall protection .................................................... 104
How the firewall works ............................................................ 106
About firewall rules ................................................................... 107
   About the elements of a firewall rule .................................. 107
   About stateful inspection .................................................. 110
   About the rule processing order ...................................... 111
Adding a firewall rule ............................................................. 112
Changing the order of a firewall rule ......................................... 113
Enabling and disabling rules .................................................. 113
Exporting and importing rules ............................................... 114
About the built-in firewall rules ............................................... 114
Enabling traffic settings and stealth Web browsing settings ........ 115
Enabling Smart Traffic Filtering ............................................. 116
Enabling network file and printer sharing ............................... 116
Blocking traffic ........................................................................ 118
Configuring application-specific settings ................................. 120
   Removing the restrictions from an application .................. 121
Managing intrusion prevention protection ............................... 122
How Intrusion Prevention protection works ............................ 122
Enabling or disabling intrusion prevention settings .................. 123
Configuring intrusion prevention notifications ........................ 124
Blocking and unblocking an attacking computer ...................... 125

Section 3 Managing protection on the Symantec Network Access Control client .......................... 127

Chapter 7 Managing Network Access Control .............................. 129
How Symantec Network Access Control works .......................... 129
Running a Host Integrity check ............................................... 131
Section 4  Monitoring and logging .................................................. 139

Chapter 8  Using and managing logs .............................................. 141

About logs ................................................................................. 141
Managing log size ...................................................................... 143
  Configuring the retention time for the Antivirus and Antispyware
   Protection log entries .............................................................. 143
  Configuring the size of the Network Threat Protection logs and
   the Client Management logs .................................................... 144
  Configuring the retention time for the Network Threat Protection
   log entries and the Client Management log entries ................ 144
  About deleting the contents of the Antivirus and Antispyware
   System Log .............................................................................. 144
  Deleting the contents of the Network Threat Protection logs and
   the Client Management logs .................................................... 145
Quarantining risks and threats from the Risk Log and the Threat
  Log ........................................................................................... 145
Using the Network Threat Protection logs and the Client Management
  logs ............................................................................................. 146
  Refreshing the Network Threat Protection logs and the Client
   Management logs ...................................................................... 147
  Enabling the Packet Log ............................................................ 147
  Stopping an active response ....................................................... 147
  Tracing logged events back to their source ............................. 147
Using the Client Management logs with Symantec Network
  Access Control ............................................................................. 148
Exporting log data ...................................................................... 148

Index .............................................................................................. 151
Getting started on the client

- Chapter 1. Introducing the client
- Chapter 2. Responding to the client
- Chapter 3. Managing the client
Introducing the client

This chapter includes the following topics:

- About the client
- About the Symantec Endpoint Protection client
- About the Symantec Network Access Control client

About the client

Symantec produces the following two endpoint protection products that can be used together or separately.

### Table 1-1

<table>
<thead>
<tr>
<th>Client type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec Endpoint Protection</td>
<td>Symantec Endpoint Protection protects your computer from Internet threats and security risks.</td>
</tr>
<tr>
<td></td>
<td>See “About the Symantec Endpoint Protection client” on page 16.</td>
</tr>
<tr>
<td>Symantec Network Access Control</td>
<td>Symantec Network Access Control ensures that your computer’s security settings conform to network policies. Security settings can include software, software configuration settings, signature files, patches, or other elements.</td>
</tr>
<tr>
<td></td>
<td>See “About the Symantec Network Access Control client” on page 18.</td>
</tr>
</tbody>
</table>

You or your administrator has installed one or both of these Symantec client software products on your computer. If your administrator installed the client, then your administrator determined the products to enable on the client. Your
administrator can advise you as to what tasks you should perform by using the client.

If you installed the client on your computer, then it is a stand-alone installation. A stand-alone installation means that an administrator does not manage your client software.

See “About centrally managed clients and self-managed clients” on page 28.

**Note:** If you or your administrator has installed only one of these products on your computer, that product’s name appears in the title bar. When both types of protection are enabled, Symantec Endpoint Protection appears on the title bar.

---

### About the Symantec Endpoint Protection client

The default settings for the client provide Antivirus and Antispyware Protection, Proactive Threat Protection, and Network Threat Protection. You can adjust the default settings to suit your company’s needs, to optimize system performance, and to disable the options that do not apply.

See “About Antivirus and Antispyware Protection” on page 16.

See “About Proactive Threat Protection” on page 17.

See “About Network Threat Protection” on page 18.

You can use the Symantec Endpoint Protection client to protect your computer in the following ways:

- Scan your computer for viruses, known threats, and security risks.
  See “Scanning your computer immediately” on page 34.

- Monitor ports for known attack signatures.
  See “About logs” on page 141.

- Monitor programs on your computer for suspicious behavior.
  See “About TruScan proactive threat scans” on page 91.

- Protect your computer from network attacks.
  See “Managing firewall protection” on page 104.

### About Antivirus and Antispyware Protection

Antivirus and Antispyware Protection makes sure that your computer is protected from known viruses and security risks. Viruses that are quickly detected and removed from your computer cannot spread to other files and cause damage. The effects of viruses and security risks can be repaired. When the Symantec Endpoint
Protection client detects a virus or a security risk, by default the client notifies you about the detection. If you do not want to be notified, you or your administrator can configure the client to handle the risk automatically.

Antivirus and Antispyware Protection provides signature-based scans and includes the following:

- **Auto-Protect scans**
  Auto-Protect runs constantly and provides real-time protection for your computer by monitoring activity on your computer. Auto-Protect looks for viruses and security risks when a file is executed or opened. It also looks for viruses and security risks when you make any modifications to a file. For example, you might rename, save, move, or copy a file to and from folders.
  See “About Auto-Protect” on page 57.
  See “Configuring Auto-Protect to determine file types” on page 60.

- **Scheduled, startup, and on-demand scans**
  You or your administrator can configure other scans to run on your computer. These scans search for residual virus signatures in infected files. These scans also search for the signatures of security risks in infected files and system information. You or your administrator can initiate scans to systematically check the files on your computer for viruses and security risks. The security risks might include adware or spyware.
  See “Scheduling a user-defined scan” on page 66.
  See “Scheduling a scan to run on demand or when the computer starts up” on page 69.

### About Proactive Threat Protection

Proactive Threat Protection includes TruScan proactive threat scans, which make sure that your computer has zero-day attack protection from unknown threats. These scans use heuristics to analyze a program’s structure, its behavior, and other attributes for virus-like characteristics. In many cases it can protect against threats such as mass-mailing worms and macro viruses. You might encounter worms and macro viruses before you update your virus and security risk definitions. Proactive threat scans look for script-based threats in HTML, VBScript, and JavaScript files.

See “About TruScan proactive threat scans” on page 91.

Proactive threat scans also detect the commercial applications that can be used for malicious purposes. These commercial applications include remote control programs or keyloggers.
You can configure proactive threat scans to quarantine detections. You can manually restore the items that are quarantined by proactive threat scans. The client can also automatically restore quarantined items.

See “Managing TruScan proactive threat detections” on page 95.

About Network Threat Protection

The Symantec Endpoint Protection client provides a customizable firewall that protects your computer from intrusion and misuse, whether malicious or unintentional. It detects and identifies known port scans and other common attacks. In response, the firewall selectively allows or blocks various network services, applications, ports, and components. It includes several types of protection firewall rules and security settings to protect client computers from the network traffic that can cause harm.

Firewall rules determine whether your computer allows or blocks an inbound or an outbound application that tries to access your computer through your network connection. Firewall rules systematically allow or block the inbound or the outbound applications and traffic from or to specific IP addresses and ports. The security settings detect and identify common attacks, send email messages after an attack, display customizable messages, and perform other related security tasks.

See “Managing firewall protection” on page 104.

Network Threat Protection also provides intrusion prevention signatures to prevent intrusion attacks and malicious content. The firewall allows or blocks the traffic according to various criteria.

See “Managing intrusion prevention protection” on page 122.

About the Symantec Network Access Control client

The Symantec Network Access Control client evaluates whether a computer is properly protected and compliant 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 antivirus and firewall applications. If your computer does not run the required software, either you or the client must update the software. If your security software is not 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.
Responding to the client

This chapter includes the following topics:

- About client interaction
- Acting on infected files
- About notifications and alerts

About client interaction

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.

You might see the following types of alerts or notifications:

<table>
<thead>
<tr>
<th>Virus or security risk detection</th>
<th>If Auto-Protect or a scan detects a virus or a security risk, the Symantec Endpoint Protection Detection Results dialog appears. Details about the infection are included. The dialog box also displays the action that Symantec Endpoint Protection performed on the risk. You usually do not need to take any further actions other than to review the activity and to close the dialog. You can take action if necessary, however. See “Acting on infected files” on page 20.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-related notifications</td>
<td>When a program on your computer tries to access a network, Symantec Endpoint Protection might prompt you to allow or deny permission. See “Responding to application-related notifications” on page 22.</td>
</tr>
</tbody>
</table>
Security alerts

Symantec Endpoint Protection informs you when it blocks a program or when it detects an attack against your computer.

See “Responding to security alerts” on page 25.

If you have Symantec Network Access Control enabled on the computer, you might see a Network Access Control message. This message appears when your security settings do not conform to the standards that your administrator has configured.

See “Responding to Network Access Control notifications” on page 25.

Acting on infected files

By default, Auto-Protect runs continuously on your computer. For unmanaged clients, an automatically-generated Active Scan runs when you start up your computer. For managed clients, your administrator typically configures a full scan to run at least one time each week. Auto-Protect displays a results dialog box when it makes a detection. When scans run, a scan dialog box appears to show the results of the scan. For managed clients, your administrator might turn off these types of notifications.

If you receive these types of notifications, you might need to act on an infected file.

The default options for Auto-Protect and all scan types are to clean a virus from an infected file on detection. If the client cannot clean a file, it logs the failure and moves the infected file to the Quarantine. The local Quarantine is a special location that is reserved for infected files and related system side effects. For security risks, the client quarantines the infected files and removes or repairs their side effects. The client logs the detection if it cannot repair the file.

**Note:** In the Quarantine, the virus cannot spread. When the client moves a file to the Quarantine, you do not have access to the file.

When Symantec Endpoint Protection repairs a virus-infected file, you do not need to take further action to protect your computer. If the client quarantines a security risk-infected file, and then removes and repairs it, you do not need to take additional action.

You might not need to act on a file, but you might want to perform an additional action on the file. For example, you might decide to delete a cleaned file because you want to replace it with an original file.

You can use the notifications to act on the file immediately. You can also use the log view or the Quarantine to act on the file later.
See “Interpreting scan results” on page 71.

See “Quarantining risks and threats from the Risk Log and the Threat Log” on page 145.

See “About handling quarantined files” on page 82.

To act on an infected file

1. Do one of the following actions:
   - In the scan progress dialog box, select the files that you want when the scan completes.
   - In the scan results dialog box, select the files that you want.
   - In the client, in the sidebar, click View Logs, and then next to Antivirus and Antispyware Protection, click View Logs. In the log view, select the files that you want.

2. Right-click the file or files, and then select one of the following options. Note, that in some cases, the client might not be able to perform the action that you selected.
   - Undo Action Taken: Reverses the action taken.
   - Clean (viruses only): Removes the virus from the file.
   - Delete Permanently: Deletes the infected file and all side effects. For security risks, use this action with caution. In some cases, if you delete security risks you might cause an application to lose functionality.
   - Move to Quarantine: Places the infected files in the Quarantine. For security risks, the client also tries to remove or repair the side effects.
   - Properties: Displays the information about the virus or security risk.

About the damage that viruses cause

If Symantec Endpoint Protection finds an infection soon after the infection occurs, the infected file might be fully functional after the client cleans it. In some instances, however, Symantec Endpoint Protection may clean an infected file that a virus already damaged. For example, Symantec Endpoint Protection might find a virus that damages a document file. Symantec Endpoint Protection removes the virus but cannot repair the damage inside the infected file.
About notifications and alerts

You may see several different types of notifications on your computer. These notifications usually describe a situation and indicate how the client tries to resolve the issue.

You may see the following types of notifications:

- Application-related notifications
  See “Responding to application-related notifications” on page 22.
- Security alerts
  See “Responding to security alerts” on page 25.

Responding to application-related notifications

You may see a notification that asks you whether you want to allow an application or a service to run.

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.
- The client switched users through Fast User Switching.
  See “Fast user switching notifications” on page 24.
- Your administrator updated the client software.
  See “Responding to automatic update notifications” on page 24.

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

Internet Explorer (IEXPLORE.EXE) is trying to connect to www.symantec.com using remote port 80 (HTTP - World Wide Web).
Do you want to allow this program to access the network?

To respond to applications that try to access the network

1. In the message box, click Detail.
   You can view more information about the connection and the application, such as the file name, version number, and path name.

2. If you want the client to remember your choice the next time that this application tries to access your network connection, click Remember my answer, and do not ask me again for this application.

3. Do one of the following tasks:
To allow the application to access the network connection, click **Yes**. Click **Yes** only if you recognize the application and you are sure that you want it to access the network connection. If you are unsure whether to allow the application to access the network connection, ask your administrator.

To block the application from accessing the network connection, click **No**.

Table 2-1 displays how you can respond to notifications that ask you whether you want to allow or block an application.

<table>
<thead>
<tr>
<th>If you check “Remember my answer...” check box?</th>
<th>If you click</th>
<th>The client...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>Yes</td>
<td>Allows the application and does not ask again.</td>
</tr>
<tr>
<td>No</td>
<td>Yes</td>
<td>Allows the application and asks you every time.</td>
</tr>
<tr>
<td>Yes</td>
<td>No</td>
<td>Blocks the application and does not ask you again.</td>
</tr>
<tr>
<td>No</td>
<td>No</td>
<td>Blocks the application and asks you every time.</td>
</tr>
</tbody>
</table>

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 120.

**Changed application notifications**

Occasionally, you might see a message that indicates an application has changed. The following message is an example.

“Telnet Program has changed since the last time you opened it, this could be because you have updated it recently. Do you want to allow it to access the network?”

The application that is listed in the preceding message tries to access your network connection. Although the client recognizes the name of the application, something about the application has changed since the last time the client encountered it. Most likely, you have upgraded the product recently. Every new product version uses a different file fingerprint file than the older version. The client detects that the file fingerprint file changed.
Fast user switching notifications

If you use Windows Vista/XP, you may see one of the following notifications:

“Symantec Endpoint Protection is unable to show the user interface. If you are using Windows XP Fast User Switching, make sure all other users are logged off of Windows and try logging off of Windows and then log back on. If you are using Terminal Services, the user interface is not supported.”

or

“Symantec Endpoint Protection was not running but will be started. However, the Symantec Endpoint Protection is unable to show the user interface. If you are using Windows XP Fast User Switching, make sure all other users are logged off of Windows and try logging off of Windows and then log back on. If you are using Terminal Services, the user interface is not supported.”

Fast User Switching is a Windows feature that makes it possible for you to quickly switch between users without having to log off the computer. Multiple users can share a computer simultaneously, and switch back and forth without closing the applications they run. One of these windows appears if you switch users by using Fast User Switching.

To respond to a fast user switching message, follow the instructions in the dialog box.

