

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



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 11.00.00.00.02

Legal Notice

Copyright © 2007 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, LiveUpdate, Sygate, Symantec AntiVirus, Bloodhound, Confidence Online, Digital Immune System, and Norton 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.

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.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014

<http://www.symantec.com>

Contents

Section 1 Introduction

Chapter 1 Introducing your Symantec client

About the client	11
About managed clients and unmanaged clients	12
About the notification area icon	12
What keeps your computer's protection current	14
About the role of Symantec Security Response	15
How protection is updated on managed clients	15
How protection is updated on unmanaged clients	15
About security policies	16
Updating the security policy	16
Where to get more information	16
Accessing online Help	17
Accessing the Symantec Security Response Web site	17

Chapter 2 Responding to the client

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	24
Responding to Network Access Control notifications	25

Chapter 3 Managing the client

About LiveUpdate	27
Running LiveUpdate at scheduled intervals	28
Running LiveUpdate manually	28
Testing the security of your computer	29
About locations	29
Changing locations	30
About Tamper Protection	30
Enabling, disabling, and configuring Tamper Protection	31

Section 2 Symantec Endpoint Protection

Chapter 4 Introducing Symantec Endpoint Protection

About Symantec Endpoint Protection	35
How Symantec Endpoint Protection protects your computer	36
About Antivirus and Antispyware Protection	36
About Network Threat Protection	37
About Proactive Threat Protection	37

Chapter 5 Symantec Endpoint Protection client basics

About viruses and security risks	39
How the client responds to viruses and security risks	42
Enabling and disabling protection components	43
Enabling and disabling Antivirus and Antispyware Protection	43
Enabling and disabling Network Threat Protection	45
Enabling or disabling Proactive Threat Protection	46
Using the client with Windows Security Center	47
Pausing and delaying scans	48

Chapter 6 Managing Antivirus and Antispyware Protection

About Antivirus and Antispyware Protection	51
About scanning files	52
When the Symantec Endpoint Protection client detects a virus or security risk	55
About Auto-Protect	55
About Auto-Protect and security risks	56
About Auto-Protect and email scanning	56
Disabling Auto-Protect handling of encrypted email connections	58
Viewing Auto-Protect scan statistics	58
Viewing the risk list	59
Configuring Auto-Protect to determine file types	59
Disabling and enabling Auto-Protect security risk scanning and blocking	60
Configuring network scanning options	60
Working with antivirus and antispyware scans	62
How the Symantec Endpoint Protection client detects viruses and security risks	63
About definitions files	64
About scanning compressed files	65

Initiating on-demand scans	65
Configuring antivirus and antispymware scanning	65
Creating scheduled scans	66
Creating on-demand and startup scans	69
Editing and deleting startup, user-defined, and scheduled scans	71
Interpreting scan results	72
About interacting with scan results or Auto-Protect results	73
Submitting information about antivirus and antispymware scans to Symantec Security Response	74
Configuring actions for viruses and security risks	75
Tips for assigning second actions for viruses	78
Tips for assigning second actions for security risks	78
About risk impact ratings	79
Configuring notifications for viruses and security risks	80
Configuring centralized exceptions for antivirus and antispymware scans	82
About the Quarantine	84
About infected files in the Quarantine	84
About handling infected files in the Quarantine	85
About handling files infected by security risks	86
Managing the Quarantine	86
Viewing files and file details in the Quarantine	86
Rescanning files in the Quarantine for viruses	87
When a repaired file can't be returned to its original location	87
Clearing backup items	88
Deleting files from the Quarantine	88
Automatically deleting files from the Quarantine	88
Submitting a potentially infected file to Symantec Security Response for analysis	89

Chapter 7

Managing Proactive Threat Protection

About Proactive Threat Protection	91
About proactive threat scans	92
About exceptions for proactive threat scans	93
About proactive threat scan detections	93
About acting on false positives	94
Configuring how often to run proactive threat scans	95
Managing proactive threat detections	95
Specifying the types of processes that proactive threat scans detect	96

Specifying actions and sensitivity levels for detecting Trojan horses, worms, and keyloggers	97
Setting the action for the detection of commercial applications	98
Configuring notifications for proactive threat scan detections	98
Submitting information about proactive threat scans to Symantec Security Response	99
Configuring a centralized exception for proactive threat scans	100

Chapter 8 Managing Network Threat Protection

About Network Threat Protection	101
How the client protects against network attacks	102
Viewing network activity	105
Configuring the firewall	107
About firewall rules	108
Adding rules	112
Changing the order of rules	113
Enabling and disabling rules	114
Exporting and importing rules	114
Editing and deleting rules	115
Enabling traffic settings and stealth Web browsing settings	115
Enabling Smart traffic filtering	117
Blocking traffic	118
Configuring intrusion prevention	119
Configuring intrusion prevention notifications	120
Blocking an attacking computer	121
Configuring application-specific settings	122
Removing the restrictions from an application	124
Enabling and disabling file and print sharing	124

Section 3 Symantec Network Access Control

Chapter 9 Symantec Network Access Control basics

About Symantec Network Access Control	127
How Symantec Network Access Control works	128
About updating the Host Integrity Policy	129
Running a Host Integrity check	129
Remediating your computer	129
Viewing the Symantec Network Access logs	130
About enforcement	131
Configuring the client for 802.1x authentication	131

Reauthenticating your computer	134
--------------------------------------	-----

Section 4 Monitoring and logging

Chapter 10 Using and managing logs

About logs	137
Viewing the logs and the log details	142
Filtering the log views	143
Managing log size	146
Configuring the retention time for the Antivirus and Antispyware Protection log entries and the Proactive Threat Protection log entries	146
Configuring the size of the Network Threat Protection logs and the Client Management logs	146
Configuring the retention time for the Network Threat Protection log entries and the Client Management log entries	147
About deleting the contents of the Antivirus and Antispyware System Log	147
Deleting the contents of the Network Threat Protection logs and the Client Management logs	147
Quarantining risks and threats from the Risk Log and the Threat Log	148
Using the Network Threat Protection logs and the Client Management logs	149
Refreshing the Network Threat Protection logs and the Client Management logs	150
Enabling the Packet Log	150
Stopping an active response	150
Tracing logged events back to their source	150
Using the Client Management logs with Symantec Network Access Control	152
Exporting log data	152

Index

Introduction

- [Introducing your Symantec client](#)
- [Responding to the client](#)
- [Managing the client](#)

Introducing your Symantec client

This chapter includes the following topics:

- [About the client](#)
- [What keeps your computer's protection current](#)
- [About security policies](#)
- [Where to get more information](#)

About the client

Symantec produces two endpoint security products that can be used together or separately: Symantec Endpoint Protection and Symantec Network Access Control. 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.

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.

Symantec Endpoint Protection protects your computer from Internet threats and security risks. It can perform the following actions:

- Scan your computer for viruses, known threats, and security risks.
- Monitor ports for known attack signatures.
- Monitor programs on your computer for suspicious behavior.

See [“About Symantec Endpoint Protection”](#) on page 35.

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.

See [“About Symantec Network Access Control”](#) on page 127.

About managed clients and unmanaged clients

The administrator of your Symantec product can install the client as either an unmanaged client or an administrator-managed client. An unmanaged client means that an administrator does not control the settings and actions in the Symantec client. In an unmanaged client, you control all the settings and actions in the client.

In a managed environment, your administrator uses the Symantec Endpoint Protection Manager to monitor, configure, and update your client remotely. This management server lets your administrator determine the amount of control that you have over the settings and actions in the client. Your client checks in with the management server to determine if new policy information or updates are available.

In a managed environment, you might not be able to view or access every client component. The visible components and the available actions in the client depend on the level of access that your administrator has granted your computer. 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 protection.

In all environments, the client prompts you with information and questions. You must respond to these prompts.

See [“About client interaction”](#) on page 19.

About the notification area icon

The client has a notification area icon that is located in the lower-right hand corner of your desktop. Right-click this icon to show frequently used commands.

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

[Table 1-1](#) describes the commands that are available from the notification area icon.

Table 1-1 Notification area icon commands

Option	Description
Open Symantec Endpoint Protection Open Symantec Network Access Control	Opens the main window
Update Policy	Retrieves the latest security policies from the server Note: This command is available on managed clients only.
Re-authentication	Reauthenticates the client computer. Note: This command is available only when your administrator configures the client as a built-in 802.1x supplicant.
Disable Auto-Protect	Turns off all client protection. After you disable the client, the command text changes from "Disable" to "Enable." You can select this command to turn on all client protection.

See [“Reauthenticating your computer”](#) on page 134.

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 task bar.

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

To hide the notification area icon

- 1 In the main window, in the sidebar, click **Change Settings**.
- 2 On the Change Settings page, next to Client Management, click **Configure Settings**.
- 3 In the Client Management Settings dialog box, on the General tab, under Display Options, select the location to which you want to change.
- 4 Uncheck **Show Symantec Endpoint Protection icon in notification area**.
- 5 Click **OK**.

To display the notification area icon

- 1 In the main window, in the sidebar, click **Change Settings**.
- 2 On the Change Settings page, next to Client Management, click **Configure Settings**.
- 3 In the Client Management Settings dialog, under Display Options, select the location to which you want to change.
- 4 Check **Show Symantec Endpoint Protection icon in notification area**.
- 5 Click **OK**.

What keeps your computer's protection current

Symantec engineers track reported outbreaks of computer viruses to identify new viruses. They also track blended threats, security risks such as spyware, and other vulnerabilities that can be exploited when your computer connects to the Internet. After they identify a risk, they write a signature (information about the risk) and store it in a definitions file. This definitions file contains the necessary information to detect, eliminate, and repair the effects of the risk. When Symantec Endpoint Protection scans for viruses and security risks, it searches for these types of signatures.

Other items that your client must keep current are the lists of allowed and restricted processes and attack signatures. The lists of processes help Proactive Threat Protection identify suspicious program behavior even if the client does not recognize a specific threat. Attack signatures provide the information that the Intrusion Prevention System needs to keep your computer safe from intruders.

In addition to definitions files, process lists, and attack signatures, your client needs to update its components occasionally. Such components can include the Antivirus and Antispyware Protection engine, the Proactive Threat Protection engine, and the Network Threat Protection firewall. These updates can consist of minor defect repairs or product enhancements.

Symantec makes updates available on an ongoing basis. Definitions are updated daily on the Symantec Security Response Web site. New definitions are made available at least weekly for delivery using LiveUpdate, and whenever a destructive new virus appears.

Note: Your administrator might control your client's definition update frequency.

See [“About LiveUpdate”](#) on page 27.

About the role of Symantec Security Response

The strength behind Symantec Endpoint Protection is Symantec Security Response. Symantec Security Response researchers disassemble each virus and security risk sample to discover its identifying features and behavior. With this information, they develop the definitions that Symantec products use to detect, eliminate, and repair the effects of viruses and security risks.

Because of the speed at which new viruses spread, Symantec Security Response has developed automated software analysis tools. Submissions of infected files from your computer to Symantec Security Response significantly reduces the time from discovery to analysis to cure.

Symantec Security Response researchers also research and produce technologies to protect computers from security risks such as spyware, adware, and hacking tools .

Symantec Security Response maintains an encyclopedia that provides detailed information about viruses and security risks. In necessary cases, they provide information about risk removal. The encyclopedia is located on the Symantec Security Response Web site at the following URL:

<http://securityresponse.symantec.com>

How protection is updated on managed clients

Your administrator determines how your virus and security risk definitions are updated. You may not have to do anything to receive new definitions.

Your administrator can set up the LiveUpdate feature in Symantec Endpoint Protection to make sure that your virus and security risk protection remains current. LiveUpdate connects to a computer that stores the updates, determines if your client needs to be updated, and downloads and installs the proper files. The computer that stores the updates may be a Symantec Endpoint Protection Manager server that is internal to your company. Alternatively, it may be a Symantec LiveUpdate server that you access through the Internet.

See [“About LiveUpdate”](#) on page 27.

How protection is updated on unmanaged clients

Administrators do not update the protection on unmanaged clients. You can update the software and definitions files by using LiveUpdate. If your unmanaged client uses the default LiveUpdate settings, it checks for updates from a Symantec server over the Internet once a week.

You can change the frequency with which LiveUpdate checks for updates. You can also run LiveUpdate manually if you know about a virus outbreak or other security risk outbreak.

See [“About LiveUpdate”](#) on page 27.

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.

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 security policy.

