Symantec™ Endpoint Protection 14.x for Mac Client Guide

Symantec Endpoint Protection for Mac Client Guide

Product version 14.2.1 (14.2 RU1)

Documentation version: 1

This document was last updated on: April 23, 2019

Legal Notice

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

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. 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
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Symantec Support

Knowledge Base articles and Symantec Connect

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

https://support.symantec.com/

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

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

Technical Support and Enterprise Customer Support

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

Before you contact Symantec Support, see:

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

To contact Symantec Support, see:

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

Contents

Chapter 1

Getting started with the Mac client

This chapter includes the following topics:

How Symantec Endpoint Protection protects your Mac

Symantec Endpoint Protection combines several layers of protection to secure your computer against virus and spyware attacks as well as intrusion attempts.

Table 1-1 describes each layer of protection.

Table 1-1 Types of protection

Protection	Description
Virus and Spyware Protection	Symantec Endpoint Protection includes scheduled virus scans, on-demand scans, and Auto-Protect, which runs in the background, monitoring for viruses. When a virus is found, Symantec Endpoint Protection eliminates it. See "How Virus and Spyware Protection protects your Mac" on page 9.
Network Threat Protection	Symantec Endpoint Protection intercepts the data at the network layer. It uses signatures to scan packets or streams of packets. It scans each packet individually by looking for the patterns that correspond to network attacks or browser attacks. Network Threat Protection includes the following: ▪ Intrusion prevention, which detects attacks on operating system components and the application layer. When Symantec Endpoint Protection detects a network threat, it blocks the threat. ▪ Firewall, which allows or blocks network traffic based on firewall policies and rules. (As of version 14.2.) See "How Network Threat Protection protects your Mac" on page 10.
Device Control	Symantec Endpoint Protection Manager administrators configure a device control policy. Devices can be blocked or unblocked with this policy by device name, device vendor, device model, or serial number. On a managed client, you can see the settings for Device Control on the **Settings** tab. Device control is not available for unmanaged clients. See "About device control on the Symantec Endpoint Protection client for Mac" on page 12.

The client automatically downloads the virus definitions, IPS definitions, and the product updates to your computer.

See “Updating virus definitions, intrusion prevention definitions, and the client software” on page 18.

Getting started on the Status page

When you open Symantec Endpoint Protection, the **Status** page appears.

The message **Your Computer is protected** appears at the top of the page, unless there is a problem that needs to be resolved. Click **Fix** to resolve any issues.

Table 1-2 displays the main tasks that you can perform from the **Status** page.

Table 1-2 **Status** page options

Option	Description
Settings	Gives more detailed options for Virus and Spyware Protection, Network Threat Protection, and LiveUpdate.
View log history	Shows the **History** pages for the various types of logs on the client.
LiveUpdate Now	Runs LiveUpdate to update the definitions and product files for Symantec Endpoint Protection. See “Updating the content on Symantec Endpoint Protection immediately” on page 19.
Scan	Runs a scan of your computer immediately. You can choose to run a custom scan or run a full scan. See “Running a manual scan” on page 27.

How Virus and Spyware Protection protects your Mac

Symantec Endpoint Protection uses virus definitions to detect known viruses during scheduled scans and manual scans. Auto-Protect uses virus definitions to constantly scan your computer activity.

Symantec Endpoint Protection notifies you that if it has detected a virus or other security risk. A virus or other security risk is detected when one of the following occurs:

- Auto-Protect finds a virus while it monitors your computer.
- Auto-Protect finds a virus from a scan that you scheduled or started manually.

With default settings, Symantec Endpoint Protection automatically attempts to repair any virus it finds. If it can’t repair the file, the client safely quarantines the file so that it cannot harm your computer. Usually, the client performs these repairs without any action by you. When your computer finds a virus, you can choose to submit information about it to Symantec.

In certain circumstances, the client prompts you to choose whether you want to repair, delete, or restore an infected file that it has found. Your responses determine what the client does with the infected file.

See “Responding to messages about infections and risk detections” on page 29.

See “Turning on or turning off the submission of security information to Symantec” on page 30.

How Network Threat Protection protects your Mac

Network Threat Protection includes the following protection technologies:

- Intrusion prevention
- Firewall

Intrusion prevention

Intrusion prevention automatically detects and blocks network attacks. Intrusion prevention is an inner layer of defense to protect client computers. Intrusion prevention is sometimes called the intrusion prevention system (IPS).