Responding to automatic update notifications

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.
Responding to security alerts

Security alerts display a notification above the notification area icon. You only need to acknowledge that you read the message by clicking OK. The notifications appear for one of the following reasons:

**Blocked application messages**

An application that has been launched from your computer has been blocked in accordance with the rules that are set by your administrator. For example, you may see the following message:

Traffic has been blocked from this application: (application name)

These notifications indicate that your client has blocked the traffic that you specified as not trusted. 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.

**Intrusions**

An attack was launched against your computer, and an alert either informs you of the situation or provides instructions on how to deal with it. For example, you may see the following message:

Traffic from IP address 192.168.0.3 is blocked from 10/10/2006 15:37:58 to 10/10/2006 15:47:58. Port Scan attack is logged.

Your administrator may have disabled intrusion prevention notifications on the client computer.

To see what types of attacks your client detects, you can enable the client to display intrusion prevention notifications.

See “Configuring intrusion prevention notifications” on page 124.

Responding to Network Access Control notifications

If the Symantec Network Access Control client does not comply with security policies, it might not be able to access the network. In this case, you might see a message that states that the Symantec Enforcer blocked your traffic because the Host Integrity check failed. Your network administrator might have added text to this message that suggests possible remediation actions. After you close the message box, open the client to see if it displays any suggested procedures to restore network access.

**To respond to Network Access Control notifications**

1. Follow any suggested procedures that appear in the message box.
2. In the message box, click OK.
Responding to the client

About notifications and alerts
Managing the client

This chapter includes the following topics:

- About centrally managed clients and self-managed clients
- Converting a self-managed client to a centrally managed client
- Updating the computer's protection
- About security policies
- Updating the policy file manually
- Verifying that policies have been updated
- Scanning your computer immediately
- Pausing and delaying scans
- Enabling and disabling protection technologies
- About Tamper Protection
- Enabling, disabling, and configuring Tamper Protection
- Testing the security of your computer
- About locations
- Changing locations
- About the notification area icon
- Hiding and displaying the notification area icon
- About preventing an administrator from restarting your computer
About centrally managed clients and self-managed clients

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

### Table 3-1

<table>
<thead>
<tr>
<th>Client type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Centrally managed client | A centrally managed client communicates with a management server in your network. The administrator configures the protection and the default settings, and the management server downloads the settings to the client. If the administrator makes a change to the protection, the change is almost immediately downloaded to the client. Administrators can change the level at which you interact with the client in the following ways:  
  - The administrator manages the client completely.  
    You are not required to configure the client. All the settings are locked or unavailable, but you can view information about what the client does on your computer.  
  - The administrator manages the client, but you can change some client settings and perform some tasks. For example, you may be able to run your own scans and manually retrieve client updates and protection updates.  
    The availability of the client settings, as well as the values of the settings themselves, can change periodically. For example, a setting might change when your administrator updates the policy that controls your client’s protection.  
  - The administrator manages the client, but you can change all the client settings and perform all the protection tasks. |
Table 3-1  Differences between a centrally managed client and a self-managed client (continued)

<table>
<thead>
<tr>
<th>Client type</th>
<th>Description</th>
</tr>
</thead>
</table>
| Self-managed client | A self-managed client does not communicate with a management server and an administrator does not manage the client.  
A self-managed client can be one of the following types:  
■ A standalone computer that is not connected to a network, such as a home computer or a laptop. The computer must include a Symantec Endpoint Protection 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 “Converting a self-managed client to a centrally managed client” on page 29.

Table 3-2 describes the differences in the user interface between a centrally managed and self-managed client.

Table 3-2  Differences between a centrally managed client and a self-managed client by feature area

<table>
<thead>
<tr>
<th>Feature area</th>
<th>Centrally managed client</th>
<th>Self-managed client</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus and Antispyware</td>
<td>The client displays a locked padlock option and the option appears dimmed for the options that you cannot configure.</td>
<td>The client does not display either a locked padlock or an unlocked padlock.</td>
</tr>
<tr>
<td>Client management and Network Threat Protection settings</td>
<td>The settings that the administrator controls do not appear.</td>
<td>All the settings appear.</td>
</tr>
</tbody>
</table>

See “About client interaction” on page 19.

Converting a self-managed client to a centrally managed client

If your client is installed as an unmanaged client, you can convert it to a managed client. A managed client communicates with the management server and receives
content definition updates and configuration information. An unmanaged client does not communicate with a management server.

See “About centrally managed clients and self-managed clients” on page 28.

To convert an unmanaged client to a managed client, you import a sylink.xml file that contains the communication settings. Your administrator must either send you the file or save it to a location that you can access. The default name for the file is group name_sylink.xml.

After you have imported the communications file, the notification area icon appears in the lower-right hand corner of the desktop.

See “About the notification area icon” on page 44.

To convert an unmanaged client to a managed client

1. In the client, click Help and Support, and then click Troubleshooting.
2. In the Management dialog box, under Communication Settings, click Import.
3. In the Import Communication Settings dialog box, locate the group name_sylink.xml file, and then click Open.
4. Click Close.

Updating the computer's protection

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

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

Protection updates can include the following files:

- Virus definition files for Antivirus and Antispyware Protection.
  See “How antivirus and antispyware scans work” on page 64.

- Heuristic signatures and commercial application lists for Proactive Threat Protection.

- IPS definition files for Network Threat Protection.
  See “About managing Network Threat Protection” on page 104.
Product updates are improvements to the installed client. Product updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis. The client receives product updates directly from a LiveUpdate server. A centrally managed client can also receive product updates automatically from a management server at your company.

Table 3-3  Ways to update content on your computer

<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 a self-managed client, you can disable or change a LiveUpdate schedule.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the content on a schedule” on page 32.</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 31.</td>
</tr>
</tbody>
</table>

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

Updating the content immediately

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

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

See “Updating the content on a schedule” on page 32.

See “Updating the computer’s protection” on page 30.

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 run LiveUpdate during a time that you do not use your computer.

See “Updating the content immediately” on page 31.

Note: You can only configure LiveUpdate to run on a schedule if your administrator has enabled you to.

To update your protection on a schedule

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

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

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

About security policies

A security policy is a collection of security settings that the administrator of a managed client configures and deploys to clients. Security policies determine your client's settings, including the options that you can view and access.

See “About centrally managed clients and self-managed clients” on page 28.
Managed clients are connected to the management server and automatically receive the latest security policies. If you have difficulty with network access, your administrator may instruct you to manually update to your policy file. See “Updating the policy file manually” on page 33.

### Updating the policy file manually

The settings that control protection on the client are stored on the computer in a policy file. The policy file updates the settings for Antivirus and Antispyware Protection, Network Threat Protection, Proactive Threat Protection, and Network Access Control. This policy file normally updates automatically. However, you can also update the policy file manually if you do not want to wait until the policy file is updated.

**Note:** You can view the System log to verify that the operation updated the policy successfully.

See “About security policies” on page 32.

See “Verifying that policies have been updated” on page 33.

**To update the policy file manually**

1. In the Windows notification area, right-click the client icon.
2. In the pop-up menu, click **Update Policy**.

### Verifying that policies have been updated

When you update a policy on the client, you can check to see whether the client received the policy.

See “About security policies” on page 32.

See “Updating the policy file manually” on page 33.

**To verify that the client computers obtained updated policies**

1. On the client computer, in the main Symantec Endpoint Protection window, click **View Logs**.
2. Beside Client Management, click **View Logs**, and then click **System Log**.
   
   You see an entry for the policy update that contains the serial number.
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 69.

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 Antivirus and Antispyware Protection, click Options > Run Active Scan.
  - In the client, in the sidebar, click Scan for threats.
    Do one of the following actions:
    - Click Run Active Scan.
    - Click Run Full Scan.
    - In the scan list, right-click any scan, and then click Scan Now.
      The scan starts. A progress window appears on your computer to show the progress of the scan and the results.

    You can also pause or cancel the scan.

    See “Pausing and delaying scans” on page 34.

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 not supported on 64-bit operating systems.

Pausing and delaying scans

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

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

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

**To pause a scan you initiated**

1. When the scan runs, in the scan dialog box, click **Pause Scan**.
   
   The scan stops where it is and the scan dialog box remains open until you start the scan again.

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

**To pause or delay an administrator-initiated scan**

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

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

---

**Enabling and disabling protection technologies**

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

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

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

**Table 3-4** describes the reasons why you might want to disable each protection technology.
### Table 3-4 Purpose for disabling a protection technology

<table>
<thead>
<tr>
<th>Protection technology</th>
<th>Purpose for disabling the protection technology</th>
</tr>
</thead>
</table>
| Antivirus and Antispyware Protection          | If you disable this protection, you disable Auto-Protect only. The scheduled or startup scans still run if you or your administrator has configured them to do so.  
You or the administrator can enable or disable Auto-Protect for the following reasons:  
- Auto-Protect might block you from opening a document. For example, if you open a Microsoft Word that has a macro, Auto-Protect may not allow you to open it. If you know the document is safe, you can disable Auto-Protect.  
- Auto-Protect may warn you about a virus-like activity that you know is not the work of a virus. For example, you might get a warning when you install new computer applications. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect.  
- Auto-Protect may interfere with Windows driver replacement.  
- Auto-Protect might slow down the client computer.  
See “Enabling or disabling Auto-Protect” on page 38. |
| Proactive Threat Protection                   | You might want to disable Proactive Threat Protection for the following reasons:  
- You see too many warnings about the threats that you know are not threats.  
- Proactive Threat Protection might slow down the client computer.  
See “Enabling or disabling Proactive Threat Protection” on page 39. |
Table 3-4  Purpose for disabling a protection technology (continued)

<table>
<thead>
<tr>
<th>Protection technology</th>
<th>Purpose for disabling the protection technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Threat Protection</td>
<td>You might want to disable Network Threat Protection for the following reasons:</td>
</tr>
<tr>
<td></td>
<td>■ You install an application that might cause the firewall to block it.</td>
</tr>
<tr>
<td></td>
<td>■ A firewall rule or firewall setting blocks an application due to an administrator's mistake.</td>
</tr>
<tr>
<td></td>
<td>■ The firewall or the intrusion prevention system causes network connectivity-related issues.</td>
</tr>
<tr>
<td></td>
<td>■ The firewall might slow down the client computer.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling or disabling Network Threat Protection” on page 39.</td>
</tr>
<tr>
<td></td>
<td>See “Enabling or disabling intrusion prevention settings” on page 123.</td>
</tr>
</tbody>
</table>

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

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

See “About excluding items from being scanned” on page 80.

When any of the protections are disabled:

- The status bar at the top of the Status page is red.
- The client's icon appears with a universal no sign, a red circle with a diagonal slash. The client icon appears as a full shield in the taskbar in the lower-right corner of your Windows desktop. In some configurations, the icon does not appear.
  
  See “About the notification area icon” on page 44.

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

**To enable protection technologies from the Status page**

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

**To enable or disable protection technologies from the taskbar**

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

Click Disable Symantec Endpoint Protection.

See “Enabling, disabling, and configuring Tamper Protection” on page 41.

Enabling or disabling Auto-Protect

You can enable or disable File System Auto-Protect for files and processes, Internet email, and email groupware applications. When any type of Auto-Protect is disabled, the antivirus and antispyware 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 “Enabling and disabling protection technologies” on page 35.

Note: On a centrally managed client, your administrator might lock Auto-Protect so that you cannot disable it. Also, 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.

To enable or disable File System Auto-Protect

◆ In the client, on the Status page, next to Antivirus and Antispyware Protection, do one of the following actions:

To enable or disable Auto-Protect for email

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

2 Next to Antivirus and Antispyware 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 or disabling Network Threat Protection**

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

See “**Enabling and disabling protection technologies**” on page 35.

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

Your administrator may have set the following limits for when and how long you can disable protection:

- Whether the client allows either all traffic or all outbound traffic only.
- The length of time the protection is disabled.
- How many times you can disable protection before you restart the client.

See “**Managing firewall protection**” on page 104.

See “**Blocking and unblocking an attacking computer**” on page 125.

**To enable or disable Network Threat Protection**

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

**Enabling or disabling Proactive Threat Protection**

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

Proactive Threat Protection is enabled when both the **Scan for trojans and worms** and the **Scan for keyloggers** settings are enabled. If one setting or the other is disabled, the client shows the Proactive Threat Protection status as disabled.

On a centrally managed client, your administrator might lock Proactive Threat Protection so that you cannot disable it. Proactive Threat Protection is disabled

See “About TruScan proactive threat scans” on page 91.

To enable or disable Proactive Threat Protection

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

About Tamper Protection

Tamper Protection provides real-time protection for Symantec applications. It thwarts attacks by malicious software such as worms, Trojan horses, viruses, and security risks.

You can set Tamper Protection to take the following actions:

- Block tamper attempts and log the event
- Log the tampering event but do not interfere with the tampering event

Tamper Protection is enabled for both the managed clients and the unmanaged clients, unless your administrator has changed the default settings. When Tamper Protection detects a tampering attempt, the action it takes by default is to log the event in the Tamper Protection Log. You can configure Tamper Protection to display a notification on your computer when it detects a tampering attempt. You can customize the message. Tamper Protection does not notify you about attempts to tamper unless you enable that functionality.

If you use an unmanaged client, you can change your Tamper Protection settings. If you use a managed client, you can change these settings if your administrator allows it.

A best practice when you initially use Symantec Endpoint Protection is to leave the default action Log the event only while you monitor the logs once a week. When you are comfortable that you see no false positives, then set Tamper Protection to Block it and log the event
Note: If you use a third-party security risk scanner that detects and defends against unwanted adware and spyware, the scanner typically impacts Symantec processes. If you have Tamper Protection enabled while you run a third-party security risk scanner, Tamper Protection generates a large number of notifications and log entries. A best practice is to always leave Tamper Protection enabled, and to use log filtering if the number of events that are generated is too large.

See “Enabling, disabling, and configuring Tamper Protection” on page 41.

Enabling, disabling, and configuring Tamper Protection

You can enable or disable Tamper Protection. 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: If an administrator manages your computer, and these options display a padlock icon, you cannot change these options because your administrator has locked them.

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

See “About Tamper Protection” on page 40.

To enable or disable Tamper Protection

1. In the main window, in the sidebar, click Change settings.
2. Beside 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 main window, in the sidebar, click Change settings.
2. Beside 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**.

## Testing the security of your computer

You can test the effectiveness of your computer to outside threats and viruses by scanning it. This scan is an important step that you can take to ensure that your computer is protected from possible intruders. The results can help you to set the various options on the client to protect your computer from attack.

**To test the security of your computer**

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

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

3 Click **Tools > Test Network Security**.

4 In the Symantec Security Check Web site, do one of the following:
   - To check for online threats, click **Security Scan**.
   - To check for viruses, click **Virus Detection**.

5 In the End-user License Agreement dialog box, click **I accept**, and then click **Next**.

   If you clicked Virus Detection in step 4, click **I consent**, and then click **Next**.

   If you want to stop the scan at any time, click **Stop**.

6 When the scan is finished, close the dialog box.

## About locations

A location refers to a security policy that is based on your network environment. For instance, if you connect to the office network by using your laptop from home, your administrator can set up a location named Home. If you use the laptop in
the office, you may use a location named Office. Other locations may include VPN, branch office, or hotel.