See [“Updating the security policy”](#) on page 16.

Updating the security policy

The settings that control protection on the client are stored on the computer in a policy file. This security policy file normally updates automatically. However, your administrator might instruct you to update the security policy manually under certain circumstances.

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

See [“Viewing the logs and the log details”](#) on page 142.

To update the security policy

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

Where to get more information

If you need more information, you can access the online Help. You can obtain additional information about viruses and security risks from the Symantec Security Response Web site at the following URL:

<http://securityresponse.symantec.com>

Accessing online Help

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

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

To access online Help

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

Accessing the Symantec Security Response Web site

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

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

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

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

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. If you have Symantec Endpoint Protection enabled on the client, you might experience the following types of client interaction:

Virus or security risk detection

If Auto-Protect or a scan detects a virus or a security risk, the Symantec Endpoint Protection Detection Results dialog appears with details about the infection. The dialog 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.

Application-related notifications

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.

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 24.

If you have Symantec Network Access Control enabled on the client, 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 quick 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 72.

See [“Quarantining risks and threats from the Risk Log and the Threat Log”](#) on page 148.

See [“About the Quarantine”](#) on page 84.

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:
 - 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.

In some cases, the client might not be able to perform the action that you selected.

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
- Security alerts

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.
- Your administrator updated the client software.

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 2-1 Application permission notifications

If you click	If you check “Remember my answer...” check box?	The client...
Yes	Yes	Allows the application and does not ask again.
Yes	No	Allows the application and asks you every time.
No	Yes	Blocks the application and does not ask you again.
No	No	Blocks the application and asks you every time.

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 122.

Changed application notifications

Occasionally, you might see a message that indicates an application has changed.

```

"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 following 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 features 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.

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:

```
Application Internet Explorer has been blocked,
file name is IEXPLORE.EXE.
```

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 120.

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.

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**.

After you close the message box, open the client to see if it displays any suggested procedures to restore network access.

Managing the client

This chapter includes the following topics:

- [About LiveUpdate](#)
- [Running LiveUpdate at scheduled intervals](#)
- [Running LiveUpdate manually](#)
- [Testing the security of your computer](#)
- [About locations](#)
- [Changing locations](#)
- [About Tamper Protection](#)
- [Enabling, disabling, and configuring Tamper Protection](#)

About LiveUpdate

LiveUpdate obtains program and protection updates for your computer by using your Internet connection.

Program updates are minor improvements to your installed product. These differ from product upgrades, which are newer versions of entire products. Program updates are usually created to extend the operating system or hardware compatibility, adjust a performance issue, or fix program errors. Program updates are released on an as-needed basis.

Note: Some program updates may require that you restart your computer after you install them.

LiveUpdate automates program update retrieval and installation. It locates and obtains files from an Internet site, installs them, and then deletes the leftover files from your computer.

Protection updates are the files that keep your Symantec products up-to-date with the latest threat protection technology. The protection updates you receive depend on which products are installed on your computer.

By default, LiveUpdate runs automatically at scheduled intervals. Based on your security settings, you can run LiveUpdate manually. You might also be able to disable LiveUpdate or change the LiveUpdate schedule.

Running LiveUpdate at scheduled intervals

You can create a schedule so that LiveUpdate runs automatically at scheduled intervals.

To run LiveUpdate at scheduled intervals

- 1 In the client, in the sidebar, click **Client Management > Options**.
- 2 In the Client Management Settings dialog box, click **Scheduled Updates**.
- 3 On the Scheduled Updates tab, check **Enable automatic updates**.
- 4 In the Frequency group box, select whether you want the updates to run daily, weekly, or monthly.
- 5 In the When group box, select the day or week and time of day you want the updates to run.
- 6 To specify how to handle missed updates, click **Advanced**.
- 7 In the Advanced Schedule Options dialog box, select the options for LiveUpdate to retry missed updates.

For more information on these options, click **Help**.

- 8 Click **OK**.
- 9 Click **OK**.

Running LiveUpdate manually

You can update the software and definitions files by using LiveUpdate. LiveUpdate retrieves the new definitions files from a Symantec site, and then replaces the old definitions files. Symantec products depend on current information to protect your computer from newly discovered threats. Symantec makes this information available to you through LiveUpdate.

To obtain updates by using LiveUpdate

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

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

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.

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.

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 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 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 and Log.

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.

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.

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

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 tampering**.
- 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 list box, select Block and Log or Log Only.
- 4 If you want to be notified when Tamper Protection detects suspicious behavior, check **Display the following 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 displays, type in new text or delete any text you want in the message field.
- 6 Click **OK**.

Symantec Endpoint Protection

- [Introducing Symantec Endpoint Protection](#)
- [Symantec Endpoint Protection client basics](#)
- [Managing Antivirus and Antispyware Protection](#)
- [Managing Proactive Threat Protection](#)
- [Managing Network Threat Protection](#)

Introducing Symantec Endpoint Protection

This chapter includes the following topics:

- [About Symantec Endpoint Protection](#)
- [How Symantec Endpoint Protection protects your computer](#)

About Symantec Endpoint Protection

You can install Symantec Endpoint Protection as either a stand-alone installation or as an administrator-managed installation. A stand-alone installation means that an administrator does not manage your Symantec Endpoint Protection software, so it is a stand-alone client.

If you manage your own computer, it must be one of the following types:

- A stand-alone 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 your corporate network that must meet security requirements before it connects.

The default settings for Symantec Endpoint Protection provide Antivirus and Antispyware Protection, Proactive Threat Protection, and Network Threat Protection by using a desktop firewall and host-based intrusion prevention. 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.

If an administrator manages your computer, some options may be locked or unavailable, depending upon your administrator's security policy. Your administrator runs scans on your computer and can set up scheduled scans.

Your administrator can advise you as to what tasks you should perform by using Symantec Endpoint Protection.

How Symantec Endpoint Protection protects your computer

Symantec Endpoint Protection provides a security policy that contains several types of protection for your computer.

The following types of protection work together to protect your computer from risks:

- Antivirus and Antispyware Protection
- Network Threat Protection
- Proactive Threat Protection

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.
- 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.

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.

Network threat protection provides a firewall and the intrusion prevention signatures to prevent intrusion attacks and malicious content. The firewall allows or blocks the traffic according to various criteria.

Firewall rules determine whether your computer allows or blocks an inbound or an outbound application or service 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 [“About Network Threat Protection”](#) on page 101.

About Proactive Threat Protection

Proactive Threat Protection makes sure that your computer has zero-day attack protection from unknown threats. This protection uses heuristic-based scans 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.

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.

Symantec Endpoint Protection client basics

This chapter includes the following topics:

- [About viruses and security risks](#)
- [How the client responds to viruses and security risks](#)
- [Enabling and disabling protection components](#)
- [Using the client with Windows Security Center](#)
- [Pausing and delaying scans](#)

About viruses and security risks

The Symantec Endpoint Protection client can scan for both viruses and for security risks, such as spyware or adware. These risks can put your computer, as well as a network, at risk. Antivirus and antispware 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.

By default, all antivirus and antispware scans, including Auto-Protect scans, check for viruses, Trojan horses, worms, and all categories of security risks.

[Table 5-1](#) describes the types of viruses and security risks.

Table 5-1 Viruses and security risks

Risk	Description
Viruses	<p>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.</p> <p>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.</p>
Malicious Internet bots	<p>The programs that run automated tasks over the Internet for malicious purposes.</p> <p>Bots can be used to automate attacks on computers or to collect information from Web sites.</p>
Worms	The programs that replicate without infecting other programs. Some worms spread by copying themselves from disk to disk, while others replicate only in memory to slow a computer down.
Trojan horses	The programs that contain code that is disguised as or hiding in something benign, such as a game or utility.
Blended threats	The threats that blend the characteristics of viruses, worms, Trojan horses, and code with server and Internet vulnerabilities to initiate, transmit, and spread an attack. Blended threats use multiple methods and techniques to spread rapidly and cause widespread damage throughout the network.
Adware	<p>The stand-alone or appended 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.</p> <p>Adware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads adware by accepting an End User License Agreement from a software program.</p>
Dialers	The programs that use a computer, without the user's permission or knowledge, to dial a 900 number or an FTP site. The programs typically accrue charges.
Hacking tools	The programs that are used by a hacker to gain unauthorized access to a user's computer. For example, one hacking tool is a keystroke logger, which tracks and records individual keystrokes and sends this information back to the hacker. The hacker can then perform port scans or vulnerability scans. Hacking tools may also be used to create viruses.
Joke programs	The programs that alter or interrupt the operation of a computer in a way that is intended to be humorous or frightening. For example, a program can be downloaded from a Web site, email message, or instant messenger program. It can then move the Recycle Bin away from the mouse when the user tries to delete it. It can also cause the mouse to click in reverse.
Other	Any other security risks that do not conform to the strict definitions of viruses, Trojan horses, worms, or other security risk categories.

Table 5-1 Viruses and security risks (*continued*)

Risk	Description
Remote access programs	The programs that allow access over the Internet from another computer so that they can gain information or attack or alter a user's computer. You might install a legitimate remote access program. A process might install this type of application without your knowledge. The program can be used for malicious purposes with or without modification of the original remote access program.
Spyware	<p>The stand-alone programs that can secretly monitor system activity and detect passwords and other confidential information and relay it back to another computer.</p> <p>Spyware can be unknowingly downloaded from Web sites, typically in shareware or freeware, or can arrive through email messages or instant messenger programs. Often a user unknowingly downloads spyware by accepting an End User License Agreement from a software program.</p>
Trackware	The stand-alone or appended applications that trace a user's path on the Internet and send information to the target system. For example, the application can be downloaded from a Web site, email message, or instant messenger program. It can then obtain confidential information regarding user behavior.

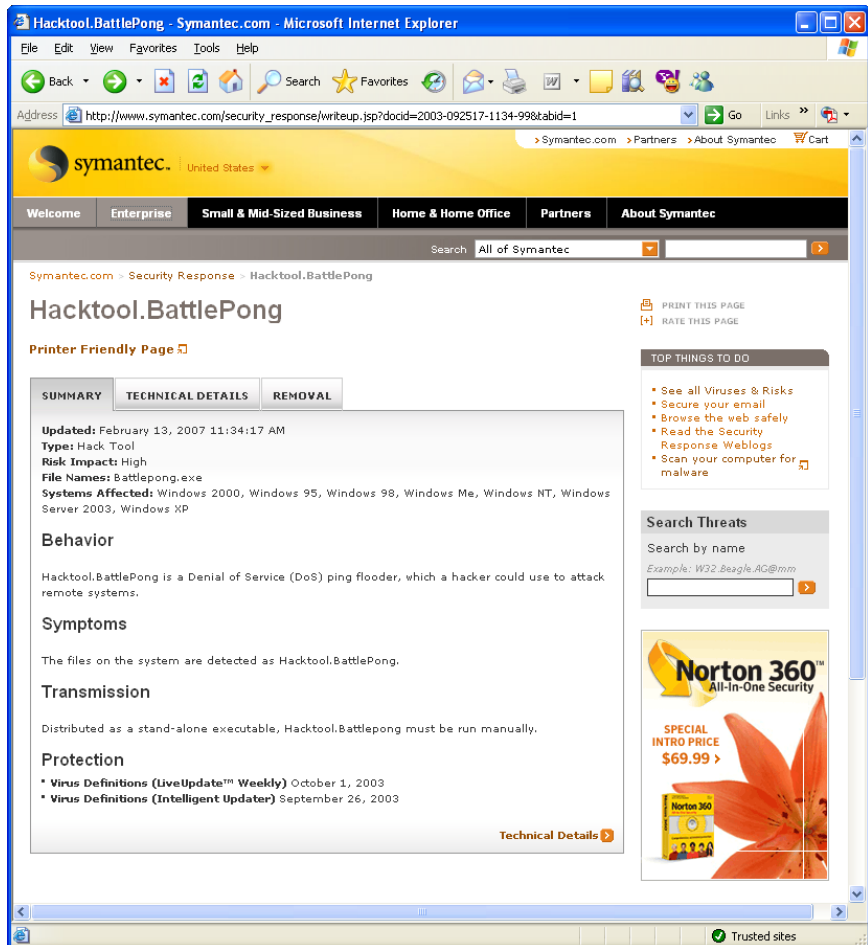
By default, antivirus and antispyware scans do the following:

- 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.

[Figure 5-1](#) shows the information about a hacking tool and how Symantec Security Response suggests that you handle it.

Figure 5-1 Symantec Security Response security risk description



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.

Enabling and disabling protection components

You can enable or disable the protections on your computer.

When any of the protections are disabled, the status bar at the top of the status page indicates that the protection is turned off. You can click the Fix option to enable all disabled protections. Or you can enable the individual protections separately.

Enabling and disabling Antivirus and Antispyware Protection

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 could be the work of a virus), or a security risk is detected, Auto-Protect alerts you.

You can enable or disable Auto-Protect for files and processes. You can also enable or disable Auto-Protect for Internet email and Auto-Protect for email groupware applications. In managed environments, your administrator can lock these settings.

When you might want to disable Auto-Protect

In some cases, 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 programs. If you plan to install more applications and you want to avoid the warning, you can temporarily disable Auto-Protect. Be sure to enable Auto-Protect when you have completed your task to ensure that your computer remains protected.

If you disable Auto-Protect, other types of scans (scheduled or startup) still run if you or your administrator has configured them to do so.

Your administrator might lock Auto-Protect so that you cannot disable it for any reason. Instead, your administrator might specify that you can disable Auto-Protect temporarily, but that Auto-Protect turns on automatically after a specified amount of time.

About Auto-Protect and Antivirus and Antispyware Protection status

Your Auto-Protect settings determine the antivirus and the antispyware protection status in the client and in the Windows notification area.

When any type of Auto-Protect is disabled, the antivirus and antispyware status appears red on the status page.

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

When you disable Auto-Protect for files and processes, the client icon appears with a universal no sign, a red circle with a diagonal slash. A green dot appears with the icon when File System Auto-Protect is enabled, even if Auto-Protect for email is disabled.

Enabling or disabling File System Auto-Protect

You can enable or disable Auto-Protect monitoring of the file system unless your administrator locks the setting.

To enable or disable File System Auto-Protect 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 Auto-Protect**.
 - Click **Disable Auto-Protect**.

To enable or disable File System Auto-Protect from the client

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

Enabling or disabling Auto-Protect for email

You can enable or disable Auto-Protect for internet email, Microsoft Outlook email, or Lotus Notes email. Your administrator might lock these settings.

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 and disabling Network Threat Protection

You may want to disable network threat protection in certain circumstances. For example, you may want to install an application that may otherwise cause the client to block it.

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.

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

See [“About Network Threat Protection”](#) on page 101.

See [“Blocking an attacking computer”](#) on page 121.

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

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.

See [“About Proactive Threat Protection”](#) on page 91.

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

To enable or disable Proactive Threat Protection

- 1 In the client, in the sidebar, click **Change settings**.
- 2 Next to Proactive Threat Protection, click **Change Settings**.
- 3 In the Proactive Threat Scan 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**.

Using the client with 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 5-2](#) shows the protection status reporting in WSC.

Table 5-2 WSC protection status reporting

Symantec product condition	Protection status
Symantec Endpoint Protection is not installed	NOT FOUND (red)
Symantec Endpoint Protection is installed with full protection	ON (green)
Symantec Endpoint Protection is installed, and virus and security risk definitions are out of date	OUT OF DATE (red)
Symantec Endpoint Protection is installed and File System Auto-Protect is not enabled	OFF (red)
Symantec Endpoint Protection is installed, File System Auto-Protect is not enabled, and virus and security risk definitions are out of date	OFF (red)
Symantec Endpoint Protection is installed and Rtvscan is turned off manually	OFF (red)

[Table 5-3](#) shows the Symantec Endpoint Protection firewall status reporting in WSC.

Table 5-3 WSC firewall status reporting

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

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

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

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 network administrator determines whether you can pause an administrator-scheduled scan.

For the scheduled scans that your network administrator initiates, you may also be allowed to delay the scan. If your administrator has enabled the Snooze feature, you can delay an administrator-scheduled scan for a set interval of time. When the scan resumes, it restarts from the beginning.

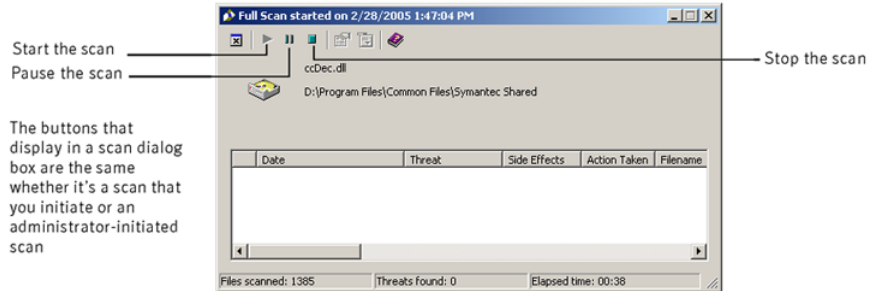
Pause the scan if want to resume the scan after a temporary break. Use the Snooze feature to delay the scan for a longer period of time.

Use the following procedures to pause a scan that you or your administrator initiated. If the Pause the Scan option is not available, your network administrator disabled the Pause feature.

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.

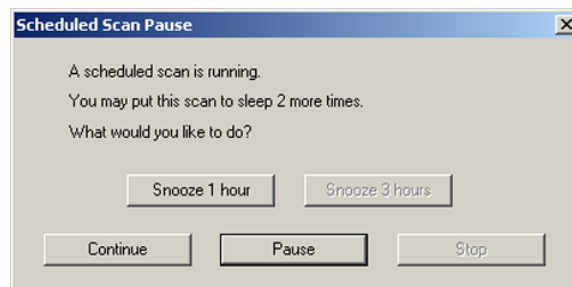
To pause a scan

- 1 When the scan runs, in the scan dialog box, click the pause icon.



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

If your administrator initiated the scan, the Scheduled Scan Pause dialog box appears.



- 2 In the Scheduled Scan Pause dialog box, click **Pause**.

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

- 3 In the scan dialog box, click the start icon to continue the scan.

To delay an administrator-scheduled scan

- 1 When the administrator-scheduled scan runs, in the scan dialog box, click **Pause the Scan**.