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

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

Firewall

The firewall monitors network traffic and blocks potentially harmful traffic to protect your Mac. The Symantec Endpoint Protection firewall is not available on the unmanaged client.

The Symantec Endpoint Protection firewall monitors traffic at the Transport and Internet layer. The built-in Mac firewall monitors traffic at the higher Application layer, after the Symantec Endpoint Protection firewall monitors it. Therefore, you can enable both firewalls at once to run in parallel.

The firewall uses the following types of rules to allow or block network traffic:

- Default rules
- Custom rules
- Built-in rules
- Protection rules

These rules include portscan detection, denial of service detection, anti-MAC spoofing, smart DHCP, and smart DNS. Firewall settings are controlled entirely by the Symantec Endpoint Protection Manager administrator. You can enable or disable the firewall only if the administrator allows the user client control over the Mac.

Firewall protection was added in version 14.2.

See “Managing intrusion prevention” on page 32.

See “Managing firewall protection for the Mac client” on page 33.

Managing your Mac's protection with Symantec Endpoint Protection

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

Depending on the settings that your administrator sets, you should perform the following tasks to help maintain your protection.

Note: Your administrator may not have given you control over these tasks.

Table 1-3 Protecting your computer

Steps	Task	Description
Step 1	Check that Virus and Spyware Protection and that Network Threat Protection are both enabled.	The **Status** page appears, and shows a green checkmark and the message, **Your Computer is protected**, if your protections are turned on. See “Turning on and turning off Virus and Spyware Protection” on page 23. See “Turning on or turning off Network Threat Protection” on page 33.
Step 2	Make sure that the software and definitions are up to date	The **Status** page displays the last date that definitions were updated for Virus and Spyware Protection and Network Threat Protection. Under **LiveUpdate**, the date of the last product update appears. To see the version number of the software, on the menu bar, click **Symantec Endpoint Protection > About Symantec Endpoint Protection**.

Table 1-3 Protecting your computer *(continued)*

Steps	Task	Description
Step 3	Update the software or definitions if necessary	On the **Status** page, click **LiveUpdate Now** to update software and definitions immediately. See "Updating virus definitions, intrusion prevention definitions, and the client software" on page 18.
Step 4	Run a scan	You can schedule scans to run at regular intervals, or you can run a scan immediately. See "Setting up scheduled scans" on page 26. See "Running a manual scan" on page 27.

See "Managing your Virus and Spyware Protection settings" on page 22.

About updating your product license

You may see a message under the Symantec Endpoint Protection client icon on the menu bar that the license for Symantec Endpoint Protection is expired. The Symantec Endpoint Protection client uses a license to update the following:

- The client software
- The protection definition files for virus and spyware scans and intrusion prevention

The client may use a trial license or a paid license. If either license is expired, the client does not update any definitions or the client software.

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

See "Responding to messages about infections and risk detections" on page 29.

About device control on the Symantec Endpoint Protection client for Mac

Symantec Endpoint Protection Manager administrators can configure managed clients with a device control policy. Devices can be blocked or unblocked with this policy by device name, device vendor, device model, or serial number. You can view device control activity on the **Status** page by clicking **View Log History**.

Settings in the Symantec Endpoint Protection client interface for **Device Control** let you enable or disable device control. If device control is enabled, you can optionally enable or disable notifications when devices are blocked or unblocked.

To change the settings, you must authenticate with Mac administrator credentials. If these settings are grayed out, then the administrator has locked it to prevent you from enabling or disabling this feature.

You cannot add or edit devices to be blocked or unblocked through the Symantec Endpoint Protection client interface.

Note: The device control policy from Symantec Endpoint Protection Manager controls the device control settings. At the next heartbeat, any changes that you make to these settings revert to what the policy dictates.

Device control is not available for unmanaged clients.

Installing the Symantec Endpoint Protection client for Mac

You can directly install a Symantec Endpoint Protection client on a Mac computer if you cannot use or do not want to use Remote Push. The steps are similar whether the client is unmanaged or managed.

The only way to install a managed client is with a package that Symantec Endpoint Protection Manager creates. You can convert an unmanaged client to a managed client at any time by importing client-server communication settings into the Mac client.

Note: To prepare the Symantec Endpoint Protection client for Mac for use with third-party remote deployment software, see Exporting and Deploying a Symantec Endpoint Protection client via Apple Remote Desktop or Casper.