The client switches between these locations because your security needs and usage needs can differ between network environments. For example, when your laptop connects to your office network, your client might use a restrictive set of policies that your administrator configured. When it connects to your home network, however, your client might use a policy set that gives you access to more configuration options. Your administrator plans and configures your client accordingly, so that the client bridges those differences automatically for you.

**Note:** In a managed environment, you can change locations only if your administrator has provided the necessary access.

See “Changing locations” on page 43.

### Changing locations

You can change a location if necessary. For example, you might need to switch to a location that lets a colleague access files on your computer. The list of locations that are available is based on your security policies and on your computer's active network.

See “About locations” on page 42.

**Note:** Based on the available security policies, you may or may not have access to more than one location. You may find that when you click a location, you do not change to that location. This means that your network configuration is not appropriate for that location. For example, a location that is called Office may be available only when it detects the office local area network (LAN). If you are not currently on that network, you cannot change to that location.

**To change a location**

1. In the client, in the sidebar, click **Change settings**.
2. On the **Change Settings** page, beside **Client Management**, click **Configure Settings**.
3. On the **General** tab, under **Location Options**, select the location to which you want to change.
4. Click **OK**.
About the notification area icon

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

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

Table 3-5 displays the Symantec Endpoint Protection client status icons that appear in the notification area.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Icon" /></td>
<td>The client runs with no problems. It is either offline or self-managed. Self-managed clients are not connected to a management server. The icon is a plain yellow shield.</td>
</tr>
<tr>
<td><img src="image2" alt="Icon" /></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="image3" alt="Icon" /></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="image4" alt="Icon" /></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 3-6 displays the Symantec Network Access Control client status icons that appear in notification area.

<table>
<thead>
<tr>
<th>Icon</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image5" alt="Icon" /></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 self-managed. Self-managed clients are not connected to a management server. The icon is a plain gold key.</td>
</tr>
</tbody>
</table>
Table 3-6  Symantec Network Access Control client status icons (continued)

<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 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 45.

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 “About the notification area icon” on page 44.

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 preventing an administrator from restarting your computer

Typically administrators can run commands remotely on your client computer. For security reasons, you might want to prevent an administrator from remotely restarting your computer.
You must set a Windows registry key on the client computer, which blocks any restart command from the management server. On the client computer, you can set the DisableRebootCommand key to 1. Then, if an administrator selects the **Restart Client Computers** command from the console, the client computer does not restart.
Managing protection on the Symantec Endpoint Protection client

- Chapter 4. Managing Antivirus and Antispyware Protection
- Chapter 5. Managing Proactive Threat Protection
- Chapter 6. Managing Network Threat Protection
Managing Antivirus and Antispyware Protection

This chapter includes the following topics:

- About viruses and security risks
- How the client responds to viruses and security risks
- About antivirus and antispyware settings
- About scanning files
- When the client detects a virus or security risk
- About Auto-Protect
- Working with antivirus and antispyware scans
- Scheduling a user-defined scan
- Editing and deleting startup, user-defined, and scheduled scans
- Interpreting scan results
- Configuring actions for viruses and security risks
- Configuring notifications for viruses and security risks
- About excluding items from being scanned
- Excluding items from being scanned
- About handling quarantined files
- Managing the quarantine
About viruses and security risks

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

Antivirus and antispyware scans also detect kernel-level rootkits. Rootkits are any programs that try to hide themselves from a computer's operating system and could be used for malicious purposes.

Table 4-1 describes the types of viruses and malware that the client protects against.
Table 4-1  Viruses, Trojan horses, and worms

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

Table 4-2 describes the types of security risks that the client protects against.

Table 4-2  Types of security risks

<table>
<thead>
<tr>
<th>Security risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious Internet bots</td>
<td>The programs that run automated tasks over the Internet for malicious purposes. Bots can be used to automate attacks on computers or to collect information from Web sites.</td>
</tr>
<tr>
<td>Blended threats</td>
<td>The threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage throughout the network.</td>
</tr>
<tr>
<td>Adware</td>
<td>The programs that secretly gather personal information through the Internet and relay it back to another computer. Adware may track browsing habits for advertising purposes. Adware can also deliver advertising content.</td>
</tr>
<tr>
<td>Dialers</td>
<td>The programs that use a computer, without the user's permission or knowledge, to dial a 900 number or an FTP site. The programs typically accrue charges.</td>
</tr>
</tbody>
</table>
Table 4-2  Types of security risks (continued)

<table>
<thead>
<tr>
<th>Security risk</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacking tools</td>
<td>The programs that hacker use to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.</td>
</tr>
<tr>
<td>Joke programs</td>
<td>The programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can then move the Recycle Bin away from the mouse when the user tries to delete it. It can also cause the mouse to click in reverse.</td>
</tr>
<tr>
<td>Other</td>
<td>Any other security risks that do not conform to the strict definitions of viruses, Trojan horses, worms, or other security risk categories.</td>
</tr>
<tr>
<td>Remote access programs</td>
<td>The programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. You might install a legitimate remote access program. A process might install this type of application without your knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.</td>
</tr>
<tr>
<td>Spyware</td>
<td>The programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer. Spyware can be downloaded from Web sites, email messages, instant messages, and from direct-file connections. Additionally, a user may unknowingly receive spyware by accepting an End User License Agreement from a software program.</td>
</tr>
<tr>
<td>Trackware</td>
<td>The standalone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.</td>
</tr>
</tbody>
</table>

By default, the scans do the following:

- Detect, remove, and repair the side effects of viruses, worms, Trojan horses, and blended threats.
- Detect, remove, and repair the side effects of security risks such as adware, dialers, hacking tools, joke programs, remote access programs, spyware, trackware, and others.
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.

How the client responds to viruses and security risks

The client safeguards computers from viruses and security risks no matter what the source. Computers are protected from the viruses and security risks that spread from hard drives and floppy disks, and the others that travel across networks. Computers are also protected from the viruses and security risks that spread through email attachments or some other means. For example, a security risk may install itself on your computer without your knowledge when you access the Internet.

Files within compressed files are scanned and cleaned of viruses and security risks. No separate programs or options changes are necessary for Internet-borne viruses. Auto-Protect scans uncompressed program and document files automatically as they are downloaded.

When the client detects a virus, by default the client tries to clean the virus from the infected file. The client also tries to repair the effects of the virus. If the client cleans the file, the client completely removes the risk from your computer. If the client cannot clean the file, the client moves the infected file to the Quarantine. The virus cannot spread 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.

**Note:** Your administrator may choose to scan files in the Quarantine automatically.

By default, for security risks, the client quarantines the infected files. The client also returns the system information that the security risk has changed to its previous state. Some security risks cannot be completely removed without causing another program on your computer, such as a Web browser, to fail. Your antivirus and antispyware settings might not handle the risk automatically. In that case, the client prompts you before it stops a process or restarts your computer. Alternatively, you can configure your settings to use the log only action for security risks.

When the client software discovers security risks, it includes a link in the scan window to Symantec Security Response. On the Symantec Security Response Web
site you can learn more about the security risk. Your administrator may also send a customized message.

About antivirus and antispyware settings

The client includes the default antivirus and antispyware settings that are appropriate for most users. You can change the settings to customize them for your security network. You can customize policy settings for Auto-Protect, scheduled, startup, and on-demand scans.

Antivirus and antispyware settings include the following settings:

- What to scan
- What to do if a virus or security risk is detected

About scanning files

Antivirus and antispyware scans scan all file types by default. Scheduled, startup, and on-demand scans also examine all file types by default.

You can choose to scan files by file extension, but you reduce your protection from viruses and security risks. If you select file extensions to scan, Auto-Protect can determine a file's type even if a virus changes the file's extension.

See “Configuring Auto-Protect to determine file types” on page 60.

You can also choose to exclude specific files from scans. For example, you might know that a file does not trigger a virus alert during a scan. You can exclude the file from your subsequent scans.

If your email application uses a single Inbox file

If your email application stores all email in a single file, you should create a centralized exception to exclude the Inbox file from scans. The email applications that store all email in a single Inbox file include Outlook Express, Eudora, Mozilla, or Netscape. The client might be configured to quarantine a virus that it detects. If the client detects the virus in the Inbox file, the client quarantines the entire Inbox. If the client quarantines the Inbox, you cannot access your email.

Symantec does not usually recommend that you exclude files from scans. However, when you exclude the Inbox file from scans, the client can still detect any viruses when you open email messages. If the client finds a virus when you open an email message, it can safely quarantine or delete the message.

You can exclude the file by configuring a centralized exception.
About scanning by extension

The client can scan your computer by extensions.

You can choose from the following types of file extensions:

- **Document files**: Include Microsoft Word and Excel documents, and the template files that are associated with those documents. The client searches document files for macro virus infections.

- **Program files**: Include dynamic-link libraries (.dll), batch files (.bat), command files (.com), executable files (.exe), and other program files. The client searches program files to look for file virus infections.

**To add file extensions to the scan list for Auto-Protect scans**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. In the **Antivirus and Antispyware Protection Settings** dialog box, on the **File System Auto-Protect** tab, under **File Types**, click **Selected**.
4. Click **Extensions**.
5. In the text box, type the extension to add, and then click **Add**.
6. Repeat step 5 as needed, and then click **OK**.
7. Click **OK**.

**To add file extensions to the scan list for an on-demand, scheduled, or startup scan**

1. In the client, in the sidebar, click **Scan for threats**.
2. Right-click the scan for which you want to add file extensions, and then select **Edit**.

   Changes apply only to the specific scan that you select.

3. On the **Scan Options** tab, under **File Types**, select **Selected extensions**, and then click **Extensions**.
4. Type the extension to add, and then click **Add**.
5. Repeat step 4 as needed, and then click **OK**.
6. Click **OK**.

About scanning all file types

The client can scan all of the files on your computer, regardless of extension.

Scanning all files ensures the most thorough protection. Scanning all files is more...
time-consuming than scanning by extensions, but you are better protected from viruses and security risks.

About preventing macro virus infections

The client automatically detects and removes most Microsoft Word and Excel macro viruses. When you regularly run scheduled scans, you can protect your computer from macro virus infections. Auto-Protect also regularly searches and cleans any macro viruses that it detects.

To best prevent macro virus infections, do the following actions:

■ Enable Auto-Protect.
  Auto-Protect constantly scans the files that have been accessed or modified.

■ Run Auto-Protect for your email, if available.

■ Protect your global template files by disabling automatic macros.

When the client detects a virus or security risk

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

By default, when the client detects a virus, the client tries first to clean the virus from the infected file. Then, if the client cannot clean the file, it logs the failure and moves the infected file to the Quarantine.

By default, when the client detects a security risk, it quarantines the risk. It also 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.

Note: In the Quarantine, the risk cannot spread. When a client moves a file to the Quarantine, you do not have access to the file. The client can also reverse its changes for the items that it quarantines.

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.
Note: 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.

About Auto-Protect

Auto-Protect is your best defense against virus attacks. Whenever you access, copy, save, move, or open a file, Auto-Protect scans the file to ensure that a virus has not attached itself.

Auto-Protect scans the file extensions that contain executable code and all .exe and .doc files. Auto-Protect can determine a file's type even when a virus changes the file's extension. For example, a virus might change a file's extension to one that is different from the file extensions that you configured Auto-Protect to scan.

You can enable or disable Auto-Protect if your administrator does not lock the setting.

About Auto-Protect and security risks

By default, Auto-Protect does the following actions:

- Scans for security risks such as adware and spyware
- Quarantines the infected files
- Removes or repairs the side effects of the security risks

You can disable scanning for security risks in Auto-Protect.

See “Disabling and enabling Auto-Protect security risk scanning and blocking” on page 61.

If Auto-Protect detects a process that continuously downloads a security risk to your computer, Auto-Protect displays a notification and logs the detection. (Auto-Protect must be configured to send notifications.) If the process continues to download the same security risk, multiple notifications appear on your computer and Auto-Protect logs multiple events. To prevent multiple notifications and logged events, Auto-Protect automatically stops sending notifications about the security risk after three detections. Auto-Protect also stops logging the event after three detections.
In some situations, Auto-Protect does not stop sending notifications and logging events for the security risk. Auto-Protect continues to send notifications and log events when any of the following situations is true:

■ On client computers, you or your administrator have disabled blocking the installation of security risks (the default setting is enabled).
■ The action for the type of security risk that the process downloads has an action of Leave alone.

About Auto-Protect and email scanning

Auto-Protect also scans supported groupware email clients. Protection is provided for the following email clients:

■ Lotus Notes 4.5x, 4.6, 5.0, and 6.x
■ Microsoft Exchange client 5.0 and 5.5

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

Auto-Protect also scans additional Internet email programs by monitoring all traffic that uses the POP3 or SMTP communications protocols. You can configure the client software to scan incoming and outgoing messages for risks. Scans of outgoing email help to prevent the spread of threats that use email clients to replicate and distribute themselves across a network.

*Note:* Internet email scanning is not supported for 64-bit computers.

For scans of Lotus Notes and Microsoft Exchange email, Auto-Protect scans only the attachments that are associated with email.

For Internet email scanning of the messages that use the POP3 or SMTP protocols, Auto-Protect scans the following items:

■ The body of the message
■ Any attachments to the message

When you open a message with an attachment, the attachment is immediately downloaded to your computer and scanned when the following statements are true:
You use Microsoft Exchange client or Microsoft Outlook over MAPI.

You have Auto-Protect enabled for email.

Over a slow connection, downloading messages with large attachments affects mail performance. You may want to disable this feature if you regularly receive large attachments.

See “Disabling and enabling Auto-Protect security risk scanning and blocking” on page 61.

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

Email scanning does not support the following email clients:

- IMAP clients
- AOL clients
- Web-based email such as Hotmail, Yahoo! Mail, and GMAIL

**Disabling Auto-Protect handling of encrypted email connections**

You can send and receive email over a secure link. 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.

Even though Auto-Protect does not scan the email that uses secure connections, Auto-Protect continues to protect computers from risks in attachments. Auto-Protect scans email attachments when you save the attachment to the hard drive.

**Note:** For performance reasons, Internet Email Auto-Protect for POP3 is not supported on server operating systems.

You can disable the handling of encrypted email if you need to do so. When these options are disabled, Auto-Protect scans the unencrypted email that is sent or received, but Auto-Protect blocks encrypted email. If you turn on the options and then try to send encrypted email, Auto-Protect blocks the email until you restart your email application.
Note: If you disable encrypted connections for Auto-Protect, the change does not take effect until you log off Windows and log on again. If you need to be sure that your change took effect immediately, log off and log on again.

To disable Auto-Protect handling of encrypted email connections
1. In the client, in the sidebar, click Change settings.
2. Next to Antivirus and Antispyware Protection, click Configure Settings.
3. On the Internet Email Auto-Protect tab, click Advanced.
4. Under Connection settings, uncheck Allow encrypted POP3 connections and Allow encrypted SMTP connections.
5. Click OK.

Viewing Auto-Protect scan statistics
Auto-Protect Scan Statistics displays the status of the last Auto-Protect scan, the last file that was scanned, and virus infection and security risk information.

To view Auto-Protect scan statistics
• In the client, on the Status page, next to Antivirus and Antispyware Protection, click Options > View File System Auto-Protect Statistics.