- 2 In the Scheduled Scan Pause dialog box, 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 the beginning. Your administrator specifies the number of times that you can delay the scheduled scan before this feature is disabled.

Managing Antivirus and Antispyware Protection

This chapter includes the following topics:

- [About Antivirus and Antispyware Protection](#)
- [About Auto-Protect](#)
- [Working with antivirus and antispyware scans](#)
- [Configuring antivirus and antispyware scanning](#)
- [Interpreting scan results](#)
- [Submitting information about antivirus and antispyware scans to Symantec Security Response](#)
- [Configuring actions for viruses and security risks](#)
- [Configuring notifications for viruses and security risks](#)
- [Configuring centralized exceptions for antivirus and antispyware scans](#)
- [About the Quarantine](#)
- [Managing the Quarantine](#)

About Antivirus and Antispyware Protection

The Symantec Endpoint Protection 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 59.

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.

See [“Configuring centralized exceptions for antivirus and antispyware scans”](#) on page 82.

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 **Change Settings**.
- 3 In the Antivirus and Antispyware Protection Settings dialog box, on the 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.
- 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 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.
- 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 excluding items from scans

You can configure the client to exclude a security risk from scans. You might want to exclude a risk from scanning. For example, you might need a particular piece of adware to use in your work. The client might not allow that piece of adware. If

your company's security policy allows the adware, you can exclude the risk from scans.

The client might flag a file as infected; however, the file does not contain a virus. This situation might happen because a particular virus definition is designed to catch every possible variation of the virus. Because the virus definition must be necessarily broad, the client sometimes reports that a clean file is infected.

If antivirus and antispyware scans continue to report a clean file as infected, you can exclude the file from scans. Exclusions are the items that you don't want or need to include in scans.

Your corporate security policy might let you run the software that the client reports as a risk. In that case, you can exclude the folders that contain the software.

You use a centralized exception to exclude items from scans. The exception applies to all antivirus and antispyware scans that you run. Your administrator might configure exceptions as well. Administrator-defined exceptions take precedence over user-defined exceptions.

See [“Configuring centralized exceptions for antivirus and antispyware scans”](#) on page 82.

Warning: Be careful with exclusions. If you exclude a file from a scan, the client does not take action to clean it if the file later becomes infected. This situation can be a potential risk to the security of your computer.

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 Symantec Endpoint Protection 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.

See [“Enabling and disabling Antivirus and Antispyware Protection”](#) on page 43.

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 60.

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 can disable 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 Outlook 98/2000/2002/2003/2007 (MAPI and Internet)
- Microsoft Exchange client 5.0 and 5.5

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

Antivirus and Antispyware Protection also includes Auto-Protect scanning for 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 60.

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 re-enable 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 Protection 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 your Antivirus and Antispyware Protection 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
- .xls

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 the 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 selected 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 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 options

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 **Change Settings**.
- 3 On the 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 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 Options 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**.

Working with antivirus and antispyware scans

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

Table 6-1 describes the available scans

Table 6-1 Available scans

Type	Description
Custom Scan	Scans a file, folder, drive, or entire computer at any time. You select the parts of the computer to scan.
Quick Scan	Quickly scans system memory and the locations that viruses and security risks commonly attack.
Full Scan	Scans the entire computer, including the boot sector and system memory. You might need to enter a password to scan network drives.
Scheduled Scan	Runs unattended at a specified frequency.
Startup Scan	Runs every time you start your computer and log on.

Table 6-1 Available scans (*continued*)

Type	Description
User-defined	Scans the specified file sets at any time.

As long as Auto-Protect is enabled, a daily quick 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 proactive threat scans”](#) on page 95.

How the Symantec Endpoint Protection client detects viruses and security risks

The client prevents virus infections on a computer by scanning the computer’s boot sector, memory, and files for viruses and security risks. The scan engine uses the virus and security risk signatures that are found in the definitions files. The scan engine performs an exhaustive search for any known viruses that are inside the executable files. Antivirus and antispyware scans search the executable parts of document files to find macro viruses.

You can perform a scan on demand or schedule a scan for when you are away from your desk.

[Table 6-2](#) describes the computer components that the client scans.

Table 6-2 Computer components that the client scans

Component	Description
Computer memory	The client searches the computer’s memory. Any file virus, boot sector virus, or macro virus may be memory-resident. Viruses that are memory-resident have copied themselves into a computer’s memory. In memory, a virus can hide until a trigger event occurs. Then the virus can spread to a floppy disk in the disk drive, or to the hard drive. If a virus is in memory, it cannot be cleaned. However, you can remove a virus from memory by restarting your computer when prompted.
Boot sector	The client checks the computer’s boot sector for boot viruses. Two items are checked: the partition tables and the master boot record.

Table 6-2 Computer components that the client scans (*continued*)

Component	Description
Floppy drive	A common way for a virus to spread is through the floppy disks. A floppy disk might remain in a disk drive when you start up or turn off your computer. When a scan starts, the client searches the boot sector and partition tables of a floppy disk that is located in the disk drive. When you turn off your computer, you are prompted to remove the disk to prevent possible infection.
Selected files	<p>The client scans individual files. For most types of scans, you select the files that you want scanned. The client software uses pattern-based scanning to search for traces of viruses within files. The traces of viruses are called patterns or signatures.</p> <p>Each file is compared to the innocuous signatures that are contained in a virus definitions file, as a way of identifying specific viruses. If a virus is found, by default the client tries to clean the virus from the file. If the file cannot be cleaned, the client quarantines the file to prevent further infection of your computer.</p> <p>The client also uses pattern-based scanning to search for signs of security risks within files and registry keys. If a security risk is found, by default the client quarantines the infected files and repairs the risk's effects. If the client cannot quarantine the files, it logs the attempt.</p>

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.

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.

Initiating on-demand scans

You can manually scan for viruses and security risks, such as adware and spyware, at any time. Select anything to scan from a single file to a floppy disk to your entire computer. On-demand scans include the Quick Scan and Full Scan. You can also create a custom scan to run on demand.

See [“Creating on-demand and startup scans”](#) on page 69.

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

To initiate a scan 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.

To initiate a scan from within the client

- ◆ Do one of the following actions:
 - In the client, on the Status page, next to Antivirus and Antispyware Protection, click **Options > Run Quick Scan**.
 - In the client, in the sidebar, click **Scan for threats**.
Do one of the following actions:
 - Under Quick Scan, click **Quick Scan**.
 - Under Full Scan, click **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.

Configuring antivirus and antispyware scanning

You can configure several different kinds of scans to protect your computer against viruses and security risks.

Creating scheduled scans

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 window.

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

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.

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

To create a scheduled scan

- 1 In the client, in the sidebar, click **Scan for threats**.
- 2 Click **Create a New Scan**.
- 3 In the What To Scan dialog box, select one of the following types of scan to schedule:
 - Custom: Scans the selected areas of the computer for viruses and security risks.
 - Quick: Scans the areas of the computer that viruses and security risks most commonly infect.
 - Full: Scans the entire computer for viruses and security risks.

- 4 If you selected Custom, check the appropriate check boxes to specify where to scan.

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.

- 5 Click **Next**.
- 6 In the Scan Options dialog box, you can do any of the following actions:
 - Change the default settings for what is scanned.
The default setting is to scan all files.
 - Specify how the client responds if a virus or security risk is detected.
By default, the client cleans viruses from infected files and repairs any side effects. If the client cannot remove the virus, the client quarantines the file.
By default, the client quarantines security risks and removes or repairs any side effects. If the client cannot quarantine and repair the risk, the client logs the event.
- 7 Under Scan Enhancements, select any of the locations.
- 8 Click **Advanced**.
- 9 You can set any of the following options:
 - Compressed files options
 - Backup options
 - Dialog options
 - Tuning options
 - Storage migration options

- 10 Under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.
- 11 Click **OK**.
- 12 In the Scan Options dialog box, you can also change the following options:
 - **Actions:** Change first and second actions to take when viruses and security risks are found.
 - **Notification:** 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.
 - **Centralized Exceptions:** Create an exception for a security risk detection.
- 13 Click **Next**.
- 14 In the When To Scan dialog box, click **At Specified Times**, and then click **Next**.
- 15 In the Schedule dialog box, specify the frequency and when to scan.
- 16 Click **Advanced**.
- 17 In the Advanced Schedule Options dialog box, do the following actions:
 - Check **Retry the scheduled scan within <number> hours of the scheduled time**. Set the number of hours within which you want the scan to run. For example, you might want a weekly scan to run only if it is within three days of the scheduled time for the missed event.
 - Check or uncheck **Perform this user-defined scheduled scan even when the user is not logged in**. User-defined scans are always run if the user is logged in, regardless of this setting.

For managed clients, the administrator may override these settings.
- 18 Click **OK**.
- 19 In the Schedule dialog box, click **Next**.
- 20 In the Scan Name dialog box, type a name and description for the scan.

For example, call the scan: Friday morning
- 21 Click **Finish**.

About creating multiple scheduled scans

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.

Creating on-demand and startup scans

Some users supplement a scheduled scan with an automatic scan whenever they start their computers 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.

Note: If you create more than one startup scan, the scans run sequentially in the order in which they were created.

Your Antivirus and Antispyware Protection also includes a startup scan that is called the Auto-Generated Quick Scan. The auto-generated scan checks the common infection points on the computer each time that 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.

On-demand scans must be initiated manually.

See [“Initiating on-demand scans”](#) on page 65.

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

To create an on-demand or startup scan

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

- 6 If you selected Custom, in the Select Files dialog box, check the appropriate files and folder that you want to scan.

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.

- 7 Click **Next**.

- 8 In the Scan Options dialog box, you can do any of the following actions:

- Change the default settings for what is scanned.
The default setting is to scan all files.
- Specify how the client responds if a virus or security risk is detected.
By default, the client cleans viruses from infected files and repairs any side effects. If the client cannot remove the virus, the client quarantines the file.
By default, the client quarantines security risks and removes or repairs any side effects. If the client cannot quarantine and repair the risk, the client logs the event.

- 9 Under Scan Enhancements, check any of the locations.

- 10 Click **Advanced**.

- 11 In the Advanced Scan Options dialog box, you can set any of the following options:

- Compressed files options
- Backup options
- Dialog options
- Tuning options
- Storage migration options

- 12 Under Dialog options, in the drop-down list, click **Show scan progress**, and then click **OK**.
- 13 When you are finished configuring advanced options, click **OK**.
- 14 You can also change the following options:
 - **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.
 - **Centralized Exceptions:** Create exceptions for scanning.
- 15 When you are finished configuring scan options, click **OK**.
- 16 In the When to Run dialog box, do one of the following actions:
 - Click **On Demand**.
 - Click **At Startup**.
- 17 In the Scan Options dialog box, click **Next**.
- 18 Type a name and description for the scan.
For example, call the scan: MyScan1
- 19 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 48.

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 6-3](#) describes the options and the results dialog box.

Table 6-3 Options in the Results dialog box

Button	Description
Remove Risks Now	<p>Displays the Remove Risk dialog box.</p> <p>In the Remove Risk dialog box, you can select one of the following choices for each risk:</p> <ul style="list-style-type: none"> ■ Yes The client removes the risk. The removal of the risk might require a restart. Information in the dialog box indicates whether or not a restart is required. ■ No When you close the results dialog box, 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.
Close	<p>Closes the results dialog box if you do not need to take action on any of the risks</p> <p>If you need to take action, one of the following notifications appears:</p> <ul style="list-style-type: none"> ■ Remove Risk Required. Appears when a risk requires process termination. If you choose to remove the risk, you return to the results dialog box. If a restart is also required, the information in the risk's row in the dialog box indicates that a restart is required. ■ Restart Required. Appears when a risk requires a restart. ■ Remove Risk and Restart Required. Appears when a risk requires process termination and another risk requires a restart.

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

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

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

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

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

See [“Acting on infected files”](#) on page 20.

Submitting information about antivirus and antispyware scans 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 antivirus and antispyware 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 89.

To submit information about antivirus and antispyware 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 On the Submissions tab, check **Automatically submit antivirus and antispyware detections**.
- 4 Click **OK**.

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 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.

- 2 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.

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

Clean risk	<p>Removes the virus from the infected file. This setting is the default first action for viruses.</p> <p>Note: This action is only available as a first action for viruses. This action does not apply to security risks.</p> <p>This setting should always be the first action for viruses. If the client successfully cleans a virus from a file, you don't 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.</p> <p>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.</p> <p>In some instances, however, the cleaned file might not be usable. The virus might have caused too much damage.</p> <p>Some infected files cannot be cleaned.</p>