If you downloaded the installation file or received a product disc

1. Perform one of the following tasks:

   If you downloaded the installation file, extract the contents to a folder on a Mac computer, and then open the folder.

   If you received a disc, insert it into a computer.

2. Open `SEP_MAC`.
3. Copy `Symantec Endpoint Protection.dmg` to the desktop of the Mac computer.
4. Double-click `Symantec Endpoint Protection.dmg` to mount the file as a virtual disk. You then install the Symantec Endpoint Protection client for Mac.

If you have a client installation package .zip

1. If you exported the installation package or downloaded the client installer package from MySymantec, copy the file to the desktop of the Mac computer.

   The file may be named `Symantec Endpoint Protection.zip` or `Symantec_Endpoint_Protection_`*`version`*`_Mac_Client.zip`, where *version* is the product version.

2. Right-click **Open With > Archive Utility** to extract the file's contents.
3. Open the resulting folder. You then install the Symantec Endpoint Protection client for Mac.

Note: The resulting virtual disk image or folder contains the application installer and a folder called **Additional Resources**. Both items must be present in the same location for a successful installation. If you copy the installer to another location, you must also copy **Additional Resources**.

To install the Symantec Endpoint Protection client for Mac

1. Double-click **Symantec Endpoint Protection Installer**.
2. To acknowledge the required restart, click **Continue**.
3. To review the license agreement, click **View License Agreement**.

   To begin the installation, click **Agree & Install**.

4. Enter the user name and password for the Mac administrative account when prompted, and then click **Install Helper**.
5. To authorize the Symantec Endpoint Protection kernel extension for macOS 10.13, in the installer pane, click **System Preferences**, and then in the **Security & Privacy** system preference pane, click **Allow**. You do not need to enter a password.
6. In the installer pane, click **Close & Restart** to complete the installation.

   When you log back on to the Mac computer, LiveUpdate launches to update the definitions. LiveUpdate runs silently in the background and does not display its progress onscreen.

If you were prompted to authorize the kernel extension but did not do it in step 5, do so after the computer restarts. You must authorize the kernel extension for Symantec Endpoint Protection to fully function.

See “About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later” on page 15.

About authorizing kernel extensions for Symantec Endpoint Protection for macOS 10.13 or later

Requiring the authorization of kernel extensions (kexts) is a new security feature as of macOS 10.13. Symantec Endpoint Protection 14.0.1 adds support for macOS 10.13. You must authorize the kernel extension for Symantec Endpoint Protection to fully function.

During installation of the client, click **Allow** when you are prompted under **System Preferences** in the **Security & Privacy** system preference pane. You do not need to enter a password.

The option to allow the Symantec Endpoint Protection kernel extensions in the System Preferences disappears after 30 minutes. You can get the option back in the following ways:

- Restart the Mac. You can then open the **Security & Privacy** system preference.
- Open the Symantec Endpoint Protection client user interface on the Mac and click **Fix** next to the message **Kernel extensions need authorization**. This action opens the **Security & Privacy** system preference.

If you have previously authorized the Symantec Endpoint Protection kernel extension on the Mac computer, you do not need to authorize it again. For example, you do not have to authorize the kernel extension again if you uninstall and then reinstall the client. You also do not have to explicitly authorize if you upgrade Symantec Endpoint Protection to 14.0.1 and then upgrade the operating system to macOS 10.13.

However, you need to reauthorize the kernel extension if you reinstall the operating system. You must also reauthorize the kernel extension if you upgrade from a Symantec Endpoint Protection version earlier than 14.2 to version 14.2 or later.

See “Installing the Symantec Endpoint Protection client for Mac” on page 13.

Upgrade prompt for the Symantec Endpoint Protection client for Mac

Symantec Endpoint Protection Manager administrators can assign a client installation package to automatically upgrade the managed client computers, with settings for client installation.

If you are logged on to the Mac, you may see a prompt to restart to complete the installation. You may be able to delay the restart based on the client installation settings.

If you are not logged on to the Mac, the installation automatically restarts the Mac.

Operating system compatibility with Symantec Endpoint Protection for Mac

Symantec Endpoint Protection 14.2 RU1 supports Mac OS X 10.10, 10.11, and macOS 10.12, 10.13, and 10.14.

For additional information on support for earlier Mac operating system versions, see Mac compatibility with Endpoint Protection client.