Viewing the risk list
You can view the current risks that the client detects. The list corresponds to your current virus definitions.

To view the risk list
• In the client, on the Status page, next to Antivirus and Antispyware Protection, click Options > View Threat List.

Configuring Auto-Protect to determine file types
Auto-Protect is preset to scan all files. It may complete scans faster by scanning only files with selected extensions.

For example, you might want to scan only the following extensions:
• .exe
• .com
• .dll
• .doc
Typically viruses affect only certain types of files. If you scan selected extensions, however, you get less protection because Auto-Protect does not scan all files. The default list of extensions represents those files that are commonly at risk of infection by viruses.

Auto-Protect scans the file extensions that contain executable code and all .exe and .doc files. It can also determine a file’s type even when a virus changes the file’s extension. For example, it scans .doc files even if a virus changes the file extension.

You should configure Auto-Protect to scan all file types to ensure that your computer receives the most protection from viruses and security risks.

To configure Auto-Protect to determine file types

1. In the client, in the sidebar, click Change settings.
2. Next to Antivirus and Antispyware Protection, click Configure Settings.
3. On any Auto-Protect tab, under File types, do one of the following actions:
   - Click All types to scan all files.
   - Click Selected to scan only those files that match the listed file extensions, and then click Extensions to change the default list of file extensions.
4. If you chose Selected, check or uncheck Determine file types by examining file contents.
5. Click OK.

Disabling and enabling Auto-Protect security risk scanning and blocking

By default, Auto-Protect does the following actions:

- Scans for security risks such as adware and spyware
- Quarantines the infected files
- Tries to remove or repair the effects of the security risk

In cases where blocking the installation of a security risk does not affect the stability of a computer, Auto-Protect also blocks the installation by default. If Symantec determines that blocking a security risk could compromise a computer’s stability, then Auto-Protect allows the risk to install. Auto-Protect also immediately takes the action that is configured for the risk.

From time to time, however, you might temporarily need to disable scanning for security risks in Auto-Protect scans of files, and then re-enable it. You might also
need to disable blocking security risks to control the time at which Auto-Protect reacts to certain security risks.

**Note:** Your administrator might lock these settings.

**To disable or enable Auto-Protect security risk scanning and blocking**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. On the File System Auto-Protect tab, under Options, do any of the following actions:
   - Check or uncheck **Scan for security risks**.
   - Check or uncheck **Block security risks from being installed**.
   - Check or uncheck **Scan files on network drives**.
4. Click **OK**.

**Configuring network scanning setting**

Configuration for network scans includes the following options:

- Configure whether or not your Auto-Protect trusts files on the remote computers that run Auto-Protect.
- Specify whether or not your computer should use a cache to store a record of the files that Auto-Protect scans from a network.

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.

When you read files on a remote computer, however, Auto-Protect might not scan the files. By default, Auto-Protect tries to trust remote versions of Auto-Protect. If the trust option is enabled on both computers, the local Auto-Protect checks the remote computer’s Auto-Protect settings. If the remote Auto-Protect settings provide at least as high a level of security as the local settings, the local Auto-Protect trusts the remote Auto-Protect. When the local Auto-Protect trusts the remote Auto-Protect, the local Auto-Protect does not scan the files that it reads from the remote computer. The local computer trusts that the remote Auto-Protect already scanned the files.

**Note:** The local Auto-Protect always scans the files that you copy from a remote computer.
The trust option is enabled by default. If you disable the trust option, you might reduce network performance.

To disable trust in remote versions of Auto-Protect
1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. On the File System Auto-Protect tab, click **Advanced**.
4. In the Auto-Protect Advanced Options dialog box, under Additional Advanced Options, click **Network**.
5. Under Network scanning settings, uncheck **Trust files on remote computers running Auto-Protect**.
6. Click **OK** until you return to the main window.

You can configure your computer to use a network cache. 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. When you prevent multiple scans of the same file, you might improve system performance. You can set the number of files (entries) that Auto-Protect scans and remembers. You can also set the timeout before your computer removes the entries from the cache. When the timeout expires, your computer removes the entries. Auto-Protect then scans the files if you request them from the remote computer again.

To configure a network cache
1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. In the Antivirus and Antispyware Settings dialog box, on the File System Auto-Protect tab, click **Advanced**.
4. In the Auto-Protect Advanced Options dialog box, under Additional advanced options, click **Network**.
5. In the Network Scanning Settings dialog box, check or uncheck **Network cache**.
6. If you enabled the network cache, use the defaults or do any of the following actions:
   - Use the arrows or type in the number of files (entries) that you want Auto-Protect to scan and remember.
Type the number of seconds for which you want entries to remain in the cache before your computer clears the cache.

7 Click OK until you return to the main window.

Working with antivirus and antispyware scans

Auto-Protect is your most powerful defense against virus infection and security risks. In addition to Auto-Protect, the client includes several different types of scans to provide additional protection.

Table 4-3 describes the types of scans.

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom Scan</td>
<td>Scans a file, folder, drive, or entire computer at any time. You select the parts of the computer to scan.</td>
</tr>
<tr>
<td>Active Scan</td>
<td>Quickly scans system memory and the locations that viruses and security risks commonly attack.</td>
</tr>
<tr>
<td>Full Scan</td>
<td>Scans the entire computer, including the boot sector and system memory. You might need to enter a password to scan network drives.</td>
</tr>
<tr>
<td>Scheduled Scan</td>
<td>Runs unattended at a specified frequency.</td>
</tr>
<tr>
<td>Startup Scan</td>
<td>Runs every time you start your computer and log on.</td>
</tr>
<tr>
<td>User-defined</td>
<td>Scans the specified file sets at any time.</td>
</tr>
</tbody>
</table>

As long as Auto-Protect is enabled, a daily Active Scan and a single, weekly scheduled scan of all files provides sufficient protection. If viruses frequently attack your computer, consider adding a full scan at startup or a daily scheduled scan.

You can also configure the frequency of the scans that look for suspicious behavior rather than known risks.

See “Configuring how often to run TruScan proactive threat scans” on page 95.

How antivirus and antispyware scans work

Protection scans identify and neutralize or eliminate viruses and security risks on your computers. A scan eliminates a virus or risk by using the following process:
The scan engine searches within files and other components on the computer for traces of viruses within files. Each virus has a recognizable pattern that is called a signature. Installed on the client is a virus definitions file that contains the known virus signatures, without the harmful virus code. The scan engine compares each file or component with the virus definitions file. If the scan engine finds a match, the file is infected.

The scan engine uses the definitions files to determine whether a virus or a risk caused the infection. The scan engine then takes a remediation action on the infected file. To remediate the infected file, the client cleans, deletes, or quarantines the file.

Table 4-4 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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>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>
</tbody>
</table>
Table 4-4  Computer components that the client scans (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 definitions files

Virus files include any bits of code that display certain patterns when they are broken down. The patterns can be traced in infected files. The patterns are also called signatures. Security risks, such as adware and spyware, also have recognizable signatures.

Virus definitions files contain a list of known virus signatures, without the harmful virus code, and known signatures for security risks. The scan software searches within files on your computer for the known signatures that are included in the definitions files. If a virus match is found, the file is infected. The client uses the definitions files to determine which virus caused the infection and to repair its side effects. If a security risk is found, the client uses the definitions files to quarantine the risk and repair its side effects.

New viruses and security risks are introduced into the computer community regularly. You should make sure that the definitions files on your computer are up to date. You should make sure that the client can detect and clean even the most recent viruses and security risks.

About scanning compressed files

Antivirus and antispyware scans scan within compressed files. For example, the scans scan files inside .zip files. Your administrator can specify scanning up to 10 levels deep for the compressed files that contain compressed files. Check with your administrator for the types of compressed file scans that are supported.

If Auto-Protect is enabled, any file within a compressed file is scanned.

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

See “**Scanning your computer immediately**” on page 34.

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

**To schedule a user-defined scan**

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

   **Active Scan**
   Scans the areas of the computer that viruses and security risks most commonly infect.

   **Full Scan**
   Scans the entire computer for viruses and security risks.

   **Custom Scan**
   Scans the selected areas of the computer for viruses and security risks.

4. Click **Next**.
5 If you selected **Custom 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.

- **Centralized Exceptions** Add items that the client excludes from being scanned.

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

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

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

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

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

For example, call the scan: Friday morning

11 Click Finish.

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

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

Your client also includes a startup scan that is called the Auto-Generated Active Scan. The auto-generated scan checks the common infection points on the computer each time a user logs on to the computer. You can edit this scan in the same way that you can configure any on-demand scan. However, you cannot disable the scans of the files in the memory and the other common infection points on the computer.

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 34.

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

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

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

2 Click Create a New Scan.
3 Follow steps 3 to 7 for creating a scheduled scan.
See “Scheduling a user-defined scan” on page 66.

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.

Editing and deleting startup, user-defined, and scheduled scans

You can edit and delete existing startup, user-defined, and scheduled scans. Certain options may be unavailable if they are not configurable for a particular type of scan.

To edit a scan
1 In the client, in the sidebar, click Scan for threats.
2 In the scans list, right-click the scan that you want to edit, and then click Edit.
3 Make any changes on the What to scan, Options, and General tabs.
   For scheduled scans, you can also modify the schedule.
4 Click OK.

To delete a scan
1 In the client, in the sidebar, click Scan for threats.
2 In the scans list, right-click the scan that you want to delete, and then click Delete.
3 In the Confirm Deletion dialog box, click Yes.
Interpreting scan results

Whenever an on-demand, scheduled, startup, or user-defined scan runs, by default the client software 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.

In a centrally managed network, the scan progress dialog box might not appear for administrator-initiated scans. Similarly, your administrator may choose not to display results when the client detects a virus or security risk.

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

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

By default, you are notified whenever a virus or security risk is detected.

---

**Note:** The language of the operating system on which you run the client might not be able to interpret some characters in virus names. 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.

---

If you configure the client software to display a scan progress dialog box, you can pause, restart, or stop the scan. When the scan is completed, results appear in the list. If no viruses or security risks are detected, the list remains empty and the status is completed.

See “Pausing and delaying scans” on page 34.

---

About interacting with scan results or Auto-Protect results

The scan progress dialog box and the Auto-Protect results dialog box have similar options. If the client needs to terminate a process or application or stop a service, the Remove Risk option is active. You might not be able to close the dialog box if risks in the dialog require you to take action.

*Table 4-5* describes the options in the scan results dialog box.
Table 4-5 Options in the scan results dialog box

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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>■ Yes</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>■ No</td>
</tr>
<tr>
<td></td>
<td>When you close the results dialog box, a dialog box appears. The dialog box reminds you that you still need to take action. However, the Remove Risk dialog is suppressed until you restart your computer.</td>
</tr>
<tr>
<td>Close</td>
<td>Closes the results dialog box if you do not need to take action on any of the risks</td>
</tr>
<tr>
<td></td>
<td>If you need to take action, one of the following notifications appears:</td>
</tr>
<tr>
<td></td>
<td>■ Remove Risk Required.</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>■ Restart Required.</td>
</tr>
<tr>
<td></td>
<td>Appears when a risk requires a restart.</td>
</tr>
<tr>
<td></td>
<td>■ Remove Risk and Restart Required.</td>
</tr>
<tr>
<td></td>
<td>Appears when a risk requires process termination and another risk requires a restart.</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.
Configuring actions for viruses and security risks

You can configure the actions that you want the Symantec Endpoint Protection client to take when it detects a virus or 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. You can click Help for more information about the options that are used in the procedures.

**To configure actions for viruses and security risks**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. On the File System Auto-Protect tab, click **Actions**.
4. In the Scan Actions dialog box, in the tree, select a type of virus or security risk.
   
   By default, each security risk subcategory is automatically configured to use the actions that are set for the entire Security Risks category.

5. To configure a category or specific instances of a category to use different actions, check **Override actions configured for Security Risks**, and then set the actions for that category only.

See “Acting on infected files” on page 20.
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 macro and non-macro viruses.

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.

See “Tips for assigning second actions for viruses” on page 76.

See “Tips for assigning second actions for security risks” on page 76.

7 Repeat steps 1 and 6 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**.
Tips for assigning second actions for viruses

When you select a second action for viruses, consider the following situations:

How you manage files on your computer
If you store important files on your computer without backing them up, you should not use actions like Delete risk. Though you may delete a virus this way, you can lose important data.

Another consideration is your system files. Viruses typically attack executable files. You can use the Leave alone (log only) or Quarantine risk action so that you can check which files have been infected. For example, a virus might attack Command.com. If the client could not clean the infection, you might not be able to restore the file. The file is critical to your system. You can use the Leave alone action to make sure the file is accessible.

The type of virus that has infected your computer
Different types of viruses target different areas of your computer for infection. Boot viruses infect boot sectors, partition tables, master boot records, and sometimes memory. When boot viruses are multipartite, they may also infect executable files, and the infection can be treated similarly to a file virus. File viruses typically infect the executable files that have .exe, .com, or .dll extensions. Macro viruses infect the document files and the macros that are associated with those documents. Select the actions that are based on the types of files that you might need to recover.

The type of scan that you run on your computer
All scans perform actions automatically without your consent. If you do not change the actions before a scan, the default actions are used. As a result, the default second actions are designed to give you control of a virus outbreak situation. For the scans that run automatically such as scheduled scans and Auto-Protect scans, do not assign the second actions that have permanent effects. For example, you might perform an on-demand scan when you already know that a file is infected. You can limit the Delete risk and Clean risk actions to this on-demand scan.

Tips for assigning second actions for security risks

When you select a second action for security risks, consider the level of control that you need to have over your files. If you store important files on your computer without backing them up, you should not use the Delete risk action. Even though you might delete a security risk this way, you can potentially cause another application on your computer to stop working. Use the Quarantine risk action instead so that you can reverse the changes that the client makes, if necessary.
About risk impact ratings

Symantec assesses security risks to determine how much effect they have on a computer.

The following factors are rated low, medium, or high:

- Privacy impact
- Performance impact
- Stealth
- Removal difficulty

A factor that is rated low has a minimal impact. A factor that is rated medium has some impact. A factor that is rated high has a significant impact in that area. If a particular security risk has not been assessed yet, default ratings are used. If a security risk has been assessed, but a particular factor does not apply to that risk, then a rating of none is used.

These ratings appear in the Security Risk Exceptions dialog box when you configure a centralized exception for known security risks. You can use these ratings to help to determine which security risks to exclude from scans and allow to remain on your computer.

Table 4-6 describes the rating factors and what a high rating means for each of them.

Table 4-6 Risk impact factors

<table>
<thead>
<tr>
<th>Rating factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy Impact</td>
<td>Measures the level of privacy that is lost due to the security risk's presence on the computer. A high rating indicates that personal or other sensitive information may be stolen.</td>
</tr>
<tr>
<td>Performance Impact</td>
<td>Measures the extent to which a security risk degrades a computer's performance. A high rating indicates that performance is seriously degraded.</td>
</tr>
<tr>
<td>Stealth Rating</td>
<td>Measures how easy it is to determine if the security risk is present on a computer. A high rating indicates that the security risk tries to hide its presence.</td>
</tr>
</tbody>
</table>
### Table 4-6  
**Risk impact factors (continued)**

<table>
<thead>
<tr>
<th>Rating factor</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Removal Rating</td>
<td>Measures how difficult it is to remove a security risk from a computer.</td>
</tr>
<tr>
<td></td>
<td>A high rating indicates that the risk is difficult to remove.</td>
</tr>
<tr>
<td>Overall Rating</td>
<td>Overall rating is an average of the other factors.</td>
</tr>
<tr>
<td>Dependent Program</td>
<td>This rating indicates whether or not another application depends on the presence of this security risk to function properly.</td>
</tr>
</tbody>
</table>

### Configuring notifications for viruses and security risks

By default, you are notified when a scan finds a virus or security risk. By default, you are also notified when the scanning software needs to terminate services or stop processes. The scanning software might also need to remove or repair the effects of the virus or security risk.