Quarantine risk	<p>Moves the infected file from its original location to the Quarantine. Infected files within the Quarantine cannot spread viruses.</p> <p>For viruses, moves the infected file from its original location to the Quarantine. This setting the default second action for viruses.</p> <p>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.</p> <p>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.</p>

Delete risk	<p>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.</p> <p>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.</p> <p>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.</p>
Leave alone (log only)	<p>Leaves the file as is.</p> <p>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.</p> <p>You can use Leave alone (log only) as a second action for both macro and non-macro viruses.</p> <p>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.</p> <p>For security risks, 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.</p> <p>Your administrator might send a customized message that explains how to respond.</p>

See [“Tips for assigning second actions for viruses”](#) on page 78.

See [“Tips for assigning second actions for security risks”](#) on page 78.

- 4 Repeat steps 1 and 3 for each category for which you want to set specific actions.
- 5 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.
- 6 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	<p>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.</p> <p>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.</p>
The type of virus that has infected your computer	<p>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.</p>
The type of scan that you run on your computer	<p>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 .</p>

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 6-4](#) describes the rating factors and what a high rating means for each of them.

Table 6-4 Risk impact factors

Rating factor	Description
Privacy Impact	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.
Performance Impact	Measures the extent to which a security risk degrades a computer's performance. A high rating indicates that performance is seriously degraded.
Stealth Rating	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.

Table 6-4 Risk impact factors (continued)

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

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 that 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 6-5 describes the variable fields that are available for notifications messages.

Table 6-5 Message variable fields

Field	Description
VirusName	The name of the virus or security risk that was found.

Table 6-5 Message variable fields (*continued*)

Field	Description
ActionTaken	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.
Status	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.
Filename	The name of the file that the virus or security risk infected.
PathAndFilename	The complete path and name of the file that the virus or security risk infected.
Location	The drive on the computer on which the virus or security risk was located.
Computer	The name of the computer on which the virus or security risk was found.
User	The name of the user who was logged on when the virus or security risk occurred.
Event	The type of event, such as "Risk Found."
LoggedBy	The type of scan that detected the virus or security risk.
DateFound	The date on which the virus or security risk was found.
StorageName	The affected area of the application, for example, File System Auto-Protect or Lotus Notes Auto-Protect.
ActionDescription	A full description of the actions that were taken in response to detecting the virus or security risk.

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 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 Notifications Options dialog box, under Detection Options, check **Display notification message on infected computer**. 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:
- | | |
|-----------------------------------|---|
| Automatically terminate processes | 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. |
| Automatically stop services | Configures the scan to stops 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. |
- 6 Click **OK**.

Configuring centralized exceptions for antivirus and antispyware scans

Centralized exceptions are the items that you want to exempt from scanning, such as a particular security risk or a particular file. Typically you do not need to create exceptions.

For managed clients, your administrator may have created centralized exceptions for your scans. You can view administrator-defined exceptions, however you cannot modify them. If you create a centralized exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.

This procedure describes configuring a centralized exception from the Change Settings page. You can also configure exceptions when you create or modify an on-demand, scheduled, or startup scan, or when you modify Auto-Protect settings. Exceptions apply across all antivirus and antispyware scans. If you configure an exception when you create or edit a particular scan, the exception applies to all antivirus and antispyware scans.

Note: You can also configure centralized exceptions for proactive threat scans.

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

To exclude a security risk from scans

- 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 Exception > Known Risks**.
- 4 In the Select Security Risks 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 **OK**.

To exclude a file from scans

- 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 > File**.
- 4 In the Add File Exception dialog box, select the file or type the filename that you want to exclude, and then click **Add**.
- 5 Click **OK**.
- 6 In the Centralized Exceptions dialog box, click **OK**.

To exclude a folder from scans

- 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 > Folder Exceptions**.
- 4 In the Add Folder Exception dialog box, select the folder or type the folder name that you want to exclude.
- 5 Check **Include Subfolders** if you want to exclude subfolders of the selected folder.
- 6 Select the folder that you want to exclude, and then click **OK**.
- 7 In the Centralized Exceptions dialog box, click **OK**.

To exclude extensions from scans

- 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 > Extensions**.
- 4 In the Add Extension Exceptions dialog box, type the extension that you want to exclude.

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

- 5 Click **Add**.
- 6 Repeat step 4 through step 5 to add more extensions.
- 7 In the Centralized Exceptions dialog box, click **OK**.

About the Quarantine

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 86.

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 86.

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.

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.

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 89.

To rescan files in the Quarantine using the Repair Wizard

- 1 When the Repair Wizard appears, click **Yes**.
- 2 Click **Next**.

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.

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 **Clean**.

When a repaired file can't 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 88.

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.

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.

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**.
The client deletes 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.

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.

Managing Proactive Threat Protection

This chapter includes the following topics:

- [About Proactive Threat Protection](#)
- [Configuring how often to run proactive threat scans](#)
- [Managing proactive threat detections](#)
- [Configuring notifications for proactive threat scan detections](#)
- [Submitting information about proactive threat scans to Symantec Security Response](#)
- [Configuring a centralized exception for proactive threat scans](#)

About Proactive Threat Protection

Proactive Threat Protection gives you zero-day attack protection. Zero-day attack protection means protection against unknown threats or vulnerabilities. Proactive Threat Protection scans 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 Protection 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 Protection 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 Protection?

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.

About proactive threat scans

Proactive threat scans differ from antivirus and antispyware scans. Proactive threat scans examine certain types of processes or applications that exhibit suspicious behavior.

Proactive threat 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 [“Configuring a centralized exception for 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 7-1](#) describes the processes that proactive threat scans detect.

Table 7-1 Processes detected by proactive threat scans

Type of processes	Description
Trojan horses and worms	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.

Table 7-1 Processes detected by proactive threat scans (*continued*)

Type of processes	Description
Keyloggers	Processes that exhibit characteristics of keyloggers. Proactive threat scans detect commercial keyloggers, but they also detect the unknown processes that exhibit keylogger behavior.
Commercial applications	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.
Adware and spyware	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.

About exceptions for 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 [“Configuring a centralized exception for proactive threat scans”](#) on page 100.

About 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 73.

See [“Managing the Quarantine”](#) on page 86.

See [“Viewing the logs and the log details”](#) on page 142.

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

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 [“Configuring a centralized exception for 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, it only changes the number of total detections.

See [“Managing proactive threat detections”](#) on page 95.

Configuring how often to run 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 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 Scan 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.

Managing 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.

Note: The detection of Trojan horses, worms, and keyloggers is currently not supported on Windows server operating systems. 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.)

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.

Specifying the types of processes that 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 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 Scan 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**.

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 Scan 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, select 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 Scan 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, select Low or High.
- 5 In the drop-down list, select Log, Terminate, or Quarantine.
- 6 Click **OK**.

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 Scan Settings dialog box, on the Scan Details tab, under Commercial Applications, do any of the following actions:
 - Set the action for commercial keyloggers to Log, Terminate, Quarantine, or Ignore.
 - Set the action for commercial remote control applications to Log, Terminate, Quarantine, or Ignore.
- 4 Click **OK**.

Configuring notifications for 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 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 Scan 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 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 enable or disable submitting information 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 Submissions tab, check or uncheck **Automatically submit Proactive Threat Scan detections**.
- 4 Click **OK**.

Configuring a centralized exception for proactive threat scans

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

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. You can view administrator-defined exceptions, however you cannot modify them. If you create a centralized exception that conflicts with an administrator-defined exception, the administrator-defined exception takes precedence.

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

To configure a centralized exception for 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 **Proactive Threat Protection Exception**.
- 4 In the Add Proactive Threat Exception dialog box, type a process name or select a 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**.

Managing Network Threat Protection

This chapter includes the following topics:

- [About Network Threat Protection](#)
- [Configuring the firewall](#)
- [Configuring intrusion prevention](#)
- [Configuring application-specific settings](#)
- [Enabling and disabling file and print sharing](#)

About Network Threat Protection

Network attacks take advantage of the way that computers transfer information. The Symantec Endpoint Protection client can protect your computer by monitoring the information that comes into and out of your computer, and by blocking attack attempts.

Information travels across the Internet in the form of packets. Each packet includes a header that contains information about the sending computer, the intended recipient, how the data in the packet should be processed, and the port that should receive the packet.

Ports are the channels that divide the stream of information that comes from the Internet into separate paths that the individual applications handle. When Internet applications run on a computer, they listen to one or more ports and accept the information that is sent to these ports.

Network attacks take advantage of the weaknesses in specific Internet programs. Attackers use the tools that send the packets that contain malicious programming

code to a particular port. If a program that is vulnerable to this attack listens to that port, the code can let the attacker gain access to, disable, or even take control of the computer. The programming code that is used to generate the attacks can exist inside a packet, or it can span several packets.

Your client is installed with default settings for Network Threat Protection. In most cases you do not have to change the settings. It is generally safe to leave the settings as they are. However, if you have a detailed understanding of networks, you can make many changes in the client firewall to fine-tune your protection.

How the client protects against network attacks

The client includes the following tools that protect your computer from intrusion attempts:

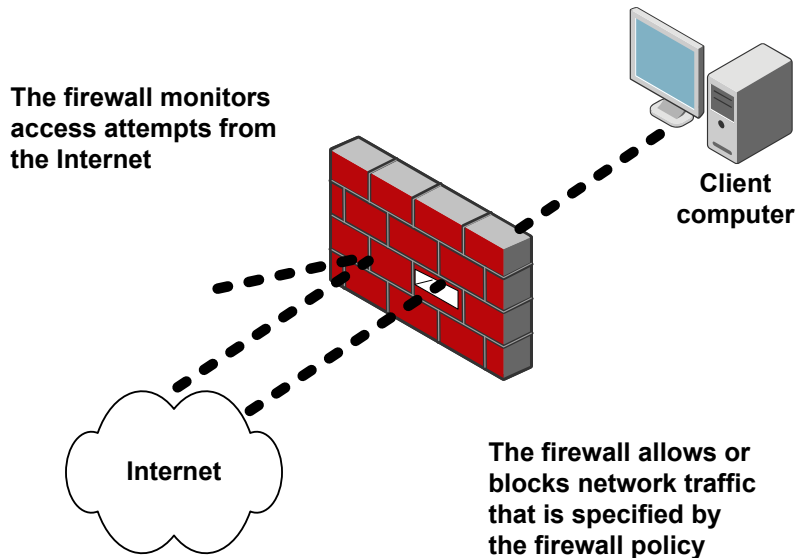
Firewall	Monitors all Internet communication and creates a shield that blocks or limits the attempts to view information on your computer.
Intrusion prevention	Analyzes all inbound the information and the outbound information for the data patterns that are typical of an attack.

To assess how to better protect your computer, you can test the vulnerability of your computer to outside network attacks and viruses. To test your computer, you can run several scans.

See [“Testing the security of your computer”](#) on page 29.

About the firewall

The firewall is software that provides a barrier between the computer and the Internet. A firewall prevents unauthorized users from accessing privately owned computers and the networks that connect to the Internet. It detects possible hacker attacks, protects personal information, and eliminates unwanted sources of network traffic, such as intrusion attempts.



All information that enters or leaves the private network must pass through the firewall. The firewall examines the information packets and blocks those that do not meet the specified security criteria. The way it examines the information packets is through the use of firewall rules. Firewall Policies consist of one or more rules that work together to allow or block users from accessing the network. Only authorized traffic can pass. A Firewall Policy defines the authorized traffic.

The firewall works in the background. Your administrator determines the level of interaction that you have with the client by permitting or by blocking your ability to configure firewall rules and firewall 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.

How the firewall monitors communications

When the firewall is active, it monitors the communications between your computer and the other computers on the Internet.

The firewall protects you from improper connection attempts by using one of the following methods:

- Blocks inbound traffic and outbound traffic.
- Warns you of any connection attempts from other computers and the attempts by applications on your computer to connect to other computers.

You can control the level of protection by customizing firewall protection.

About the intrusion prevention system

The intrusion prevention system (IPS) is the Symantec Endpoint Protection client's second layer of defense after the firewall. The intrusion prevention system is a network-based system that operates on every computer on which the client is installed and the IPS system is enabled. If a known attack is detected, one or more intrusion prevention technologies can automatically block it.

The intrusion prevention system analyzes all the inbound and the outbound information for the data patterns that are typical of an attack. It detects and blocks malicious traffic and attempts by outside users to attack your computer. Intrusion prevention monitors the outbound traffic and prevents the spread of worms.

Table 8-1 lists the common security problems that the intrusion prevention system monitors.

Table 8-1 Common security problems

Problem	Protection
Port scans	Cloaks the inactive ports on your computer and detects port scans.