Release notes, new fixes, and system requirements for all versions of Endpoint Protection

About WSS Traffic Redirection for the Mac client

Web Security Service (WSS) Traffic Redirection (WTR) automates web traffic redirection to Symantec Web Security Service and secures the web traffic on each computer that uses Symantec Endpoint Protection.

The administrator controls the settings that WSS Traffic Redirection uses, which includes the proxy configuration URL and the optional Symantec Web Security Service root certificate. Only the Symantec Endpoint Protection Manager administrator can configure these settings, which do not appear in the Symantec Endpoint Protection client UI. You can view the proxy configuration file URL on the Mac through **System Preferences > Network**, under **Proxies**. The Cloud Services certificate appears in **Keychain**.

The web browsers Safari, Chrome, and Firefox version 65 and later support WSS Traffic Redirection. Symantec Endpoint Protection versions earlier than 14.2 RU1 only support Safari and Chrome.

Uninstalling the Symantec Endpoint Protection client for Mac

You uninstall the Symantec Endpoint Protection client for Mac through the client icon on the menu bar. Uninstallation of the Symantec Endpoint Protection client for Mac requires administrative user credentials.

Note: After you uninstall the Symantec Endpoint Protection client, you are prompted to restart the client computer to complete the uninstallation. Make sure that you save any unfinished work or close all open applications before you begin.

To uninstall the Symantec Endpoint Protection client for Mac

1 On the Mac client computer, open the Symantec Endpoint Protection client, and then click **Symantec Endpoint Protection > Uninstall Symantec Endpoint Protection**.

2 Click **Uninstall** again to begin the uninstallation.

3 When you are prompted, authenticate with your Mac's administrative user name and password.

   You may also be prompted to type a password to uninstall the client. This password may be a different password than your Mac's administrative password.

4 Once the uninstallation completes, click **Restart Now**.

If the uninstallation fails, you may have to use an alternate method to uninstall. See:

Uninstall Symantec Endpoint Protection

Chapter 2

Updating content and the client software for Symantec Endpoint Protection

This chapter includes the following topics:

Updating virus definitions, intrusion prevention definitions, and the client software

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

Definition updates are the files that keep your Symantec products current with the latest threat protection technologies. LiveUpdate retrieves the new intrusion prevention signatures or virus definition files from a Symantec Internet site, and then replaces the old files.

Product updates are improvements to the installed client. Product updates are usually created to extend the operating system or hardware compatibility, adjust performance issues, or fix product errors. Product updates are released on an as-needed basis. The client receives product updates directly from a LiveUpdate server. Product updates and definitions updates together are called content updates.

Table 2-1 Ways to update content on your computer

Task	Description
Update the content on a schedule	By default, LiveUpdate runs automatically at scheduled intervals. See "Updating the content on Symantec Endpoint Protection on a schedule" on page 20.
Update the content immediately	You can run LiveUpdate immediately. See "Updating the content on Symantec Endpoint Protection immediately" on page 19.

See "Managing your Mac's protection with Symantec Endpoint Protection" on page 11.

Updating the content on Symantec Endpoint Protection immediately

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

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

To update content on Symantec Endpoint Protection immediately

1. Launch LiveUpdate in one of the following ways:
   - Click the Symantec Endpoint Protection icon in the menu bar, and then click **LiveUpdate > Run LiveUpdate**.
   - Open the client interface, and in the **Status** window, click **LiveUpdate Now**.

   LiveUpdate connects to the configured LiveUpdate server, checks for available updates, then downloads and installs them automatically. A status bar indicates the download progress.
2. Click **OK** to close the update window.

See "Updating the content on Symantec Endpoint Protection on a schedule" on page 20.

See “Updating virus definitions, intrusion prevention definitions, and the client software” on page 18.

Updating the content on Symantec Endpoint Protection on a schedule

Schedules on managed Mac clients

By default, managed Mac clients receive a schedule from Symantec Endpoint Protection Manager that runs LiveUpdate every four hours. The Symantec Endpoint Protection Manager administrator controls the schedule. Managed clients cannot remove, modify, or view the administrator-created schedule, or create a new schedule.

Schedules on unmanaged Mac clients

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

To update the content on Symantec Endpoint Protection on a schedule

1. In Symantec Endpoint Protection, in the sidebar, click **Settings** and then click the **LiveUpdate** tab.

   Your current schedule appears.