You can configure the following notifications for scans:

**Detection options**  
Construct the message that you want to appear when the client finds a virus or a security risk on your computer.

When you configure File System Auto-Protect, you can select an additional option to display a dialog box. The dialog box contains the results when Auto-Protect finds risks on your computer.

**Remediation options**  
Configure whether or not you want to be notified when the client finds a virus or a security risk. You can also be notified when the client needs to terminate a process or stop a service to remove or repair a risk.

You can construct the detection message that you want to appear on your computer. To construct the message, you type directly in the message field. You can right-click in the message field to select variables to include in the message.

**Table 4-7** describes the variable fields that are available for notification messages.

### Table 4-7  
**Message variable fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SecurityRiskName</td>
<td>The name of the virus or security risk that was found.</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ActionTaken</td>
<td>The action that the client performed when it detected the virus or security risk. This action can be either the first action or second action that was configured.</td>
</tr>
<tr>
<td>Status</td>
<td>The state of the file: Infected, Not Infected, or Deleted. This message variable is not used by default. To display this information, manually add this variable to the message.</td>
</tr>
<tr>
<td>Filename</td>
<td>The name of the file that the virus or security risk infected.</td>
</tr>
<tr>
<td>PathAndFilename</td>
<td>The complete path and name of the file that the virus or security risk infected.</td>
</tr>
<tr>
<td>Location</td>
<td>The drive on the computer on which the virus or security risk was located.</td>
</tr>
<tr>
<td>Computer</td>
<td>The name of the computer on which the virus or security risk was found.</td>
</tr>
<tr>
<td>User</td>
<td>The name of the user who was logged on when the virus or security risk occurred.</td>
</tr>
<tr>
<td>Event</td>
<td>The type of event, such as “Risk Found.”</td>
</tr>
<tr>
<td>LoggedBy</td>
<td>The type of scan that detected the virus or security risk.</td>
</tr>
<tr>
<td>DateFound</td>
<td>The date on which the virus or security risk was found.</td>
</tr>
<tr>
<td>StorageName</td>
<td>The affected area of the application, for example, File System Auto-Protect or Lotus Notes Auto-Protect.</td>
</tr>
<tr>
<td>ActionDescription</td>
<td>A full description of the actions that were taken in response to detecting the virus or security risk.</td>
</tr>
</tbody>
</table>

You can configure notifications for user-defined scans and for Auto-Protect. The notification configuration includes remediation options. Remediation options are only available for scans and File System Auto-Protect.

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

To configure notifications for viruses and security risks

1. Do one of the following actions:
   - For a new scan, in the Create New Scan - Scan Options dialog box, click Notifications.
For an existing scan, on the Scan Options tab, click Notifications.

For Auto-Protect, in the Antivirus and Antispyware Protection Settings dialog box, on any of the Auto-Protect tabs, click Notifications.

2 In the Scan Notification Options dialog box, under Detection options, you can select the option to notify you when a scan finds a virus or security risk. Check this option if you want a message to appear on your computer when the scan finds a virus or security risk.

3 In the message box, do any or all of the following actions to construct the message that you want:

- Click to type or edit text.
- Right-click, click Insert Field, and then select the variable field that you want to insert.
- Right-click, and then select Cut, Copy, Paste, Clear, or Undo.

4 For Auto-Protect configuration, check or uncheck Display the Auto-Protect results dialog.

This parameter allows or suppresses the dialog box that contains results when File System Auto-Protect finds viruses and security risks.

5 Under Remediation options, check the options that you want to set for the scan or for File System Auto-Protect. The following options are available:

<table>
<thead>
<tr>
<th>Remediation options</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terminate processes automatically</td>
<td>Configures the scan to terminate processes automatically when it needs to do so to remove or repair a virus or security risk. You are not prompted to save data before the scan terminates the processes.</td>
</tr>
<tr>
<td>Stop services automatically</td>
<td>Configures the scan to stop services automatically when it needs to do so to remove or repair a virus or security risk. You are not prompted to save data before the scan stops the services.</td>
</tr>
</tbody>
</table>

6 Click OK.

**About excluding items from being scanned**

Exceptions are known security risks, files, file extensions, processes that you want to exclude from a scan. If you have scanned your computer and know that certain files are safe, you can exclude them. In some cases, exceptions can reduce scan time and increase system performance. Typically you do not need to create exceptions.
For centrally managed clients, your administrator may have created exceptions for your scans. If you create an exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.

Table 4-8 Exception types

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security risk exceptions</td>
<td>You can exclude the following security risks:</td>
</tr>
<tr>
<td></td>
<td>- Known security risks</td>
</tr>
<tr>
<td></td>
<td>- Files</td>
</tr>
<tr>
<td></td>
<td>- Folders</td>
</tr>
<tr>
<td></td>
<td>- Extensions</td>
</tr>
<tr>
<td></td>
<td>Your administrator may have configured the client so that you cannot exclude any of these items from being scanned.</td>
</tr>
<tr>
<td></td>
<td>See “Excluding items from being scanned” on page 81.</td>
</tr>
<tr>
<td>TruScan proactive threat scan exceptions</td>
<td>You can exclude processes from the TruScan proactive threat scans. You can specify a different action to take for a known process that the TruScan proactive threat scans detect. You can force the detection of a process.</td>
</tr>
<tr>
<td></td>
<td>Your administrator may have configured the client so that you cannot exclude a process from being scanned.</td>
</tr>
<tr>
<td></td>
<td>See “Excluding a process from TruScan proactive threat scans” on page 100.</td>
</tr>
<tr>
<td>Tamper Protection exceptions</td>
<td>You can exclude files from Tamper Protection.</td>
</tr>
<tr>
<td></td>
<td>Tamper Protection prevents non-Symantec processes from affecting Symantec processes.</td>
</tr>
<tr>
<td></td>
<td>See “About Tamper Protection” on page 40.</td>
</tr>
<tr>
<td></td>
<td>See “Excluding items from being scanned” on page 81.</td>
</tr>
</tbody>
</table>

Excluding items from being scanned

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

See “About excluding items from being scanned” on page 80.

Exceptions apply across all scans. If you configure an exception when you create or edit a particular scan, the exception applies to all scans.
Note: On the Server Core installation of Windows Server 2008, the appearance of the dialog boxes might differ from the ones that are described in these procedures.

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

To exclude a security risk from being scanned

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

To exclude a file or folder from being scanned

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

About handling quarantined files

Sometimes the client detects an unknown virus that cannot be eliminated with the current set of virus definitions. You might have a file that you believe is infected but scans do not detect an infection. The Quarantine safely isolates potentially infected files on your computer. When you quarantine a virus, the virus cannot spread on your computer or to other computers in your network.
About infected files in the Quarantine

You can view the infected files in the Quarantine.

You can view the following information about the files:

- Risk
- Filename
- Type
- Original Location
- Status
- Date

**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.

When the client moves an infected file to the Quarantine, the risk cannot copy itself and infect other files. This action is a recommended second action for both macro and non-macro virus infections.

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. Viruses and macro viruses can be quarantined. Boot viruses cannot be quarantined. Usually, boot viruses reside in the boot sector or partition tables of a computer; these items cannot be moved to the Quarantine.

You can also view properties of the infected file.

See “**Viewing files and file details in the Quarantine**” on page 85.

About handling infected files in the Quarantine

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

- Restore the selected file to its original location.
- Permanently delete the selected file.
- Rescan the files after you receive updated virus definitions.
- Export the contents of the Quarantine to either a comma-delimited (*.csv) file or an Access database (*.mdb) file.
Manually add a file to Quarantine. You can browse to the location of and select the file that you want to move to the Quarantine.

Submit a file to Symantec Security Response. Follow the instructions in the on-screen wizard to submit the selected file for analysis.

See “Managing the quarantine” on page 84.

About handling files infected by security risks

You can leave the files that are quarantined because of security risks in the Quarantine or you can delete them. You should leave them in the Quarantine until you are sure that the applications on your computer have not lost any functionality.

If you delete the files that are associated with a security risk, an application on your computer might not function properly. The application might depend on the associated files that you deleted. Quarantine is a safer option because it is reversible. You can restore the files if any of the applications on your computer lose functionality after you quarantine the dependent program files.

**Note:** After you run the application successfully, you might want to delete the files to save disk space.

Managing the quarantine

Files are placed in the Quarantine in one of the following ways:

The client is configured to move the infected items that are detected during Auto-Protect or a scan to the Quarantine.

You manually select a file and add it to the Quarantine.

The default options for Auto-Protect and all scan types are to clean a virus from an infected file on detection. The scan software places the file in the Quarantine if the file cannot be cleaned. For security risks, the default option is to place the infected files in the Quarantine, and to repair the side effects of the security risk.

See “Rescanning files in the Quarantine for viruses” on page 85.

See “Clearing backup items” on page 86.

See “Deleting files from the Quarantine” on page 86.

See “Submitting a potentially infected file to Symantec Security Response for analysis” on page 88.
To add a file manually to the Quarantine

1. In the client, in the sidebar, click **View quarantine**.
2. Click **Add**.
3. Select the file that you want to add to the Quarantine, and then click **Add**.

Viewing files and file details in the Quarantine

You can view the files that have been placed in the Quarantine. You can view details about the files. The details include the name of the virus and the name of the computer on which the file was found.

To view files and file details in the Quarantine

1. In the client, in the sidebar, click **View quarantine**.
2. Right-click the file that you want to view, and then click **Properties**.

Rescanning files in the Quarantine for viruses

If a file is placed in the Quarantine, update your definitions. When you update definitions, files in the Quarantine might get scanned, cleaned, and restored automatically. You can rescan the files in the Quarantine if the Repair Wizard appears.

See “Rescanning files manually” on page 85.

If the client cannot remove the virus after rescanning files in the Quarantine, you can submit the infected file to Symantec Security Response for analysis.

See “Submitting a potentially infected file to Symantec Security Response for analysis” on page 88.

To rescan files in the Quarantine using the Repair Wizard

1. When the Repair Wizard appears, click **Yes**.
2. Click **Next**.
3. Follow the on-screen instructions to rescan the files in the Quarantine.

Rescanning files manually

You can manually rescan a file in the Quarantine for viruses, but not for security risks.

See “Rescanning files in the Quarantine for viruses” on page 85.
To rescan a file in the Quarantine manually for viruses

1 Update your definitions.
2 In the client, in the sidebar, click View quarantine.
3 Select the file and then click Rescan All.

When a repaired file cannot be returned to its original location

Occasionally, a clean file does not have a location to which to be returned. For example, an infected attachment may have been stripped from an email and placed in the Quarantine. You must release the file and specify a location.

To release a cleaned file from the Quarantine

1 In the client, in the sidebar, click View quarantine.
2 Right-click the repaired file, and then click Restore.
3 Specify the location for the cleaned file.

Clearing 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. You can also set up a time period in which files are deleted automatically.

See “Automatically deleting files from the Quarantine” on page 87.

To manually clear backup items

1 In the client, in the sidebar, click View quarantine.
2 Select one or more backup files.
3 Click Delete.

Deleting files from the Quarantine

You can manually delete the files that you no longer need from the Quarantine. You can also set up a time period by which files are deleted automatically.

**Note:** Your administrator may specify a maximum number of days that items are allowed to stay in the Quarantine. Items are automatically deleted from the Quarantine after that time limit.

See “Automatically deleting files from the Quarantine” on page 87.
To manually delete files from the Quarantine

1. In the client, in the sidebar, click **View quarantine**.
2. Select one or more files.
3. Click **Delete**.

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 “Deleting files from the Quarantine” on page 86.

To automatically delete files

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**.
Submitting a potentially infected file to Symantec Security Response for analysis

Sometimes, the client cannot clean a virus from a file. Or, you suspect that a file is infected and the client does not detect the infection. If you submit the file to Symantec Security Response, they can analyze your file to make sure that it is not infected. You must have an Internet connection to submit a sample.

**Note:** The Submit to Symantec Security Response option is not available if your administrator disables these types of submissions.

See “Automatically deleting files from the Quarantine” on page 87.

See “Submitting information about scan detections to Symantec Security Response” on page 88.

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.

Submitting information about scan detections to Symantec Security Response

You can specify that information about Auto-Protect or scan detection rates is automatically sent to Symantec Security Response. Information about detection rates potentially helps Symantec refine virus definitions updates. Detection rates show the viruses and security risks that are detected most by customers. Symantec Security Response can remove the signatures that are not detected, and provide a segmented signature list for the customers who request it. Segmented lists increase scan performance.

The submission of detection rates is enabled by default.

**Note:** Your administrator might lock the submission settings.

You can also submit items in the Quarantine to Symantec.
See “Submitting a potentially infected file to Symantec Security Response for analysis” on page 88.

To submit information about scan detections to Symantec Security Response

1 In the client, in the sidebar, click **Change settings**.
2 Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3 On the Submissions tab, check **Automatically submit antivirus and security risk detections**.
4 Click **OK**.

### 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 4-9** shows the protection status reporting in WSC.

<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 File System Auto-Protect is not enabled</td>
<td>OFF (red)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed, File System Auto-Protect is not enabled, and virus and security risk definitions are out of date</td>
<td>OFF (red)</td>
</tr>
<tr>
<td>Symantec Endpoint Protection is installed and Rtvscan is turned off manually</td>
<td>OFF (red)</td>
</tr>
</tbody>
</table>

**Table 4-10** shows the Symantec Endpoint Protection firewall status reporting in WSC.
## Table 4-10  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 Proactive Threat Protection

This chapter includes the following topics:

- About TruScan proactive threat scans
- Configuring how often to run TruScan proactive threat scans
- Managing TruScan proactive threat detections
- Configuring notifications for TruScan proactive threat scan detections
- Submitting information about TruScan proactive threat scans to Symantec Security Response
- Excluding a process from TruScan proactive threat scans

About TruScan proactive threat scans

TruScan proactive threat scans gives you zero-day attack protection. Zero-day attack protection means protection against unknown threats or vulnerabilities. Proactive threat scans examine your computer for the active processes that exhibit the behavior that might be malicious. Since unknown threats do not have signatures to identify them, proactive threat scans identify potential risks by flagging suspicious behavior.

The default proactive threat scan settings are appropriate for many users. You can change the settings to address the level of heuristic protection that your computer requires.

You should ask the following questions before you make changes to the proactive threat scan settings:

- Do you want to be informed when a threat occurs on your computer?
How often and when do you want to scan processes?

How much computer resources do you want to provide for proactive threat scans?

**Note:** If your administrator does not lock proactive threat scan settings, you can configure the settings. Locked settings include a locked padlock icon. The labels on locked settings appear grayed-out.