Denial of service attacks	Examines all network packets for specific known attacks that limit your computer's use of the services that you would normally expect to have.
Intrusions	Detects and blocks malicious traffic and the attempts by outside users to attack your computer, and scans outbound traffic to prevent the spread of worms.

How intrusion prevention analyzes traffic

The intrusion prevention system scans each packet that enters and exits computers in your network for attack signatures, and for packet sequences that identify an attacker's attempt to exploit a known operating system or program vulnerability.

If the information matches a known attack, the IPS automatically discards the packet. The IPS can also sever the connection with the computer that sent the data for a specified amount of time. This feature is called active response, and it protects computers on your network from being affected in any way.

The client includes the following types of IPS engines that identify attack signatures.

Symantec IPS signatures

The Symantec IPS signatures use a stream-based engine that scans multiple packets. Symantec IPS signatures intercept network data at the session layer and capture segments of messages that are passed back and forth between an application and the network stack.

The Symantec IPS examines packets in two ways. It scans each packet individually by looking for the patterns that do not adhere to specifications and that can crash the TCP/IP stack. It also monitors the packets as a stream of information, by looking for the commands that are directed at a particular service to exploit or crash the system. The IPS can remember the list of patterns or partial patterns from previous packets, and the IPS can apply this information to subsequent packet inspections.

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.

Custom IPS signatures

The custom IPS signatures use a packet-based engine that scans each packet individually.

Both the stream-based and packet-based engines detect signatures in the network data that attack the TCP/IP stack, operating system components, and the application layer. However, packet-based signatures can detect attacks in the TCP/IP stack earlier than stream-based signatures. The packet-based engine does not detect signatures that spans multiple packets. The packet-based IPS engine is more limited, because it does not buffer partial matches, and it scans single packet payloads only.




The intrusion prevention system logs the detected attacks in the Security Log. The custom IPS signatures may log detected attacks in the Packet Log.

See [“Configuring intrusion prevention”](#) on page 119.

Viewing network activity

You can view information about inbound traffic and outbound traffic from your computer. You can also view a list of applications and services that have run since the client service started. [Table 8-2](#) describes the actions that the client takes on traffic. The icons that represent the actions that the client takes for the applications that access the client computer or network.

Table 8-2 Actions that the client takes when applications access the client or network

Icon	Action	Description
	Allow	Allows the inbound traffic to access the client computer and the outbound traffic to access the network. If the client receives traffic, the icon displays a small blue dot in the lower left-hand corner. If the client sends traffic, the icon displays the dot in the lower right-hand corner.
	Ask	Asks whether inbound traffic is allowed to access your computer or company network. If you or your administrator configured the client to ask you whether to allow your applications to access network resources, the icon appears with a small, yellow question mark. You can set the client to remember your responses, so that you do not have to tell the client again.
	Block	Blocks the inbound traffic and the outbound traffic from accessing the network or an Internet connection.

Note: The client does not detect network traffic from PDA (personal digital assistant) devices.

To view traffic history

- 1 In the client, in the sidebar, click **Status**.
- 2 Beside Network Threat Protection, click **Options > View Network Activity**.
 For more information on the graphs and fields, click **Help**.
- 3 Click **Close**.

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

To show or hide Windows services and broadcast traffic

- 1 In the client, in the sidebar, click **Status**.
- 2 Beside Network Threat Protection, click **Options > View Network Activity**.
- 3 In the Network Activity dialog box, right-click the Running Applications field and do the following actions:

- To show or hide Windows services, check or uncheck **Show Windows Services**.
 - To display broadcast traffic, check **Show Broadcast Traffic**.
 - To display unicast traffic, uncheck **Show Broadcast Traffic**.
- 4 Click **Close**.
- To change the way the application icon appears**
- 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 one of the following views:
 - Large Icons
 - Small Icons
 - List
 - Application Details
 - Connection Details
 - 4 Click **Close**.

Configuring the firewall

The default firewall settings protect your computer. If the default settings are not appropriate, you can customize the Firewall Policy. To customize the Firewall Policy, you add or change the following firewall features:

Firewall rules	<p>Monitors all Internet communication and creates a shield that blocks or limits attempts to view information on the computer. Firewall rules can make your computer invisible to others on the Internet.</p> <p>Firewall rules protect remote users from hacker attacks and prevents hackers from gaining backdoor access to the corporate network through these computers. You can notify users when the firewall blocks an application on their computer.</p>
Smart traffic filters	<p>Allows specific the types of traffic that are required on most networks. This type of traffic includes DHCP, DNS, and WINS traffic.</p>

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

Your administrator may or may not have given you permission to customize firewall rules and firewall settings. If you do not have permission, the administrator creates firewall rules and enables settings in a Firewall Policy and distributes the policy to the client. If you do have permission, you can create rules and modify settings on the client to fit your network environment. Your administrator may have configured the client to merge the rules that your administrator created and rules that you have created.

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

See [“Enabling and disabling Network Threat Protection”](#) on page 45.

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. Firewall rules control how the client protects the client computer from malicious inbound traffic and outbound traffic. The firewall automatically checks all the inbound and the outbound packets against these rules. The firewall then allows or blocks the packets that are based on the information that is specified in rules.

About the elements of a rule

A firewall rule describes the conditions in which a network connection may be allowed or blocked.

[Table 8-3](#) describes the criteria you use to define a firewall rule.

Table 8-3 Firewall rule conditions

Condition	Description
Triggers	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.

Table 8-3 Firewall rule conditions (*continued*)

Condition	Description
Conditions	<p>Schedule and screen saver state.</p> <p>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.</p>
Actions	<p>Allow or block, and log or do not log.</p> <p>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.</p> <p>If the firewall allows traffic, it lets the traffic that the rule specifies to access your network.</p> <p>If the firewall blocks traffic, it blocks the traffic that the rule specifies so that it does not access your network.</p>

For example, a rule may state that remote port 80 is allowed to the IP address 192.58.74.0, between 9 AM and 5 PM daily.

[Table 8-4](#) describes the triggers you can define in a firewall rule.

Table 8-4 Firewall rule triggers

Trigger	Description
Application	<p>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.</p>

Table 8-4 Firewall rule triggers (continued)

Trigger	Description
Host	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.
Protocol	<p>A protocol trigger identifies one or more network protocols that are significant in relation to the described network traffic.</p> <p>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.</p> <p>You can define the following types of protocols:</p> <ul style="list-style-type: none">■ 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.

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 don't 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.

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.

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. The firewall inspects the rules in this order. If the first rule does not specify how to handle a packet, the firewall inspects the second rule for information on how to handle a packet. This process continues

until the firewall finds a match. After the firewall finds a match, the firewall takes the action that the rule specifies, and subsequent lower priority rules are not inspected. For example, if a rule that blocks all traffic is listed first, followed by a rule that allows all traffic, the client blocks all traffic.

You can order the rules within the priority categories so that the firewall evaluates the rules in a logical sequence. You can order the rules so that they are evaluated according to exclusivity, with the most restrictive rules evaluated first and the most general rules evaluated last. For example, if you create rules that block traffic, you must place these rules near the top because other rules may allow the traffic.

Table 8-5 shows the order in which the firewall processes the rules and the settings.

Table 8-5 Order that the firewall processes rules, firewall settings, IPS signatures, and IPS settings

Priority	Setting
First	Custom IPS signatures
Second	Intrusion prevention settings, traffic settings, and stealth settings
Third	Smart traffic filters
Fourth	Firewall rules
Fifth	Port scan checks
Sixth	IPS signatures that are downloaded through LiveUpdate

Adding rules

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.

To add 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, 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 network adapter for the rule, in the **Apply this rule to the following network adapter** drop-down list, select a network adapter.

- 6 To choose whether you want the state of the screen saver to activate the rule, select an option in the **Apply this rule while the screen saver is** drop-down list.
- 7 To specify the state of the screen saver, select an option in the **Apply this rule while the screen saver is** drop-down list.
- 8 To define the triggers for the rule, select any one of the following tabs:
 - Hosts
 - Ports and Protocols
 - ApplicationsFor more information about the options on each tab, click **Help**.
- 9 To define the time period when the rule is active or inactive, click **Scheduling**, and then set up a schedule.
- 10 When you're done making changes, click **OK**.
- 11 In the Configure Firewall Rules dialog box, make sure the check mark appears in the Rule Name column to enable the rule.
- 12 Click **OK**.

Changing the order of rules

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

See [“About the rule processing order”](#) on page 111.

To change the order of 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 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 blue up arrow.
 - To have the firewall process this rule after the rule below it, click the blue down arrow.
- 5 When you are done moving rules, click **OK**.

Enabling and disabling rules

You must enable rules so that the firewall to 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.

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

Exporting and importing rules

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

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

To export 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**.

Editing and deleting rules

You can change rules if they do not function the way that you want.

You can remove the firewall rules you have added when they are no longer necessary.

To edit 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 rule, and then click **Edit**.
- 4 Change the settings on any tab.
- 5 When you have finished changing rules, click **OK**.

To delete 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 one or more rules and click **Delete**.
- 4 In the message box that appears, click **Yes**.
- 5 Click **OK**.

Enabling traffic settings and stealth Web browsing settings

You can enable various traffic settings and stealth Web browsing settings in the Firewall Policy to protect against certain types of network attacks on the client.

[Table 8-6](#) defines the traffic and stealth settings you can enable.

Table 8-6 Traffic and stealth Web browsing settings

Options	Description
Enable driver-level protection	<p>Checks the traffic that comes from both the TCP/IP stack and other protocol drivers.</p> <p>Most attacks in an enterprise network occur through Windows TCP/IP connections. Other attacks can potentially be launched through other protocol drivers. Any protocol drivers that access a network are network applications. The client then blocks protocol drivers from accessing the network unless a rule specifically allows the access. If a protocol driver tries to access the network, a notification asks whether you want to allow it.</p>
Enable NetBIOS protection	<p>Blocks the NetBIOS traffic from an external gateway.</p> <p>You can use Network Neighborhood file and printer sharing on a LAN and protect a computer from NetBIOS exploits from any external network. This option blocks the NetBIOS packets that originate from the IP addresses that are not part of the defined ICANN internal ranges. ICANN internal ranges include 10.x.x.x, 172.16.x.x, 192.168.x.x, and 169.254.x.x, with the exception of the 169.254.0.x and 169.254.255.x subnets. NetBIOS packets include UDP 88, UDP 137, UDP 138, TCP 135, TCP 139, TCP 445, and TCP 1026.</p>
Allow token ring traffic	<p>Allows the client computers that connect through a token ring adapter to access the network, regardless of the firewall rules on the client.</p> <p>If you disable this setting, any traffic that comes from the computers that connect through a token ring adapter cannot access the corporate network. The firewall does not filter token ring traffic. It either allows all token ring traffic or blocks all token ring traffic.</p>
Block all traffic until the firewall starts and after the firewall stops	<p>Blocks all inbound traffic to and outbound traffic from the client computer when the firewall is not running for any reason.</p> <p>The computer is not protected:</p> <ul style="list-style-type: none"> ■ After the client computer turns on and before the firewall service starts. ■ After the firewall service stops and the client computer stops. <p>This time frame is a small security hole that can allow unauthorized communication. This setting prevents unauthorized applications from communicating with other computers.</p>
Allow initial DHCP and NetBIOS traffic	<p>Allows the initial traffic that enables network connectivity. This traffic includes the initial DHCP and NetBIOS traffic that allows the client to obtain an IP address.</p>
Enable stealth mode Web browsing	<p>Detects the HTTP traffic from a Web browser on any port and removes the browser name and version number, the operating system, and the reference Web page. It stops Web sites from knowing which operating system and browser the computer uses. It does not detect HTTPS (SSL) traffic.</p>

Table 8-6 Traffic and stealth Web browsing settings (*continued*)

Options	Description
Enable TCP resequencing	<p>Prevents an intruder from forging or spoofing an individual's IP address.</p> <p>Hackers use IP spoofs to hijack a communication session between two computers, such as computer A and B. A hacker can send a data packet that causes computer A to drop the communication. Then the hacker can pretend to be computer A and communicate with and attack computer B.</p> <p>To protect the computer, TCP resequencing randomizes TCP sequence numbers.</p>
Enable OS fingerprint masquerading	<p>Prevents the detection of the operating system of a client computer.</p> <p>The client changes the TTL and identification value of TCP/IP packets to prevent the identification of an operating system.</p>
Enable anti-MAC spoofing	<p>Allows inbound and outbound ARP (Address Resolution Protocol) traffic only if an ARP request was made to that specific host. It blocks all other unexpected ARP traffic and logs it in the Security Log.</p>

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

You can enable Smart traffic filters to allow DHCP, DNS, and WINS traffic on most networks. The Smart traffic filters allow outbound requests and inbound replies for the network connections that have been configured to use DHCP, DNS, and WINS, respectively.

The Smart traffic filters allow a DHCP, DNS, or WINS client to receive an IP address from a server while they protect the client against attacks from a network, as follows:

- If the client sends a request to the server, the client waits for five seconds to allow an inbound response.
- If the client does not send a request to the server, each filter does not allow the packet.

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

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**.

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. Your administrator may have configured this option to be unavailable.

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 network 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**.

You can allow all traffic by disabling Network Threat Protection.

See [“Enabling and disabling Network Threat Protection”](#) on page 45.

Configuring intrusion prevention

You can customize the intrusion prevention settings to change the default protection.