2. Select an interval from the LiveUpdate Schedule drop-down menu.

   The initial setting is to run every **4** hours. You can also choose to run **Daily** or **Weekly**, choosing a time or a day and time, respectively.

3. Click **Apply Changes**.

See “Updating the content on Symantec Endpoint Protection immediately” on page 19.

See “Updating virus definitions, intrusion prevention definitions, and the client software” on page 18.

About connecting to the management server through a proxy server

You might be asked to allow Symantec Endpoint Protection to use your credentials to connect to the management server through a proxy. You receive a message that asks whether you want to allow access to your credentials to the `symdaemon` process.

You must click **Always Allow** in the message. Otherwise, you continue to receive the same message every time the client communicates with the LiveUpdate server. If you click **Deny**, your client cannot receive updates to software or definitions.

See “Updating virus definitions, intrusion prevention definitions, and the client software” on page 18.

Chapter 3

Managing Virus and Spyware Protection

This chapter includes the following topics:

Managing your Virus and Spyware Protection settings

By default, Symantec Endpoint Protection protects against viruses and security risks, which includes network threats, as soon as your computer starts. Virus and Spyware Protection includes Auto-Protect, which checks programs for viruses as they run. It also monitors your computer for any activity that might indicate the presence of a virus or a security risk. Auto-Protect interception prevents viruses from infecting your computer, and you should keep Auto-Protect turned on.

For managed clients, the amount of control that you have over these settings depends on how the administrator configured the client. In addition, any changes that you make to these settings may revert to what the policy dictates at the next heartbeat.

Table 3-1 describes the tasks you can accomplish to manage Virus and Spyware Protection on your Mac.

Table 3-1 Managing Virus and Spyware Protection

Task	Description
Turn on or turn off Virus and Spyware Protection	You can easily enable and disable Virus and Spyware Protection. Symantec recommends that you leave it turned on. See "Turning on and turning off Virus and Spyware Protection" on page 23.
Customize your Auto-Protect settings	Auto-Protect is an important part of Virus and Spyware Protection. You can configure these options from the **Settings** page. See "Configuring Auto-Protect settings and Scan Zone settings" on page 24.
Scan your computer for viruses	You can set up virus scans to run on a schedule or to run immediately. See "Setting up scheduled scans" on page 26. See "Pausing, snoozing, and stopping scans" on page 28. See "Running a manual scan" on page 27.
Respond when Symantec Endpoint Protection detects a virus	When Symantec Endpoint Protection scans your computer, it may: ▪ Notify you of the actions that you can take. ▪ Inform you about the protective actions that it has taken for you. See "Responding to messages about infections and risk detections" on page 29.

Turning on and turning off Virus and Spyware Protection

By default, Virus and Spyware Protection is turned on, along with Auto-Protect.

You can exercise more precise control over Auto-Protect by setting specific options.

If Virus and Spyware Protection is turned off, a red "x" appears on the **Status** page, with the message **Virus and Spyware Protection is disabled**. If the protection has been disabled, you should enable it as soon as possible.

Note: Scheduled scans continue, regardless of whether Virus and Spyware Protection is enabled or disabled. Your administrator may restrict access to some Symantec Endpoint Protection settings. You may not be allowed to disable these settings, schedule scans, or customize protection options.

You may be required to provide your Mac administrator password to change any of these settings.

To turn on and turn off Virus and Spyware Protection

- Click the Symantec Endpoint Protection icon in the menu bar, and then click **Symantec Endpoint Protection > Enable Virus and Spyware Protection** to enable it. If it is enabled, click **Symantec Endpoint Protection > Disable Virus and Spyware Protection** to disable it.

See "Configuring Auto-Protect settings and Scan Zone settings" on page 24.

See "Managing your Virus and Spyware Protection settings" on page 22.

See "Responding to messages about infections and risk detections" on page 29.

Configuring Auto-Protect settings and Scan Zone settings

On managed clients, if your administrator lets you, you can customize how Auto-Protect monitors viruses and repairs infected files.

The Auto-Protect settings appear as options under **Virus and Spyware Protection**. You must enable **Virus and Spyware Protection** to enable Auto-Protect.

Scan Zone settings let you specify the files to include in a scan or to exclude from a scan.

To configure Auto-Protect settings

1. In Symantec Endpoint Protection, in the sidebar, click **Settings**.
2. On the **Virus and Spyware Protection** tab, under **Auto-Protect Settings**, click **Configure**.