See “Managing TruScan proactive threat detections” on page 95.

### Processes and applications that TruScan proactive threat scans examine

Proactive threat scans examine certain types of processes or applications that exhibit suspicious behavior. The scans detect the processes that appear to act like Trojan horses or worms, or keyloggers. You can enable or disable the detection.

In addition to Trojan horses, worms, and keyloggers, proactive threat scans detect the processes that behave similarly to adware and spyware. You cannot configure how proactive threat scans handle these types of detections. If proactive threat scans detect the adware or the spyware that you want to allow on your client computers, you or your administrator should create a centralized exception.

See “Excluding a process from TruScan proactive threat scans” on page 100.

Proactive threat scans also detect the well-known commercial applications that can be used for malicious purposes. Symantec maintains a list of these commercial applications, and periodically updates the list. These applications include the commercial applications that monitor or record a user’s keystrokes or that control a user’s computer remotely. You can set actions for how Symantec Endpoint Protection handles these detections.

**Table 5-1** describes the processes that proactive threat scans detect.

<table>
<thead>
<tr>
<th>Type of processes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trojan horses and worms</td>
<td>Processes that exhibit characteristics of Trojan horses or worms. Proactive threat scans use heuristics to look for the processes that behave like Trojan horses or worms. These processes may or may not be threats.</td>
</tr>
</tbody>
</table>
### Table 5-1 Processes detected by TruScan proactive threat scans (continued)

<table>
<thead>
<tr>
<th>Type of processes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Keyloggers</td>
<td>Processes that exhibit characteristics of keyloggers. Proactive threat scans detect commercial keyloggers, but they also detect the unknown processes that exhibit keylogger behavior.</td>
</tr>
<tr>
<td>Commercial applications</td>
<td>Known commercial applications that might be used for malicious purposes. Proactive threat scans detect several different types of commercial applications. You can configure actions for two types: keyloggers and remote control programs.</td>
</tr>
<tr>
<td>Adware and spyware</td>
<td>Processes that exhibit the characteristics of adware and spyware. Proactive threat scans uses heuristics to detect the unknown processes that behave like adware and spyware. These processes may or may not be risks.</td>
</tr>
</tbody>
</table>

### About exceptions for TruScan proactive threat scans

You can create some exceptions for proactive threat scans unless your administrator locked the centralized exceptions settings.

Your administrator might also create centralized exceptions for proactive threat scans. You cannot modify the exceptions that your administrator creates.

See “Excluding a process from TruScan proactive threat scans” on page 100.

### About TruScan proactive threat scan detections

Proactive threat scans log, quarantine, or terminate the potentially malicious processes that they detect. You can view detections by using the scan results dialog box, the Proactive Threat Protection logs, or the Quarantine list.

See “About interacting with scan results or Auto-Protect results” on page 71.

See “Managing the quarantine” on page 84.

**Note:** Proactive threat scan settings have no effect on antivirus and antispyware scans, which use signatures to detect known risks. Symantec Endpoint Protection detects known risks first.

By default, the client does the following actions:
Logs the detection of well-known commercial applications

Logs the detection of processes that behave like Trojan horses, worms, or keyloggers

Quarantines processes that behave like Trojan horses, worms, or keyloggers and that require remediation

When a proactive threat scan quarantines a detection, it handles any side effects of the process. If the client rescans the detection after content updates are downloaded to your computer, the client might restore the process to your computer. The client restores the process if the process is no longer considered malicious. The client also restores any side effects of the process. However, the client does not automatically restart the process.

For detection of commercial keylogger or remote control applications, you or your administrator can specify a different action. For example, you might want to ignore the detection of commercial keylogger applications. When the client ignores an application, it allows the application and does not log its detection.

For Trojan horse, worm, or keylogger detections, you can specify a particular action that the client always uses when it makes a detection.

About acting on false positives

TruScan proactive threat scans sometimes detect false positives. These scans look for applications and processes with suspicious behavior rather than known viruses or security risks. By their nature, these scans typically flag the items that you might not want to detect.

If a proactive threat scan detects a process that you determine is not a problem, you can create an exception so that future scans do not flag the process. If there is a conflict between a user-defined exception and an administrator-defined exception, the administrator-defined exception takes precedence.

See “Excluding a process from TruScan proactive threat scans” on page 100.

To minimize false positive detections, make sure that the Symantec content for proactive threat scans is current. The version appears on the Status page under Proactive Threat Protection. You can download the latest content by running LiveUpdate.

Note: Your administrator might schedule automatic updates.

If you choose to manage the detection of Trojan horses, worms, and keyloggers yourself, you can change the sensitivity of proactive threat scans. However,
changing the sensitivity might not change the number of false positives, because it only changes the number of total detections.

See “Managing TruScan proactive threat detections” on page 95.

Configuring how often to run TruScan proactive threat scans

You can configure how often to run proactive threat scans.

**Note:** If you increase how often proactive threat scans run, you might impact the performance of your computer.

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

**To configure how often to run TruScan proactive threat scans**

1. In the client, in the sidebar, click Change settings.
2. Next to Proactive Threat Protection, click Configure Settings.
3. In the Proactive Threat Protection Settings dialog box, on the Scan Frequency tab, check At a custom scanning frequency.
4. Do one or more of the following actions:
   - Next to Scan every, set the length of time in number of days, hours, and minutes between scanning processes.
   - Check Scan new processes immediately to scan new processes when they are detected.
5. Click OK.

Managing TruScan proactive threat detections

Administrators might lock the proactive threat detection settings. If your settings are unlocked, or if you are running an unmanaged client, you can configure the types of processes that proactive threat detections detect.

See “Specifying the types of processes that TruScan proactive threat scans detect” on page 98.
Note: The detection of Trojan horses, worms, and keyloggers is currently not supported on Windows server operating systems or 64-bit Windows XP Professional. The detection of keyloggers is also not supported on Windows 7. On the clients that run on server operating systems, the scan options are unavailable. If your administrator modifies these options in a policy that is applied to your computer, the options might appear checked and unavailable.

When the detection of Trojan horses, worms, or keyloggers is enabled, you can choose how you want to manage the detections. By default, proactive threat scans use Symantec defaults. This means that the client determines the action for the detection. (The defaults that are unavailable on the user interface do not reflect the Symantec defaults. The unavailable settings reflect the default settings that you use when you manually manage detections.)

See “Specifying actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers” on page 97.

Typically, the Symantec default settings provide the best way to handle detections. However, if you have experience with scan results on your computer, you might want to configure the actions and sensitivity levels manually. To configure these parameters, you disable the Symantec defaults option.

To minimize false-positive detections, Symantec recommends that you use the Symantec-managed defaults initially. After a certain length of time, you can observe the number of false positives that the clients detect. If the number is low, you might want to tune the proactive threat scan settings gradually. For example, for the detection of Trojan horses and worms, you might want to move the sensitivity slider slightly higher than its default. You can observe the results of the proactive threat scans that run after you set the new configuration.

Note: For managed clients, typically your administrator configures the proactive threat scan settings that are appropriate for your computer.

For commercial applications, you can specify the type of action to take when a proactive threat scan detects commercial keylogger or commercial remote control programs. You can change these settings regardless of the configuration for Trojan horses, worms, or keyloggers.

See “Setting the action for the detection of commercial applications” on page 96.

Setting the action for the detection of commercial applications

You can change the action that the client takes when a proactive threat scan detects certain types of commercial applications.
You can click Help for more information about the options that are used in the procedure.

**To set the action for commercial application detections**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Proactive Threat Protection, click **Configure Settings**.
3. In the Proactive Threat Protection Settings dialog box, on the Scan Details tab, under Commercial Applications, do any of the following actions:
   - Set the action for commercial keyloggers to Ignore, Log, Terminate, or Quarantine.
   - Set the action for commercial remote control applications to Ignore, Log, Terminate, or Quarantine.
4. Click **OK**.

**Specifying actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers**

If you choose to manage Trojan horse, worm, or keylogger detections yourself, you can configure the action to take when these processes are detected. That action is always used when proactive threat scans make a detection. For example, you might set the action to log only. If a proactive threat scan detects a process that it categorizes as a true positive, the client logs the detection. The client does not quarantine the process.

You can also set different sensitivity levels for the detection of Trojan horses and worms and the detections of keyloggers. The sensitivity level determines how sensitive proactive threat scans should be when they scan processes. A higher sensitivity results in more detections. Keep in mind that some of these detections might be false positives. Setting the sensitivity level lower or higher might not change the percentage of false positives that proactive threat scans produce. It only changes the number of total detections.

You might want to keep the sensitivity level lower until you see the results of proactive threat scans on your computer. If proactive threat scans do not produce any detections at a lower sensitivity level, you can increase the sensitivity.

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

**To set the action and the sensitivity level for Trojan horses and worms**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Proactive Threat Protection, click **Configure Settings**.
3 In the Proactive Threat Protection Settings dialog box, on the Scan Details tab, under Trojans and Worms, ensure that Scan for trojans and worms is checked, and then uncheck **Use defaults defined by Symantec**.

4 Under Sensitivity, move the slider to the left or right to decrease or increase the sensitivity respectively.

5 In the drop-down list, click **Log**, **Terminate**, or **Quarantine**.

6 Click **OK**.

**To set the action and sensitivity level for keyloggers**

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

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

3 In the Proactive Threat Protection Settings dialog box, on the Scan Details tab, under Keyloggers, ensure that Scan for keyloggers is checked, and then uncheck **Use defaults defined by Symantec**.

4 For the sensitivity level, click **Low** or **High**.

5 In the drop-down list, click **Log**, **Terminate**, or **Quarantine**.

6 Click **OK**.

**Specifying the types of processes that TruScan proactive threat scans detect**

You can configure whether or not proactive threat scans scan for Trojan horses and worms or keyloggers. Your administrator may lock some of these settings.

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

**To specify the types of processes that TruScan proactive threat scans detect**

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

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

3 In the Proactive Threat Protection Settings dialog box, on the Scan Details tab, under Trojans and Worms, check or uncheck **Scan for trojans and worms**.

4 Under Keyloggers, check or uncheck **Scan for keyloggers**.

5 Click **OK**.
Configuring notifications for TruScan proactive threat scan detections

You can configure messages to appear when proactive threat scans make detections. By default, the client displays the messages when the detections occur. You are also notified when a detection requires the client to terminate services or stop processes.

**Note:** Your administrator can lock these settings.

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

**To enable or disable notifications for TruScan proactive threat scan detections**

1. In the client, click Change settings.
2. Next to Proactive Threat Protection, click Configure Settings.
3. In the Proactive Threat Protection Settings dialog box, on the Notifications tab, check Display a message when there is a detection.
4. Check or uncheck Prompt before terminating a process and Prompt before stopping a service.
5. Click OK.

Submitting information about TruScan proactive threat scans to Symantec Security Response

By default, proactive threat scans submit information about detected processes to Symantec Security Response. When the scans submit information, Symantec analyzes the information to determine if a threat is real. If Symantec determines that the threat is real, Symantec can generate a signature to address the threat. Symantec includes the signature in the updated versions of the definitions.

When you submit information about a process, the submission includes the following information:

- The path to the executable
- The executable
- The information about the file and the registry load points that refer to the threat
- The internal state information
The content version that the proactive threat scan used

Any personal information that can identify your computer is not submitted.

The submission of proactive threat scan detections to Symantec Security Response is enabled by default.

**Note:** Your administrator can lock the submissions settings.

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

**To submitting information about TruScan proactive threat scans to Symantec Security Response**

1. In the client, in the sidebar, click **Change settings**.
2. Next to Antivirus and Antispyware Protection, click **Configure Settings**.
3. In the Antivirus and Antispyware Protection Settings dialog box, on the Submission tab, check or uncheck **Automatically submit TruScan proactive threat scan detections**.
4. Click **OK**.

**Excluding a process from TruScan proactive threat scans**

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

See “**About excluding items from being scanned**” on page 80.

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

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

Your administrator might also create centralized exceptions for your scans. If you create a centralized exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.
To exclude a process from TruScan proactive threat scans

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

This chapter includes the following topics:

- About managing Network Threat Protection
- Managing firewall protection
- How the firewall works
- About firewall rules
- Adding a firewall rule
- Changing the order of a firewall rule
- Enabling and disabling rules
- Exporting and importing rules
- About the built-in firewall rules
- Enabling traffic settings and stealth Web browsing settings
- Enabling Smart Traffic Filtering
- Enabling network file and printer sharing
- Blocking traffic
- Configuring application-specific settings
- Managing intrusion prevention protection
- How Intrusion Prevention protection works
About managing Network Threat Protection

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

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

<table>
<thead>
<tr>
<th>Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewall</td>
<td>The firewall protects unauthorized users from accessing your computer and the networks that connect to the Internet. The firewall detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic. The firewall allows or blocks inbound and outbound traffic. See “How the firewall works” on page 106. See “Managing firewall protection” on page 104.</td>
</tr>
<tr>
<td>Intrusion Prevention System</td>
<td>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 “Managing intrusion prevention protection” on page 122. See “How Intrusion Prevention protection works” on page 122.</td>
</tr>
</tbody>
</table>

Managing firewall protection

By default, the firewall allows all incoming and outgoing network traffic. You can configure the firewall to allow or block specific types of traffic.
On any client, you can disable Network Threat Protection temporarily for troubleshooting purposes. For example, you might not be able to open an application.

See “Enabling or disabling Network Threat Protection” on page 39.

Your administrator determines the level of interaction that you have with the client by permitting your ability to configure firewall rules, firewall settings, and intrusion prevention settings. You can interact with the client only when it notifies you of new network connections and possible problems, or you can have full access to the user interface.

Table 6-2 displays the firewall tasks you might want to perform to protect your computer.

Table 6-2  Managing firewall protection

<table>
<thead>
<tr>
<th>Action</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 the firewall works” on page 106.</td>
</tr>
<tr>
<td>Add firewall rules</td>
<td>Supplement the client’s default firewall rules with the firewall rules that you configure. For example, you might want to block an application that you do not want to run on your computer, such as an adware application. See “Adding a firewall rule” on page 112. You can enable or disable built-in firewall rules that allow certain types of traffic. See “Enabling traffic settings and stealth Web browsing settings” on page 115. See “Enabling Smart Traffic Filtering” on page 116.</td>
</tr>
<tr>
<td>Monitor firewall protection</td>
<td>You can regularly check the firewall protection status on your computer to see whether: ■ The firewall rules that you created work correctly. ■ The client blocked any network attacks. ■ The client blocked any applications that you expected to run. You can use the Traffic Log and the Packet Log to check the firewall protection status. See “Using the Network Threat Protection logs and the Client Management logs” on page 146.</td>
</tr>
</tbody>
</table>
How the firewall works

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

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

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

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

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

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

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

See “About firewall rules” on page 107.

**About firewall rules**

When a computer tries to connect to another computer, the firewall compares the type of connection with its list of firewall rules. The firewall automatically checks all the inbound and the outbound traffic packets against these rules. The firewall then allows or blocks the packets that are based on the information that is specified in rules.

See “About the elements of a firewall rule” on page 107.

See “Adding a firewall rule” on page 112.