You can enable:

- 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.

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

To enable 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, 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**.

- 5 To hear a beep when the notification appears, check **Use sound when notifying users**.
- 6 Type an amount of time you want the notifications to appear in the **Number of seconds to display notifications** field.
- 7 Click **OK**.

Blocking 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.

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**.

- 3 In the Security Log, select the row that contains Active Response in the Event Type column, and then click **Action > Stop Active Response**.
To unblock the blocked IP addresses, click **Action > Stop All Active Response**. If you unblock an active response, the Event Type column displays Active Response canceled. If the active response times out, the Event Type column displays Active Response disengaged.
- 4 In the message box that appears, click **OK**.
- 5 Click **File > Exit**.

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.

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

See “[Viewing network activity](#)” on page 105.

To configure application-specific settings

- 1 In the client, in the sidebar, click **Status**.
- 2 Beside Network Threat Protection, click **Options > View Applications List**.
- 3 In the View Applications List 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 field, 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 Applications List dialog box, to change the action, right-click the application, and then click **Allow**, **Ask**, or **Block**.
 - 13 Click **OK**.

You can also change the action for the application from the Network Activity dialog box.

To change an application's action from the Network Activity dialog box

- 1 In the client, in the sidebar, click **Status**.
- 2 Beside Network Threat Protection, click **Options > View Network Activity**.
- 3 In the Network Activity dialog box, in the Running Applications field, right-click the application or service, and then click **Allow**, **Ask**, or **Block**.
- 4 Click **Close**.

When you change the application's action, the application appears in the Applications list.

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 Click **OK**.

Removing the restrictions from an application

You can remove the application's restrictions. When you remove the restriction, the action that the client takes on the application is also erased. When the application or the service tries to connect to the network again, you may be asked again whether to allow or block the application.

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

To remove the restrictions from an application

- 1 In the client, in the sidebar, click **Status**.
- 2 Beside Network Threat Protection, click **Options > View Applications List**.
- 3 In the View Applications List 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 **OK**.

Enabling and disabling file and print sharing

To protect your computer, you can disable file and print sharing to prevent network-based attacks. You can enable the client to share files and printers on your local network and for others to access your files and printers.

If a firewall rule blocks this traffic, the rule takes priority over this setting.

To enable and disable 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 on the selected network, click **Browse files and printers on the network**.
- 5 To enable other users to browse files on your computer, click **Share my files and printers with others on the network**.
- 6 Click **OK**.

Symantec Network Access Control

- [Symantec Network Access Control basics](#)

Symantec Network Access Control basics

This chapter includes the following topics:

- [About Symantec Network Access Control](#)
- [Running a Host Integrity check](#)
- [Remediating your computer](#)
- [Viewing the Symantec Network Access logs](#)
- [About enforcement](#)
- [Configuring the client for 802.1x authentication](#)

About Symantec Network Access Control

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.

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.

This network access control process includes the following steps:

- The client continuously evaluates its compliance.
You turn on the client computer. The client runs a Host Integrity check that compares the computer's configuration with the Host Integrity Policy that was downloaded from the management server. The Host Integrity check evaluates your computer for compliance with the Host Integrity Policy for antivirus software, patches, hot fixes, and other security requirements. For example, the policy may check how recently its antivirus definitions have been updated, and which were the latest patches applied to the operating system.
- A Symantec Enforcer authenticates the client computer and either grants the computer network access or blocks and quarantines non-compliant computers. If the computer meets all the policy's requirements, the Host Integrity check passes. The Enforcer grants full network access to computers that pass the Host Integrity check.
If the computer does not meet the policy's requirements, the Host Integrity check fails. When a Host Integrity check fails, the client or a Symantec Enforcer blocks or quarantines your computer until you remediate your computer. Quarantined computers have limited or no access to the network.
See [“About enforcement”](#) on page 131.
Your administrator may have set up the policy so that a Host Integrity check passes even if a specific requirement fails.
The client may display a notification every time the Host Integrity check passes.
See [“Responding to Network Access Control notifications”](#) on page 25.
- The client remediates non-compliant computers.
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 129.
- The client proactively monitors compliance.
The client actively monitors the compliance state for all client computers. If at any time the computer's compliance status changes, so do the network access privileges of the computer.

You can view more information about the Host Integrity check results in the Security Log.

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 security policy”](#) on page 16.

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 Beside 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.

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 Symantec Network Access logs

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

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

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

You can export the log data from these logs.

To view Symantec Network Access Control logs

- 1 In the client, in the sidebar, click **Status**.
- 2 To view the System Log, beside Network Access Control, click **Options > View Logs**.
- 3 To view the Security Log, in the Client Management Logs - System log dialog box, click **View > Security Log**.
- 4 Click **File > Close**.

See [“About logs”](#) on page 137.

About enforcement

The client interacts with a Symantec Enforcer. The Enforcer ensures that all the computers that connect to the network 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 Symantec Network Access Control client runs.
- The client has a unique identifier (UID).
- The client been updated with the latest Host Integrity Policy.
- The client computer passed the Host Integrity check.

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. You 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 802.11 network switch.
- The network switch relays the information to the LAN Enforcer. The LAN Enforcer sends the user information to the authentication server for authentication. The RADIUS server is the authentication server.
- If the client fails the user-level authentication or is not in compliance with the Host Integrity Policy, the Enforcer may block network access. The Enforcer places the non-compliant client computer in a quarantine network where the computer can be remediated.
- After the client remediates the computer and brings it into compliance, the 802.1x protocol reauthenticates the computer and grants the computer access to the network.

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

Table 9-1 describes the types of options you can configure for 802.1x authentication.

Table 9-1 802.1x authentication options

Option	Description
Third-party supplicant	<p>Uses a third-party 802.1x supplicant.</p> <p>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.</p> <p>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.</p>
Transparent mode	<p>Uses the client to run as an 802.1x supplicant.</p> <p>You use this method if the administrator does not wish to use a RADIUS server to perform user authentication. The LAN Enforcer runs in transparent mode and acts as a pseudo-RADIUS server.</p> <p>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.</p> <p>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.</p>
Built-in supplicant	<p>Uses the client computer's built-in 802.1x supplicant.</p> <p>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.</p>

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 > 802.1x**.
- 3 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 rules”](#) 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 > 802.1x**.
- 3 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 > Local Area Connection**.
- 2 In the Local Area Connection Status dialog box, on the General tab, click **Properties**.
- 3 In the Local Area Connection Properties dialog box, click **Authentication**.

- 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 Transparent Mode
- 5 Click **OK**.
- 6 Click **Close**.

Reauthenticating your computer

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

The network 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**.

Monitoring and logging

- [Using and managing logs](#)

Using and managing logs

This chapter includes the following topics:

- [About logs](#)
- [Viewing the logs and the log details](#)
- [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 records of security-related activities on your computer, which includes virus and security risk activities, configuration changes, and errors. They also include information about virus and security risk definitions file information, computer status, and the traffic that enters or exits your computer. These records are called events or entries. The logs display these events with any relevant additional information. 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. The Network 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.

If you have Symantec Endpoint Protection installed, the following log views are available:

- Scan Log, from Antivirus and Antispyware Protection
- Risk Log, from Antivirus and Antispyware Protection
- System Log, from Antivirus and Antispyware Protection
- Threat Log, from Proactive Threat Protection
- System Log, from Proactive Threat Protection
- Tamper Protection Log, from Tamper Protection
- Traffic Log, from Network Threat Protection
- Packet Log, from Network Threat Protection
- Security Log, from Client Management and Network Threat Protection
- Control Log, from Client Management
- System Log, from Client Management

If you have Symantec Network Access Control installed, the following logs are available:

- Security Log
- System Log

The logs can tell you when your computer has been blocked from the network and help you to determine why your access has been blocked.

For more information about a log, you can press F1 to view the help for that log. [Table 10-1](#) describes each log and what you can do with it.

Table 10-1 Client logs and description

Log	Description
Scan Log	<p>The Scan Log contains entries about the scans that have run on your computer over time. You can perform the following tasks in the Scan Log:</p> <ul style="list-style-type: none">■ View a list of the scans that have occurred on your computer over time. Scans are displayed with additional relevant information about the scans.■ Export the data in the log to a comma-delimited text file, for use in other applications.■ Right-click an entry and view its properties.

Table 10-1 Client logs and description (*continued*)

Log	Description
Risk Log	<p>The Risk Log contains entries about viruses and security risks, such as adware and spyware, that have infected your computer. Security risks include a link to the Symantec Security Response Web page that provides additional information.</p> <p>You can perform the following tasks in the Risk Log:</p> <ul style="list-style-type: none"> ■ View a list of the virus- and security risk-related events. ■ Export the data in the log to a comma-delimited text file, for use in other applications. ■ Clean a risk from your computer. ■ Delete a risk permanently from your computer. ■ Undo the changes that Symantec Endpoint Protection made when it deleted a risk or repaired its side effects. ■ Quarantine the risks that have been detected on your computer. ■ Right-click an entry and view its properties.
Antivirus and Antispyware Protection System Log	<p>The Antivirus and Antispyware Protection System Log contains information about system activities on your computer that are related to viruses and security risks. This information includes configuration changes, errors, and definitions file information.</p> <p>You can perform the following tasks in the Antivirus and Antispyware Protection System Log:</p> <ul style="list-style-type: none"> ■ View a list of the antivirus- and antispyware-related events. ■ Export the data in the log to a comma-delimited text file, for use in other applications. ■ Filter the information in the log to view only one or a few types of events. ■ Right-click an entry and view its properties.
Threat Log	<p>The Threat Log contains information about the threats that Proactive Threat Protection has detected on your computer. These include the commercial applications that can be used for malicious purposes. Examples are Trojan horses, worms, or keyloggers, or mass-mailing worms, macro viruses, and script-based threats.</p> <p>You can perform the following tasks in the Threat Log:</p> <ul style="list-style-type: none"> ■ View the list of the Proactive Threat Protection threat-related events. ■ Export the data in the log to a comma-delimited text file, for use in other applications. ■ Terminate the malicious programs or the malicious processes that have been found on your computer. ■ Restore items from the Quarantine. ■ Put the threats that have been detected on your computer into the Quarantine. ■ Right-click an entry and view its properties. <p>Note: The action buttons that are active depend on the actions that are appropriate for the selected log entry.</p>

Table 10-1 Client logs and description (*continued*)

Log	Description
Proactive Threat Protection System Log	<p>The Proactive Threat Protection System Log contains information about system activities on your computer that are related to Proactive Threat Protection.</p> <p>You can perform the following tasks in the Proactive Threat Protection System Log:</p> <ul style="list-style-type: none"> ■ View the system events related to Proactive Threat Protection. ■ Export the data to a comma-delimited text file, for use in other applications. ■ Filter the information in the log to view only one or a few types of events. ■ Right-click an entry and view its properties.
Tamper Protection Log	<p>The Tamper Protection Log contains entries about the attempts to tamper with the Symantec applications on your computer. These entries contain information about the attempts that Tamper Protection detected or detected and thwarted.</p> <p>You can perform the following tasks in the Tamper Protection Log:</p> <ul style="list-style-type: none"> ■ View the list of the Tamper Protection-related events. ■ Export the data in the log to a comma-delimited text file, for use in other applications. ■ Right-click an entry and view its properties.
Traffic Log	<p>The Traffic Log contains information about the connections that your computer makes through the network.</p> <p>You can perform the following tasks in the Traffic Log:</p> <ul style="list-style-type: none"> ■ View a list of the incoming traffic events and the outgoing traffic events whenever your computer is connected to a network. ■ From the File menu, clear all the entries from the log. ■ From the File menu, export the data in the log to a tab-delimited text file, for use in other applications. ■ From the File menu, access the Network Threat Protection settings and change the settings that are available to you. ■ From the View menu, switch between a local view and a source view. ■ From the Filter menu, filter the entries by selecting a time range. ■ From the Action menu, back trace the data packets that were used in attempted attacks to locate their origin. Note that not every entry can be back traced. <p>Note: Actions that are inappropriate for a particular entry or that your administrator does not allow are unavailable.</p>

Table 10-1 Client logs and description (*continued*)

Log	Description
Packet Log	<p>The Packet Log contains information about the packets of data that enter or leave through the ports on your computer.</p> <p>You can perform the following tasks in the Packet Log:</p> <ul style="list-style-type: none">■ View a list of the incoming traffic events and the outgoing traffic events whenever your computer is connected to a network.■ From the File menu, clear all the entries from the log.■ From the File menu, export the data to a tab-delimited text file, network monitor format, or Netxray format, for use in other applications.■ From the File menu, access the Network Threat Protection settings and change the settings that are available to you.■ From the View menu, switch between a local view and a source view.■ From the Filter menu, filter the entries by selecting a time range.■ From the Action menu, back trace the data packets that were used in attempted attacks to locate their origin. Note that not every entry can be back traced.