3 In the **Auto-Protect Settings** dialog box, make changes to any of the following options:

Auto Quarantine	You can choose whether to send any files that cannot be repaired to the Quarantine.
Auto Repair	You can choose to have Auto-Protect automatically repair any infected files that it finds.
Scan	You can designate **All disks** or **Selected disks**. In **Selected disks**, you can choose **Data Disks** and **All other disks**.
Scan compressed files	You can choose whether to include compressed files in an Auto-Protect scan. The scan includes the compressed file and the files inside the compressed file.

Warning: If you do not choose **Auto Repair**, any infected files are not moved to the Quarantine, even if you choose **Auto Quarantine**.

The software asks whether you want to repair an infected file. If you do not repair the file, it is left on the computer. If you choose **Auto Repair**, and if you do not choose **Auto Quarantine**, any infected files are deleted.

4 Click **Done**.

To configure Scan Zone settings

1 In Symantec Endpoint Protection, in the sidebar, click **Settings**

2 On the **Virus and Spyware Protection** tab, under **Scan Zone Settings**, click **Configure**.

3 Make changes to any of the following options:

Scan Everywhere	All files and processes on your computer are scanned as you access them.
Scan Only	Only the files or folders that you specify are included in the scan.
Don't Scan	All files are scanned except for the files or folders that you specify to exclude from the scan.
Use Defaults	This choice scans everywhere.

4 Click **OK**.

See “How Virus and Spyware Protection protects your Mac” on page 9.

See “Turning on and turning off Virus and Spyware Protection” on page 23.

See “Managing quarantined files” on page 30.

Setting up scheduled scans

Symantec Endpoint Protection automatically runs a default scan if you have a managed client. If your administrator lets you do so, you can set up additional scheduled scans.

Note: On an unmanaged client, you must run your own scans. Symantec recommends that you perform a full manual scan as soon as possible, and then set up a regular scheduled scan. You can pause or delay any scan, including both scheduled scans and manual scans.

On a managed client, the default scan runs daily at 8:00 P.M., with Auto Repair enabled.

See “Running a manual scan” on page 27.

To set up scheduled scans

1 In Symantec Endpoint Protection, in the sidebar, click **Settings**

2 On the **Virus and Spyware Protection** tab, under **Scheduled Scans**, click **Configure**.

3 In the dialog box, click **Add scheduled scans**, or click a current scheduled scan and then click **Edit** to adjust the settings for it.

Make any changes to the scan settings on the **Scan Items** and **Scan Schedule** tabs:

On the **Scan Items** tab, you can set the following options:

Drives

You can choose whether to scan **Hard drives** and **Removable drives**.

Folders

You can choose to scan your **Home folder (Active user)**, **Applications**, and **Library** files.

Note: If no user is logged on at the time of the scheduled scan of a Home folder, then the scan does not run.

Scan Options

You can choose from the following options:

- **Scan Compressed**
- **Auto Repair**
- **Auto Quarantine**
- **Enable Idle Time Scan**

On the **Scan Schedule** tab, you can set the following options:

Scan Schedule

You can set up a scan to run at a specific interval in hours, daily, weekly, or monthly. **Run at a specific interval** is selected by default when you schedule a new scan.

Run every	Available when **Run at specific interval** is selected for **Scan Schedule**.
Start Time	Available when you select **Daily**, **Weekly**, or **Monthly** for the scan schedule. You can choose the time of day to run the scan. You should choose a time when you typically are not at work, because scans can slow the performance of your computer.
On	Available when you select **Weekly** or **Monthly** for the scan schedule. You can choose the day of the week or month to run the scan. We recommend that you choose a time when you typically are not at work because scans can slow the performance of your computer.

4 Click **OK**.

5 Click **Done**.

See "Pausing, snoozing, and stopping scans" on page 28.

See "Managing your Mac's protection with Symantec Endpoint Protection" on page 11.

See "Responding to messages about infections and risk detections" on page 29.

See "Turning on or turning off the submission of security information to Symantec" on page 30.

Running a manual scan

You might need to scan some files manually. For example, you might need to scan the files that were saved to your computer before Symantec Endpoint Protection was installed. Or you might decide that some files that were excluded from a scheduled scan should be scanned.

Note: You can pause or delay any scan, including both scheduled scans and manual scans.