**About the elements of a firewall rule**

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 AM and 5 PM daily.
Table 6-3 describes the criteria that you use to define a firewall rule.

### Table 6-3: Firewall rule conditions

<table>
<thead>
<tr>
<th>Condition</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Triggers</strong></td>
<td>Applications, hosts, protocols, and network adapters. 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.</td>
</tr>
<tr>
<td><strong>Conditions</strong></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><strong>Actions</strong></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>

Table 6-4 describes the triggers that you can define in a firewall rule.
Table 6-4  Firewall rule triggers

<table>
<thead>
<tr>
<th>Trigger</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>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.</td>
</tr>
<tr>
<td>Host</td>
<td>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.</td>
</tr>
<tr>
<td>Protocol</td>
<td>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. You can define the following types of protocols:</td>
</tr>
</tbody>
</table>
|               | ■ All IP protocols
|               |   Any protocol.                                                                                                                                     |
|               | ■ TCP                                                                                                                                            |
|               |   Port or port ranges.                                                                                                                               |
|               | ■ UDP                                                                                                                                            |
|               |   Port or port ranges.                                                                                                                               |
|               | ■ ICMP                                                                                                                                            |
|               |   Type and code.                                                                                                                                  |
|               | ■ Specific IP Protocol
|               |   Protocol number (IP type).
|               |   Examples: Type 1 = ICMP, Type 6 = TCP, Type 17 = UDP                                                                                           |
| Network adapter| 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. |

See “About stateful inspection” on page 110.

See “Adding a firewall rule” on page 112.
About stateful inspection

The firewall uses stateful inspection, a process that tracks information about current connections such as source and destination IP addresses, ports, applications, and so forth. The client makes traffic flow decisions by using this connection information before it inspects firewall rules.

For example, if a firewall rule permits a client 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 client is expected, and permits the Web server traffic to flow to the initiating client without inspecting the rulebase. A rule must permit the initial outbound traffic before the firewall logs the connection.

Stateful inspection lets you simplify rulebases because you do not have to create the rules that permit traffic in both directions for traffic that is typically initiated in one direction only. Client traffic that is typically initiated in one direction includes Telnet (port 23), HTTP (port 80), and HTTPS (port 443). Clients initiate this traffic outbound so you only have to create a rule that permits outbound traffic for these protocols. The firewall permits the return traffic.

By configuring only the outbound rules, you increase client security in the following ways:

- Reduce rulebase complexity.
- Eliminate the possibility that a worm or other malicious program can initiate connections to a client on the ports that are configured for outbound traffic only. You can also configure inbound rules only, for traffic to clients that the clients do not initiate.

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

See “About UDP connections” on page 110.

About UDP connections

For UDP communications, the client analyzes the first UDP datagram, and applies the action that is taken on the initial datagram to all subsequent UDP datagrams for the current program session. Inbound or outbound traffic between the same computers is considered part of the UDP connection.

For stateful UDP traffic, when a UDP connection is made, the inbound UDP communication is allowed, even if the firewall rule blocks it. For example, if a rule
blocks inbound UDP communications for a specific application, but you choose to allow an outbound UDP datagram, all inbound UDP communications are allowed for the current application session. For stateless UDP, you must create a firewall rule to allow the inbound UDP communication response.

A UDP session times out after 60 seconds if the application closes the port.

See “About stateful inspection” on page 110.

About the rule processing order

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

See “Adding a firewall rule” on page 112.

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

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

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

Table 6-5 shows the order in which the firewall processes the rules and the 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>Smart traffic filters</td>
</tr>
<tr>
<td>Fourth</td>
<td>Firewall rules</td>
</tr>
<tr>
<td>Fifth</td>
<td>Port scan checks</td>
</tr>
</tbody>
</table>
Table 6-5  Order that the firewall processes firewall rules and settings (continued)

<table>
<thead>
<tr>
<th>Priority</th>
<th>Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sixth</td>
<td>IPS signatures that are downloaded through LiveUpdate</td>
</tr>
</tbody>
</table>

See “Changing the order of a firewall rule” on page 113.

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.

See “About firewall rules” on page 107.

See “About the elements of a firewall rule” on page 107.

To add a firewall rule

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

   For more information about the options on each tab, click Help.
6. To define the time period when the rule is active or inactive, on the Scheduling tab, click Enable Scheduling, and then set up a schedule.
7. When you finish making changes, click OK.
8. In the Configure Firewall Rules dialog box, make sure the check mark appears in the Rule Name column to enable the rule.

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

   See “Changing the order of a firewall rule” on page 113.
9. Click OK.
Changing the order of a firewall rule

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

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

See “**About the rule processing order**” on page 111.

See “**Adding a firewall rule**” on page 112.

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**.

Enabling and disabling rules

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

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

See “**Adding a firewall rule**” on page 112.

To enable and disable 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 next to the rule that you want to enable or disable.

4 Click OK.

Exporting and importing 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.

See “Adding a firewall rule” on page 112.

To export 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 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.

About the built-in firewall rules

Network Threat Protection includes built-in rules that allow certain types of traffic. You can enable or disable these built-in rules, rather than adding the firewall rules yourself.
See “Adding a firewall rule” on page 112.

Your administrator may or may not have given you permission to customize these settings.

By default, the firewall allows most TCP/IP traffic, with the exception of IPv6. You can enable or disable the following built-in firewall rules:

### Smart traffic filters

Allows specific the types of traffic that are required on most networks. This type of traffic includes DHCP, DNS, and WINS traffic.


### Traffic and stealth settings

Enables the additional traffic features such as NetBIOS protection, token ring traffic, DNS reverse lookup, and stealth mode settings.

See “Enabling traffic settings and stealth Web browsing settings” on page 115.

You can disable the protection at certain times, such as during the installation of new software.

See “Enabling or disabling Network Threat Protection” on page 39.

You can also configure Microsoft Windows Networking settings.

See “Enabling network file and printer sharing” on page 116.

### 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 also 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**.
2. Beside Network Threat Protection, click **Configure Settings**.
3  In the Network Threat Protection Settings dialog box, click **Firewall**.

4  On the Firewall tab, in the Traffic Settings and Stealth Settings group boxes, check the check boxes to enable the settings.

5  Click **OK**.

### Enabling Smart Traffic Filtering

Smart Traffic filters allow the normal exchange of certain essential network services without defining the rules that explicitly allow those services. During processing, these filters 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. Requests for these services must originate from the client computer, and the server response must occur within a predefined 5-second period. This response is verified to ensure that it is valid for the original client request.

Smart Traffic rule filters allow the packet if a request was made. They do not block packets. The firewall rules allow or block packet

See “Enabling traffic settings and stealth Web browsing settings” on page 115.

**To enable Smart Traffic Filtering**

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

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

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

4  Check one or more of the following check boxes:

   - **Enable Smart DHCP**
   - **Enable Smart DNS**
   - **Enable Smart WINS**

5  Click **OK**.

### 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.

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. Your administrator may not have enabled this option on the client. Users on the client can enable these settings automatically.

See “About the built-in firewall rules” on page 114.

To automatically enable network file and print sharing
1 In the client, in the sidebar, click Change settings.
2 Beside Network Threat Protection, click Configure Settings.
3 In the Network Threat Protection Settings dialog box, click Microsoft Windows Networking.
4 On the Microsoft Windows Networking tab, to browse other computers and printers in the network, click Browse files and printers on the network.
5 To enable other computers to browse files on your computer, click Share my files and printers with others on the network.
6 Click OK.

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

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

**Blocking traffic**

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

- **When your computer’s screen saver is activated.**
  You can configure your computer to block all the inbound and the outbound Network Neighborhood traffic when your computer’s screen saver is activated. As soon as the screen saver turns off, your computer returns to the previously assigned security level.

- **When the firewall does not run.**
  The computer is not protected after the client computer turns on 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.

- **When you want to block all inbound and outbound traffic at any time.**
You may want to block all traffic when a particularly destructive virus attacks your company’s network or subnet. You would not block all traffic under normal circumstances.

**Note:** Your administrator may have configured this option to be unavailable. You cannot block traffic on a self-managed client.

You can allow all traffic by disabling Network Threat Protection.

See “Enabling or disabling Network Threat Protection” on page 39.

See “Blocking and unblocking an attacking computer” on page 125.

**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. In the Network Threat Protection Settings dialog box, click **Microsoft Windows Networking**.
4. On the Microsoft Windows Networking tab, click **Block Microsoft Windows Networking traffic while the screen saver runs**.
5. 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. In the Network Threat Protection Settings dialog box, click **Firewall**.
4. On the Firewall tab, click **Block all traffic until the firewall starts and after the firewall stops**.
5. Optionally click **Allow initial DHCP and NetBIOS traffic**.
6. 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**.
Configuring application-specific settings

You can configure the settings for an application that has either run since the client service started 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 AM and 8 AM overrides the schedule for a specific video application.

---

See “Adding a firewall rule” on page 112.

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**.

**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.

See “**Configuring application-specific settings**” on page 120.

**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 it, and then click **Remove**.
   - To remove all applications from the list, click **Remove All**.

4 Click **Yes**.

5 Click **OK**.
Managing intrusion prevention protection

You manage intrusion prevention protection on the Policies page.
You manage intrusion prevention protection as part of Network Threat Protection.
Table 6-6 displays the intrusion prevention tasks you might want to perform to protect your computer.

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Learn about Intrusion Prevention</td>
<td>Learn how Intrusion Prevention detects and blocks network attacks.</td>
</tr>
<tr>
<td></td>
<td>See “How Intrusion Prevention protection works” on page 122.</td>
</tr>
<tr>
<td>Ensure that Intrusion Prevention</td>
<td>Regularly check that Intrusion Prevention is enabled on your computers.</td>
</tr>
<tr>
<td>settings are enabled</td>
<td>See “Enabling or disabling intrusion prevention settings” on page 123.</td>
</tr>
<tr>
<td>Download the latest IPS signatures.</td>
<td>Download the latest IPS signatures. By default, LiveUpdate downloads the IPS signatures. However, you might want to download the IPS signatures immediately.</td>
</tr>
<tr>
<td></td>
<td>See “Updating the computer's protection” on page 30.</td>
</tr>
</tbody>
</table>

See “Blocking and unblocking an attacking computer” on page 125.

How Intrusion Prevention protection works

Intrusion Prevention protection automatically detects and blocks network attacks. Intrusion Prevention protection scans every packet that enters and exits a computer for attack signatures. An attack signature is a unique arrangement of information that identifies an attacker's attempt to exploit a known operating system or program vulnerability.

Intrusion Prevention protection uses Symantec's extensive list of attack signatures.
http://securityresponse.symantec.com/avcenter/attack_sigs/index.html

Intrusion Prevention protection optionally blocks all communication to and from an attacking computer for a specified period of time.
See “Managing intrusion prevention protection” on page 122.
See “Enabling or disabling intrusion prevention settings” on page 123.

**Figure 6-1**  Intrusion Prevention protection

---

**Enabling or disabling intrusion prevention settings**

The intrusion prevention settings are disabled by default. You might want to disable the IPS settings for troubleshooting purposes or if the client computer detects excessive false positives.

You can enable or disabling the following settings:

- Intrusion prevention system signatures that detect and prevent network attacks.
- Intrusion prevention settings that prevent port scans and denial-of-service attacks.
- Active response, which automatically blocks the computers that send attacks.

Typically, when you disable the intrusion prevention settings on your computer, your computer is less secure. However, you may need to disable these settings to prevent false positives or to troubleshoot the client computers.

The client logs the attacks and the security events that the intrusion prevention system detects in the Security Log. The client may log the attacks and the events in the Packet Log.
See “How Intrusion Prevention protection works” on page 122.

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

**To enable or disable intrusion prevention settings**

1. In the client, in the sidebar, click **Change settings**.
2. Beside **Network Threat Protection**, click **Configure Settings**.
3. In the **Network Threat Protection Settings** dialog box, click **Intrusion Prevention**.
4. To enable a setting, on the **Intrusion Prevention** tab, check any of the following check boxes:
   - Enable Intrusion Prevention
   - Enable denial of service detection
   - Enable port scan detection
   For more information on the settings, click **Help**.
5. 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.

**To configure intrusion prevention notifications**

1. In the client, in the sidebar, click **Change settings**.
2. Beside Network Threat Protection, click **Configure Settings**.
3. In the Network Threat Protection Settings dialog box, click **Intrusion Prevention**.
4. Check **Display Intrusion Prevention notifications**.
To hear a beep when the notification appears, check **Use sound when notifying users**.

Type an amount of time you want the notifications to appear in the **Number of seconds to display notifications** field.

Click **OK**.

## 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.

Updated IPS signatures, updated denial-of-service signatures, and port scans also trigger an active response.

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.

See “**Enabling or disabling intrusion prevention settings**” on page 123.

See “**Blocking traffic**” on page 118.

### To block an attacking computer

1. In the client, in the sidebar, click **Change settings**.
2. Beside Network Threat Protection, click **Configure Settings**.
3. In the Network Threat Protection Settings dialog box, click **Intrusion Prevention**.
4. 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, or 10 minutes.

5. Click **OK**.

   If you don’t want to wait the default amount of time to unblock the IP address, you can unblock it immediately.

### To unblock an attacking computer

1. In the client, in the sidebar, click **View logs**.
2. Beside Client Management, click **View Logs > Security Log**.
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.

In the message box that appears, click OK.

Click File > Exit.
Managing protection on the Symantec Network Access Control client

- Chapter 7. Managing Network Access Control
Managing Network Access Control

This chapter includes the following topics:

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

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.

Table 7-1 describes the process that Network Access Control uses to enforce policy compliance on the client computer.
### Table 7-1  
**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, hotfixes, 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 “How the client works with an Enforcer” on page 133.</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 “Responding to Network Access Control notifications” on page 25.</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 131.</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.

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 antivirus application 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 Now.
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.

About updating the Host Integrity Policy

The client updates the Host Integrity Policy at regular intervals. Your administrator may ask that you update the Host Integrity Policy before the next scheduled update for testing purposes. Otherwise, you do not need to update the policy.

See “Updating the policy file manually” on page 33.

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.

Viewing the Network Access Control logs

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

<table>
<thead>
<tr>
<th>Log</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>Records the results and status of Host Integrity checks.</td>
</tr>
<tr>
<td>System</td>
<td>Records all operational changes for the client, such as the connection to the management server and updates to the client security policy.</td>
</tr>
</tbody>
</table>

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 System Log, next to Network Access Control, click Options > View Logs.
4. Click File > Exit.

See “About logs” on page 141.
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.

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 the computer network access.

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 133.

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 reauthorizes 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 7-2 describes the types of options you can configure for 802.1x authentication.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| Third-party supplicant | Uses a third-party 802.1x supplicant. The LAN Enforcer works with a RADIUS server and third-party 802.1x supplicants to perform user authentication. The 802.1x supplicant prompts you for user information, which the LAN Enforcer passes to the RADIUS server for user-level authentication. The client sends the client profile and the Host Integrity status to the Enforcer so that the Enforcer authenticates the computer.  
**Note:** If you want to use the Symantec Network Access Control client with a third-party supplicant, then the Network Threat Protection module of the Symantec Endpoint Protection client must be installed. |
| Transparent mode  | Uses the client to run as an 802.1x supplicant. You use this method if the administrator does not want to use a RADIUS server to perform user authentication. The LAN Enforcer runs in transparent mode and acts as a pseudo-RADIUS server.  
Transparent mode means that the supplicant does not prompt you for user information. In transparent mode, the client acts as the 802.1x supplicant. The client responds to the switch’s EAP challenge with the client profile and the Host Integrity status. The switch, in turn, forwards the information to the LAN Enforcer, which acts as a pseudo-RADIUS server. The LAN Enforcer validates the Host Integrity and client profile information from the switch and can allow, block, or dynamically assign a VLAN, as appropriate.  
**Note:** To use a client as an 802.1x supplicant, you need to uninstall or disable third-party 802.1x supplicants from the client computer. |
Table 7-2  802.1x authentication options (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<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 112.