Control Log	<p>The Control Log contains information about the registry keys, files, and DLLs that an application accesses, as well as the applications that your computer runs.</p> <p>You can perform the following tasks in the Control Log:</p> <ul style="list-style-type: none">■ View a list of the control events.■ From the File menu, clear all the entries from the log.■ From the File menu, export the data in the log to a tab-delimited text file, for use in other applications.■ From the View menu, switch between a local view and a source view.■ From the Filter menu, filter the entries by selecting a time range.
Security Log	<p>The Security Log contains information about the activities that were directed toward your computer that can potentially pose a threat. Activities such as denial-of-service attacks, port scans, and executable file alterations are examples.</p> <p>You can perform the following tasks in the Security Log:</p> <ul style="list-style-type: none">■ View security-related events.■ From the File menu, clear all the entries from the log.■ From the File menu, export the data in the log to a tab-delimited text file, for use in other applications.■ From the View menu, switch between a local view and a source view.■ From the Filter menu, filter the entries, either based on a time range or based on severity.■ From the Action menu, back trace the data packets that were used in attempted attacks to locate their origin. Note that not every entry can be back traced.■ Stop the client from blocking the attacks that other computers make.

Table 10-1 Client logs and description (continued)

Log	Description
System Log	<p>The System Log contains information about all of the operational changes that have occurred on your computer. Examples include activities such as when a service starts or stops, the computer detects network applications, or software is configured.</p> <p>You can perform the following tasks in the System Log:</p> <ul style="list-style-type: none">■ View a list of the system events whenever your computer is connected to a network.■ From the File menu, clear all the entries from the log.■ From the File menu, export the data in the log to a tab-delimited text file, for use in other applications.■ From the Filter menu, filter the entries, either based on a time range or based on severity.

Note: If you are logged on to a managed client, some options in some of the logs may be unavailable. The availability of these options depends on what your administrator allows. This note applies to the Network Threat Protection and the Client Management Traffic, Packet, Control, Security, and System logs.

Options that are inappropriate for a particular entry in any log may be unavailable.

Viewing the logs and the log details

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

To view a log

- 1 In the client, in the sidebar, click **View logs**.
- 2 Beside the type of log that you want to view, click **View Logs** and then click the name of the log.

From a view of any of the Network Threat Protection logs and the Client Management logs, you can switch to a view of the other logs. Use the View menu at the top of the dialog box to access the other logs.

- 3 If you have opened a view for one of the Network Threat Protection or Client Management logs, click either **Local View** or **Source View**.

The columns in the log change depending on whether you choose the local view or source view. The local view shows the content from the perspective of the local port and the remote port. This perspective is more commonly used in a host-based firewall. The source view displays the content from the perspective of the source port and the destination port. This perspective is more commonly used in a network-based firewall.

If entries in the Network Threat Protection logs and the Client Management logs have more information available, it appears in the following locations:

- Description information appears in the lower left-hand pane of the log view.
- Data information appears in the lower right-hand pane of the log view.

You can also view the details of any entry in the Antivirus and Antispyware Protection, Tamper Protection, and Proactive Threat Protection logs. For the Risk Log, the details provide some additional information that is not available in the main log view window.

To view log entry details in the Antivirus and Antispyware Protection, the Tamper Protection, and the Proactive Threat Protection logs

- 1 In the client, in the sidebar, click **View logs**.
- 2 Beside Antivirus and Antispyware Protection, Tamper Protection, or Proactive Threat Protection, click **View Logs**.
- 3 Click the name of the log that you want to view.
- 4 Right-click an entry in the list and then select **Properties**.

Filtering the log views

You can filter the view of some of the logs in different ways. You can filter the events in Network Threat Protection and Client Management logs by the time period during which they occurred. You can filter events in some of the Network Threat Protection logs by their severity level. You can filter the events in the

Antivirus and Antispyware Protection System Log and the Proactive Threat Protection System Log by event type.

Filtering entries by time period

You can filter some logs by the time period during which the events occurred.

To filter log entries by time period

- 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 view.
- 4 In the log view window, click **Filter**, and then select the time period for which you want to view the log's events.

For example, if you select 2 Week Logs, the log viewer displays the events that were recorded over the past 14 days.

Filtering the entries by severity level

You can filter the information in the Network Threat Protection Security Log and the Client Management Security Log and System Log views by severity level. By default, events of all severity levels are displayed.

To filter log entries by severity level

- 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 Security Log or the System Log.
- 3 In the log view window, click **Filter**, and then click **Severity**.
- 4 Select one of the following to uncheck:
 - Critical (Security Log only)
 - Major (Security Log only)
 - Minor (Security Log only)
 - Error (System Log only)
 - Warning (System Log only)
 - Information

Unchecking an item eliminates events of that severity level from the view.

- 5 You can click **Severity** and select another level to eliminate additional severity levels from the view.

Filtering the System Logs by event category

In the Antivirus and Antispyware Protection System Log and the Proactive Threat Protection System Log, events are categorized as follows:

- Configuration change
- Symantec AntiVirus startup/shutdown
- Virus definition file
- Scan omissions
- Forward to Quarantine Server
- Deliver to Symantec Security Response
- Auto-Protect load/unload
- Client management and roaming
- Log Forwarding
- Unauthorized communication (access denied) warnings
- Login and certificate management
- Client Compliance
- Proactive Threat Scan load error
- Proactive Threat Scan commercial applications load error
- Proactive Threat Scan operating system not supported

You can reduce the number of events that appear in the two System Logs by displaying only certain types of events. For example, if you wanted to view only the events that are related to Auto-Protect, you could select only the Auto-Protect load/unload type. If you select one type, it does not stop the recording of events in the other categories. It only keeps the other categories from appearing when you display the System Log.

Note: Only relevant events are available for exclusion from the view.

To filter the System Logs by event category

- 1 In the client, in the sidebar, click **View logs**.
- 2 Beside AntiVirus and AntiSpyware Protection or Proactive Threat Protection, click **View Logs**.
- 3 Click **System Log**.
- 4 Click **Filter**.
- 5 Check or uncheck one or more categories of events.
- 6 Click **OK**.

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 and the Proactive Threat Protection log entries

To set the amount of time to retain 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 or Client Management, 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 84.

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

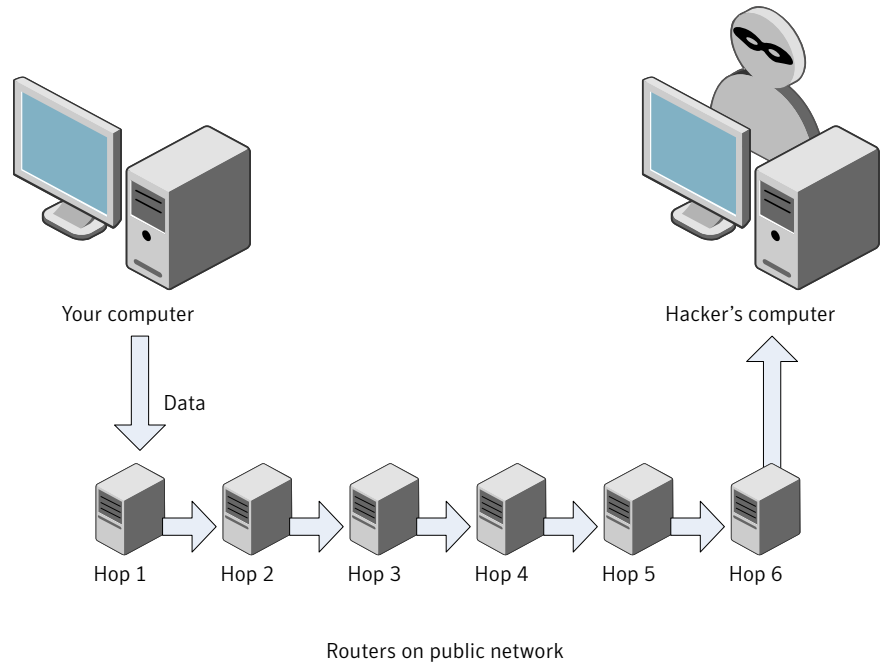
Any intrusion that is detected on the client triggers an active response. This active response automatically blocks the IP address of a known intruder for a specific amount of time. If your administrator allows, you can stop the active response immediately from the Security Log.

See [“Blocking an attacking computer”](#) on page 121.

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.

[Figure 10-1](#) displays how the client finds the source of data from a logged event.

Figure 10-1 Back tracing a packet

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 security policy”](#) on page 16.
- Check Host Integrity
See [“Running a Host Integrity check”](#) on page 129.

Exporting log data

You can export the information in some logs into a file with a comma-separated value (.csv) or an Access Database (*.mdb) format. 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 a tab-delimited text files.

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.

See [“Filtering the log views”](#) on page 143.

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.

To export data to a .csv file

- 1 In the client, in the sidebar, click **View logs**.
- 2 Beside either AntiVirus and AntiSpyware Protection, Proactive Threat Protection, or Tamper 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 is displayed. Click **Export**.
- 5 In the Save As dialog box, type a name for the file.
- 6 Browse to the directory where you want the file to be saved.
- 7 Click **Save**.

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 As dialog box, type a name for the file.
- 6 Browse to the directory where you want the file to be saved.
Click **Save**.

Index

Symbols

- 64-bit computers 65
- 802.1x authentication
 - about 131
 - configuring 133
 - reauthenticating 12

A

- actions
 - assigning second actions for viruses 78
 - tips for assigning second actions for security risks 78
- active response
 - about 121
- adapters
 - defined 110
- adware 40
- allow traffic 112, 122
- anti-MAC spoofing
 - enabling 115
- Antivirus and Antispyware Protection
 - about 36, 51
 - enabling and disabling 44
 - status 44
- Antivirus and Antispyware Protection System Log 139
- applications
 - allowing or blocking 122
 - defined 109
- attacks
 - blocking 101
 - network 104
 - signatures 104
- Auto-Protect
 - determining file types 59
 - disabling security risk scanning 60
 - disabling temporarily 44
 - enabling and disabling for email 45
 - enabling and disabling for the file system 45
 - encrypted email connections 58
 - for Internet email 56

Auto-Protect *(continued)*

- for Lotus Notes 56
- for Microsoft Exchange clients 56
- groupware email clients 56
- network cache 61
- network scanning options 61
- scanning by extension 52
- security risks 56
- status 44
- trusting remote versions 61
- using 55
- viewing scan statistics 58
- viewing the risk list 59

B

- Backup Items folder
 - clearing 88
- blended threats 40
- block an attacking computer 121
- block traffic 112, 118, 122
- bots 40
- broadcast traffic
 - showing 106

C

- centralized exceptions
 - excluding items from scans 54
 - for antivirus and antispyware scans 82
 - for proactive threat scan detections 100
- client
 - about 11
 - disabling 12
 - interacting with 19
 - opening 12
- commands
 - notification area icon 12
- Control Log 141

D

defined

scans 104

definitions file 14, 64

detection rates

sending information to Symantec 74

dialers 40

driver-level protection

enabling 115

E

email

encrypted connections 58

excluding Inbox file from scans 52

releasing attachments from Quarantine 87

email scanning. *See* Auto-Protect

enforcement

about 131

exclusions

creating for scans 54

extensions

excluding from scans 82

including in scans 52

F

files

backup of 88

excluding from scans 82

locating repaired 87

releasing files from Quarantine 87

rescanning files automatically in the

Quarantine 87

rescanning files manually in the Quarantine 87

scanning 52

submitting to Symantec Security Response 89

firewall

about 102

settings 107, 115

firewall rules

about 108

changing the order of 113

creating 112

deleting 115

editing 115

enabling and disabling 114

exporting 114

importing 114

logging 109

firewall rules *(continued)*

order processed 111

scheduling 109

folders

excluding from scans 82

H

hacking tools 40

host

defined 110

Host Integrity check

running 129

I

infected file

acting on 20

Internet bots 40

intrusion prevention

about 104

configuring 119

enabling 120

notifications for 120

respond to 24

IPS signatures

about 104

J

joke programs 40

L

LiveUpdate

how it works 15

locations

about 29

changing 30

logs

about 137

back tracing entries 150

Client Management 149

configuring how long entries are kept 146–147

configuring the size of 146

deleting 147

description 138

enabling the Packet Log 150

export formats 152–153

exporting data 152

exporting filtered log entries 153

filtering 143

logs (*continued*)

- filtering by event category 145
- filtering by severity level 144
- filtering by time period 144
- limiting the size of 146
- network access control 130
- Network Threat Protection 149
- quarantining risks and threats from 148
- refreshing 150
- Symantec Endpoint Protection 138
- Symantec Network Access Control 138
- viewing 142
- viewing entry properties 143

M

- macro virus infections
 - preventing 54
- managed clients
 - updating 15
 - vs. stand-alone clients 35
- managed environments
 - about 12
- manual scans. *See* on-demand scans
- messages
 - intrusion prevention 120
 - responding to 22

N

- NetBIOS protection
 - enabling 115
- Network Access Control
 - notifications 25
- network access control
 - about 127–128
 - enforcement 131
 - remediating the computer 129
- network activity
 - displaying 105
- network cache
 - Auto-Protect settings 61
- network scanning
 - Auto-Protect settings 61
- Network Threat Protection
 - about 37, 101
 - enabling and disabling 45
- notification area icon
 - about 12
 - hiding and displaying 13

notifications

- about 19
- intrusion prevention 120
- network access control 25
- responding to 22
- user interaction with 73

O

- on-demand scans
 - creating 69
 - initiating 65
 - scanning by extension 52
- online Help
 - accessing 17
- options
 - unavailable 36
- OS fingerprint masquerading
 - enabling 115
- Other risk category 40

P

- Packet Log 141
 - enabling 150
- policies
 - about 16
 - updating 12, 16
- port scans
 - port 104
- ports
 - about 101
- print sharing 124
- Proactive Threat Protection
 - about 37, 91
 - enabling or disabling 46
- proactive threat protection
 - managing 95
- Proactive Threat Protection System Log 140
- proactive threat scan
 - about 92
 - actions 97
 - centralized exceptions for 100
 - commercial applications 98
 - detections 93
 - false positives 94
 - frequency 95
 - notifications for 98
 - sensitivity level 97
 - submitting information about 99

proactive threat scan *(continued)*
 types of processes to detect 96

protection
 enabling and disabling types of 43
 types 11
 updating 14–15

protocol
 defined 110

Q

Quarantine 84
 deleting files 86, 88
 deleting files manually 88
 handling files infected by security risks 86
 handling infected files 85
 managing 86
 moving files to 85
 releasing files 87
 removing backup files 88
 rescanning files automatically 87
 rescanning files manually 87
 submitting files to Symantec Security
 Response 89
 viewing file details 86
 viewing infected files 85

R

reauthentication 134
 remote access programs 41
 risk impact ratings 79
 Risk Log 139
 rootkits 39

S

Scan Log 138
 scan types
 manual 65
 scans. *See* antivirus and antispyware
 all file types 53
 centralized exceptions for 82
 compressed files 65
 delaying 48
 excluding files from 54
 files 52
 interpreting results 72
 pausing 48
 scanning files by extension 52
 scheduled 66

scans *(continued)*
 snooze options 49

scheduled scans
 creating 66
 editing and deleting 71
 multiple 69
 scanning by extension 52

Security Log 141

security risk scanning
 disabling in Auto-Protect 60

security risks 39
 configuring actions for 75
 configuring notifications for 80
 detection options 80
 excluding from scans 82
 how the client detects 63
 how the client responds 42
 process continues to download 56
 remediation options 80
 tips for assigning second actions 78
 what to do when detected 55

settings
 firewall 107
 intrusion prevention 120

share files and folders 124

signatures 14

Smart DHCP 117

Smart DNS 117

Smart traffic filtering
 defined 117

Smart WINS 117

spyware 41

stand-alone clients
 vs. managed clients 35

startup scans
 creating 69
 editing and deleting 71
 scanning by extension 52

stateful inspection
 about 110
 creating rules for traffic 110

stealth mode Web browsing
 enabling 115

Symantec Security Response
 about 15
 accessing 17
 submitting files to 89
 Web site 16–17

System Log 142
 deleting entries 147

T

Tamper Protection
 about 30
 configuring 31
 enabling and disabling 31
Tamper Protection Log 140
TCP resequencing
 enabling 115
testing your computer 29
Threat Log 139
threats
 blended 40
token ring traffic
 enabling 115
Trackware 41
traffic
 allowing or blocking 122
 blocking 118
 displaying 105
Traffic Log 140
Trojan horses 40

U

UDP connections
 about 111
unblock an attacking computer 121
unmanaged clients
 updating 15
unmanaged environments
 about 12
user-defined scans
 editing and deleting 71

V

viruses 39–40
 assigning second actions 78
 configuring actions for 75
 configuring notifications for 80
 detection options 80
 file damage from 21
 how the client detects 63
 how the client responds 42
 remediation options 80
 unrecognized 89
 what to do when detected 55

W

Windows Security Center
 seeing antivirus status from 47
 seeing firewall status from 47
Windows services
 showing 106
worms 40

Z

zero-day protection 91