To run a manual scan

1 In Symantec Endpoint Protection, in the sidebar, click **Status**.

2 On the **Status** page, click **Scan**, and then click **Run full scan** or **Run custom scan**.

- If you click **Run full scan**, the scan begins immediately.
- If you click **Run custom scan**, the Finder opens and you can choose whether to **Show Hidden Files** and **Scan Compressed Files**. You can also choose to turn on **Auto Repair** and **Auto Quarantine**.

3 Once you have made those choices, navigate to the folder, file, or disk to scan, select them, and then click **Scan**.

See “Pausing, snoozing, and stopping scans” on page 28.

See “Setting up scheduled scans” on page 26.

See “Turning on or turning off the submission of security information to Symantec” on page 30.

Pausing, snoozing, and stopping scans

The pause feature lets you stop a scan and resume it at another time that you choose. You can also stop and cancel any scan at any time. You do not need administrator privileges to use these features.

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

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

If snoozing is enabled, you can also snooze a scan, but only before the scan begins. You cannot snooze a scan in progress.

To pause or stop a running scheduled scan

1 In the scan progress dialog box, click **Pause**.

2 In the scan progress dialog box, click **Resume** to continue the scan, or click **Stop** to stop the scan. You can also click **Done** to close the window.

To pause or stop a running manual scan

1 In the scan progress dialog box, click **Pause** to pause the scan.

2 Click **Cancel** to stop a running manual scan or click **Resume** to continue the scan.

To snooze a scan that is about to start

1 In the window that appears, click the drop-down menu to select a value to snooze. You can snooze for as little as 15 minutes, or as long as a day.

2 Click **OK** to snooze the scan.

You do not need to do anything if you want the scan to run as scheduled.

See “Setting up scheduled scans” on page 26.

See “Running a manual scan” on page 27.

Responding to messages about infections and risk detections

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

Your administrator may manage your client or you may run an unmanaged client. The protection tasks that you can perform depend on how much control your administrator keeps over the client.

If Symantec Endpoint Protection finds a virus or a security risk, you may be asked to take action on the risk. Based on the settings that your administrator chooses, you may be informed about the action that the client took automatically.

Table 3-2 Responding to messages about infections

Message content	Action required
Repaired the infected file	None
Requests your approval to repair the infected file	Approve the repair. This option depends on your Auto-Protect preferences. See "Managing your Virus and Spyware Protection settings" on page 22. If the option to automatically repair infected files is unchecked, you must repair the file manually. See "Repairing infected files" on page 29.
Unable to repair infected file	Manage the infection in Quarantine. See "Managing quarantined files" on page 30.

See "How Virus and Spyware Protection protects your Mac" on page 9.

Repairing infected files

If an infected file is not automatically repaired or placed in the Quarantine, you can repair the file from the scan results list. You can manually repair files on your computer's hard disk or on removable media.

To repair infected files

1 In the scan results list, select the file to repair, then click **Repair**.

  You can also right-click any file from the Mac **Finder** or **Search** menu.

2 Repeat as necessary.

3 Run another scan to check for other infected files.

4 Check the repaired files to make sure that they function correctly.

See "Managing your Virus and Spyware Protection settings" on page 22.

See "Managing quarantined files" on page 30.

Managing quarantined files

By default, if the client detects a virus in a file, it tries to remove the virus. If the virus cannot be removed, the file is placed in the Quarantine on your computer. If Symantec Endpoint Protection detects a security risk in a file, it places the file in the Quarantine first. It then repairs any side effects of the risk.

When you update your virus definitions, the client automatically checks the Quarantine. You can rescan the items in the Quarantine. The latest definitions may be able to clean or repair the files that are quarantined.

To manage quarantined files

1 In Symantec Endpoint Protection, click **Tools > Quarantine**.

2 Select the file to manage, then choose the appropriate option:

Repair	Choose this option to try to repair a quarantined file. **Note:** Make sure that your virus definitions are more recent than the date that the file was quarantined.
Delete	Choose this option to delete any files that you no longer need from the Quarantine.
Restore	If you are sure that the file does not contain a virus, you can restore it to its original location on your computer. This option does not scan the file or try to repair it.

See "Responding to messages about infections and risk detections" on page 29.

Turning on or turning off the submission of security information to Symantec

Symantec Endpoint Protection can submit pseudonymized information about detected threats to Symantec. Symantec uses this information to protect your client computers from new, targeted, and mutating threats. Any data you submit improves Symantec's ability to respond to threats and customize protection for your computer.