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**.

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**.

### Reauthenticate 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 does 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 need to log 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**.
Configuring the client for 802.1x authentication
Monitoring and logging

- Chapter 8. Using and managing logs
Using and managing logs

This chapter includes the following topics:

- About logs
- Managing log size
- Quarantining risks and threats from the Risk Log and the Threat Log
- Using the Network Threat Protection logs and the Client Management logs
- Exporting log data

About logs

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

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

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

For more information about a log, you can press F1 to view the help for that log. Table 8-1 describes the event types that each log displays.
### About logs

#### Table 8-1

<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.</td>
</tr>
<tr>
<td>Antivirus and Antispyware Protection System Log</td>
<td>Contains information about system activities on your computer that are related to viruses and security risks. This information includes configuration changes, errors, and definitions file information.</td>
</tr>
<tr>
<td>Threat Log</td>
<td>Contains information about the threats that TruScan proactive threat scans have detected on your computer. These include the commercial applications that can be used for malicious purposes. Examples are Trojan horses, worms, or keyloggers, or mass-mailing worms, and script-based threats.</td>
</tr>
<tr>
<td>Proactive Threat Protection System Log</td>
<td>Contains information about system activities on your computer that are related to TruScan proactive threat scans.</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 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.</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>
</tbody>
</table>
### Table 8-1  
**Client logs (continued)**

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

### Managing log size

You can configure how long to keep the entries in the logs. Deleting the older entries helps to keep the logs from using too much disk space. For the Network Threat Protection logs and the Client Management logs, you can also set the amount of space used.

### Configuring the retention time for the Antivirus and Antispyware Protection log entries

To configure the retention time for the Antivirus and Antispyware Protection log entries:

1. In the client, on the **Status** page, beside **Antivirus and Antispyware Protection**, click **Options**, and then click **Change Settings**.
2. On the **General** tab, set the number value and time unit for retaining the entries in these logs. The entries that are older than the value you set here are deleted.
3. Click **OK**.
Configuring the size of the Network Threat Protection logs and the Client Management logs

You can set the log size for each Network Threat Protection log and each Client Management log.

To change the size of the logs

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, on the **Logs** tab, in the **Maximum log file size** text field, type the maximum number of kilobytes you want the log file size to be.

You should keep the log file size small because of the space available on the computer. The default size for all logs is 512 KB, except for the Control Log and the Packet Log. The default size for the Control Log and the Packet Log is 1024 KB.

3. Click **OK**.

Configuring the retention time for the Network Threat Protection log entries and the Client Management log entries

You can specify how many days that entries are saved in each log. After the maximum number of days is reached, the oldest entries are replaced. You may want to delete entries to save space or to retain entries to review your computer's security.

To set the number of days to retain log entries

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, on the **Logs** tab, in the **Save each log entry for** text field, type the maximum number of days to save the log entries.

3. Click **OK**.

About deleting the contents of the Antivirus and Antispyware System Log

You cannot permanently remove event records from the System Log by using the user interface.
Deleting the contents of the Network Threat Protection logs and the Client Management logs

If your administrator allows it, you can clear the contents of the Network Threat Protection log and the Client Management logs. After you’ve cleared the log, each log immediately starts saving entries again.

**Note:** If the clear option is unavailable, you do not have permission to delete log contents.

If you have permission, you can also clear a log’s content from the File menu of the log itself.

**To delete the contents of a 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 Configure Network Threat Protection dialog box, on the **Logs** tab, beside the log that you want, click **Clear Log**.
3. When you are asked to confirm, click **Yes**.
4. Click **OK**.

**Quarantining risks and threats from the Risk Log and the Threat Log**

You can quarantine the threats that have been logged to the Proactive Threat Protection Threat History Log. You can quarantine risks from the Antivirus and Antispyware Risk Log. You can also clean and delete risks from the Antivirus and Antispyware Risk Log.
To quarantine a risk or threat

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

2. Beside either Antivirus and Antispyware Protection or Proactive Threat Protection, click **View Logs** and then click the name of the log you want.

3. Select a risk or threat and then click **Quarantine**.

   Based on the preset action for a risk detection, Symantec Endpoint Protection may or may not be able to perform the action you selected. If the threat or risk is successfully placed into quarantine, you get a success message. You don't need to take any further action to keep your computer safe from this risk or threat. You can leave the files that are quarantined because of risks in the Quarantine or you can delete them. You should leave them in the Quarantine until you are sure that the applications on your computer have not lost any functionality.

   See “**About infected files in the Quarantine**” on page 83.

   In the instances where Symantec Endpoint Protection is not able to put the risk or threat into the quarantine, you get an error message. In these instances, you may want to contact your administrator.

   You can also clean and delete risks and threats, as well as undo actions from these logs, where applicable.

   See “**Acting on infected files**” on page 20.

---

### Using the Network Threat Protection logs and the Client Management logs

The **Network Threat Protection** logs and the **Client Management** logs allow you to track your computer's activity and its interaction with other computers and networks. These logs record information about the traffic that tries to enter or exit your computer through your network connection. These logs also record information about the results of the firewall policy that is applied to the client.

You can manage the **Network Threat Protection** client logs and the **Client Management** client logs from a central location. The **Security**, **Traffic**, and **Packet** logs allow you to trace some data back to its source. It traces by using ICMP to determine all the hops between your computer and an intruder on another computer.

---

**Note:** Some options for these logs may be unavailable, based on the control type that your administrator has set for your client.
Refreshing the Network Threat Protection logs and the Client Management logs

To refresh a log

1. In the client, in the sidebar, click View logs.
2. To the right of Network Threat Protection or Client Management, click View Logs and then click the name of the log you want.
3. On the View menu, click Refresh.

Enabling the Packet Log

All Network Threat Protection logs and Client Management logs are enabled by default, except for the Packet Log. If you are allowed to by your administrator, you can enable and 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.

Stopping an active response

Any intrusion that is detected on the client triggers an active response. This active response automatically blocks the IP address of a known intruder for a specific amount of time. If your administrator allows, you can stop the active response immediately from the Security Log.

See “Blocking and unblocking an attacking computer” on page 125.

Tracing logged events back to their source

You can trace some events back to pinpoint the source of data from a logged event. Like a detective who retraces a criminal’s path at a crime scene, 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**.

**Using the Client Management logs with Symantec Network Access Control**

If you have Symantec Network Access Control installed, you can perform the following tasks from the Action menu in the Security Log and the System Log:

- Update a policy
  See “**Updating the policy file manually**” on page 33.
- Check Host Integrity
  See “**Running a Host Integrity check**” on page 131.

**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.

**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 Microsoft applications that are not available on Server Core.

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

- Antivirus and Antispyware System Log
- Antivirus and Antispyware Risk Log
- Antivirus and Antispyware 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
- Network Threat Protection Packet Log
- Client Management Security Log
- Client Management System 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 Antivirus and Antispyware 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 and then click 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.
Symbols

64-bit computers  34
802.1x authentication
  about  133
  configuring  135

A

actions
  assigning second actions for viruses  76
  tips for assigning second actions for security
    risks  76
active response
  about  125
active scans
  running  67
adapters
  defined  109
adware  51
allow traffic  120
  firewall rules  112
anti-MAC spoofing
  enabling  115
Antivirus and Antispyware Protection
  about  17,  54
  disabling  36,  38
  System Log  142
applications
  allowing or blocking  112,  120
  defined  109
  excluding from scans  81
Auto-Protect
  determining file types  61
  disabling security risk scanning  61
  enabling or disabling  36,  38
  encrypted email connections  59
  for Internet email  58
  for Lotus Notes  58
  for Microsoft Exchange clients  58
  groupware email clients  58
  network cache  63
  network scanning settings  62
Auto-Protect (continued)
  scanning by extension  55
  security risks  57
  trusting remote versions  63
  using  57
  viewing scan statistics  60
  viewing the risk list  60

B

Backup Items folder
  clearing  86
block an attacking computer  125
block traffic  118,  120
  firewall rules  112

C

centralized exceptions
  about  80
  creating  81
  for TruScan proactive threat scan
    detections  100
centrally managed clients
  vs. self-managed  28
clients
  about  15
  centrally managed vs. self-managed  28
  disabling protection on  35
  interacting with  19
computers
  updating protection on  30
Control Log  142
custom scans
  running  67

D

Debug Log  143
definitions
  about  65
  updating  30–32
definitions file  66
detection rates
  sending information to Symantec 88
disable
  Antivirus and Antispyware Protection 36
  Auto-Protect 36, 38
  Network Threat Protection 37, 39
  Proactive Threat Protection 36, 39
driver-level protection
  enabling 115

E
email
  encrypted connections 59
  excluding Inbox file from scans 54
  releasing attachments from Quarantine 86
email scanning. See Auto-Protect
enable
  Auto-Protect 38
  Network Threat Protection 39
  Proactive Threat Protection 39
enforcement
  about 133
exceptions
  about 80
  adding to scans 81
  Tamper Protection 81
  TruScan proactive threat scans 81, 100
extensions
  including in scans 55

F
File System Auto-Protect
  enabling or disabling 38
files
  backup of 86
  excluding from scans 81
  locating repaired 86
  releasing files from Quarantine 86
  rescanning files automatically in the
    Quarantine 85
  rescanning files manually in the Quarantine 86
  scanning 54
  sharing 116
  submitting to Symantec Security Response 88
firewall
  defined 104
  enabling or disabling 39
  managing 104
firewall rules
  about 107
  adding 112
  changing the order of 111, 113
  enabling and disabling 113
  exporting 114
  importing 114
  logging 108
  scheduling 108
full scans
  running 67

H
hacking tools 52
host
  defined 109
Host Integrity check
  running 131
icons
  padlock 29
  shield 44
infected file
  acting on 20
Intrusion Prevention
  about 122
intrusion prevention. See IPS
  enabling or disabling 124
  notifications for 124
  respond to 25
IPS
  about 104
  updating definitions 30

L
LiveUpdate
  creating a schedule for 32
  overview 30
  running immediately 31
locations
  about 42
  changing 43
locked and unlocked settings 29
logs
  about 141
  back tracing entries 147
Client Management 146
logs (continued)
configuring how long entries are kept 143–144
configuring the size of 144
deleting 145
enabling the Packet Log 147
export formats 149
exporting data 149
exporting filtered log entries 149
limiting the size of 143
network access control 132
Network Threat Protection 146
quarantining risks and threats from 145
refreshing 147

M
macro virus infections
preventing 56
managed clients. See centrally managed clients
manual scans. See on-demand scans
messages
intrusion prevention 124
responding to 22

N
NetBIOS protection
enabling 115
Network Access Control
notifications 25
network access control
about 18, 129
enforcement 133
remediating the computer 131
network cache
Auto-Protect settings 63
network scanning
Auto-Protect settings 62
Network Threat Protection
about 18, 104
enabling or disabling 37, 39
logs 142
managing 104
notification area icon
about 44
hiding and displaying 45
notifications
about 19
intrusion prevention 124
network access control 25
notifications (continued)
responding to 22
user interaction with 71

O
on-demand scans
creating 69
running 34
scanning by extension 55
options
unavailable 28

P
Packet Log 142
enabling 147
padlock icons 29
policies
about 32
updating 33
print sharing 116
Proactive Threat Protection
about 17
enabling or disabling 36, 39
proactive threat scan. See TruScan proactive threat scans
protection
enabling or disabling 35
types 15
updating 30–32
protocol
defined 109

Q
Quarantine 82
deleting files 84, 87
deleting files manually 87
handling files infected by security risks 84
handling infected files 83
managing 84
moving files to 83
releasing files 86
removing backup files 86
rescanning files automatically 85
rescanning files manually 86
submitting files to Symantec Security Response 88
viewing file details 85
viewing infected files 83
R
reauthentication 136
risk impact ratings 77
Risk Log 142
risks. See security risks

S
scan exceptions. See centralized exceptions
Scan Log 142
scans. See antivirus and antispyware
   all file types 56
   components that they scan 64
   compressed files 66
   delaying 34
   excluding files and folders from 81
   excluding from TruScan proactive threat scans 100
files 54
how they work 64
interpreting results 71
on-demand and startup 69
pausing 34
running 34
scanning files by extension 55
scheduled 66
snooze options 35
scheduled scans
   creating 66
   editing and deleting 70
   multiple 67
   scanning by extension 55
Security Log 143
security risk scanning
   disabling in Auto-Protect 61
security risks
   about 51
   configuring actions for 73
   configuring notifications for 78
   excluding from scans 81
   how the client detects 65
   how the client responds 53
   options 78
   process continues to download 57
   remediation options 78
   tips for assigning second actions 76
   what to do when detected 56
self-managed clients
   about 28
   vs. centrally managed 28
server
   connecting to 44
   managed clients 28
settings
   intrusion prevention 124
   share files and printers 116
   shield icon 44
   Smart DHCP 116
   Smart DNS 116
   Smart Traffic Filters
      defined 114
      enabling 116
   Smart WINS 116
spyware
   about 52
standalone clients. See self-managed clients
startup scans
   creating 69
   editing and deleting 70
   scanning by extension 55
stateful inspection
   about 110
   creating rules for traffic 110
stealth mode Web browsing
   enabling 115
Symantec Security Response
   submitting files to 88
System Log
   Antivirus and Antispyware Protection 142
   Client Management 143
   deleting entries 144
   Proactive Threat Protection 142
system tray icon 44

T
Tamper Protection
   about 40
   configuring 41
   enabling and disabling 41
Tamper Protection Log 143
testing your computer 42
Threat Log 142
token ring traffic
   enabling 115
traffic
   allowing or blocking 120
   blocking 118
Traffic and stealth settings 115
defined 114
Traffic Log 105, 142
Trojan horses
   about 51
TruScan proactive threat scans
   about 91–92
   actions 97
   commercial applications 96
   detections 93
   exceptions for 100
   false positives 94
   frequency 95
   logs 142
   managing 95
   notifications for 99
   sensitivity level 97
   submitting information about 99
   types of processes to detect 98

U
UDP connections
   about 110
   unblock an attacking computer 125
unmanaged clients. See self-managed clients
update
   definitions 30–32
user-defined scans
   editing and deleting 70

V
virus definitions
   about 65
   updating 30–32
viruses
   about 50
   assigning second actions 76
   configuring actions for 73
   configuring notifications for 78
   detection options 78
   file damage from 21
   how the client detects 65
   how the client responds 53
   remediation options 78
   unrecognized 88
   what to do when detected 56

W
Windows Security Center
   (continued)
      seeing firewall status from 90
      worms 51
Z
zero-day protection 91