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

By default, your client computer sends information about detections to Symantec. You can turn off submissions, although Symantec recommends that you leave this setting turned on.

This option only sends information about virus detections.

Note: Symantec recommends that you leave the option turned on.

To turn on or turn off the submission of pseudonymous security information to Symantec

1. In Symantec Endpoint Protection, in the sidebar, click **Settings**.
2. On the **Virus and Spyware** tab, turn on or turn off **Let this computer automatically forward selected pseudonymous security information to Symantec**.

See “Setting up scheduled scans” on page 26.

See “Running a manual scan” on page 27.

Chapter 4

Managing Network Threat Protection

This chapter includes the following topics:

- Managing intrusion prevention
- Managing firewall protection for the Mac client
- Turning on or turning off Network Threat Protection

Managing intrusion prevention

The default settings for intrusion prevention protect your Mac client. However, if you want to manage your own protection, you can manage intrusion prevention as part of Network Threat Protection.

Table 4-1 Managing intrusion prevention

Action	Description
Learn about intrusion prevention	Learn how intrusion prevention detects and blocks network attacks. See "How Network Threat Protection protects your Mac" on page 10.
Download the latest IPS signatures	By default, the latest signatures are downloaded to the client. However, you might want to download the signatures immediately. See "Updating the content on Symantec Endpoint Protection immediately" on page 19.
Enable or disable intrusion prevention	You might need to disable intrusion prevention for troubleshooting purposes or if client computers detect an excessive number of false positives. Typically, you should not disable intrusion prevention. See "Turning on or turning off Network Threat Protection" on page 33.

Table 4-1 Managing intrusion prevention *(continued)*

Action	Description
Enable intrusion prevention notifications	You can configure notifications to appear when Symantec Endpoint Protection detects an attack. See "Turning on and turning off Network Threat Protection notifications" on page 34.

Managing firewall protection for the Mac client

The Symantec Endpoint Protection firewall for Mac provides firewall protection that fully integrates into Symantec Endpoint Protection, which includes events, policies, and commands. The Symantec Endpoint Protection firewall is only available on managed clients.

Note: The Symantec Endpoint Protection firewall for Mac does not integrate with the operating system's built-in firewall. Instead, it runs in parallel. The operating system firewall inspects at the Application layer, while the Symantec Endpoint Protection firewall inspects at lower levels (IP and Transport).

The Symantec Endpoint Protection firewall for Mac does not offer peer-to-peer blocking rules, though you can create these in part through custom firewall rules.

Table 4-2 Managing firewall protection

Action	Description
Learn about firewall protection	Learn how firewall protection monitors traffic and protects against common attack vectors. See "How Network Threat Protection protects your Mac" on page 10.
Enable or disable the firewall	You might need to disable the firewall for troubleshooting purposes, such as if traffic is blocked that you expect to be allowed. Typically, you should not disable the firewall. See "Turning on or turning off Network Threat Protection" on page 33.

Turning on or turning off Network Threat Protection

Typically, when you turn off the Network Threat Protection components on your computer, your computer is less secure. However, you might want to turn off intrusion prevention to prevent false positives, or turn off the firewall to troubleshoot blocked traffic. Intrusion prevention and the firewall are a part of Network Threat Protection.

For managed clients, the amount of control that you have over these settings depends on how the administrator configured the client. In addition, any changes that you make to these settings may revert to what the policy dictates at the next heartbeat.

For unmanaged clients, the firewall is not available.

Turning on or turning off Network Threat Protection

1. On the Mac, click the Symantec Endpoint Protection icon in the menu bar, and then click **Symantec Endpoint Protection > Open Symantec Endpoint Protection**.
2. Click **Settings > Network Threat Protection**.
3. Do one or more of the following:
   - To enable or disable intrusion prevention, click **Intrusion Prevention**.
   - To enable or disable the firewall, click **Firewall**.

   If you turn off these components, you should turn them on again as soon as possible to make sure that your computer has the best protection.

Turning on and turning off Network Threat Protection notifications

1. On the Mac, click the Symantec Endpoint Protection icon in the menu bar, and then click **Symantec Endpoint Protection > Open Symantec Endpoint Protection**.
2. Click **Settings > Network Threat Protection**.
3. Turn on or turn off **Display Network Threat Protection Notifications**. These notifications are for intrusion prevention and for firewall.

   When notifications are turned on, you can turn on or turn off **Use sound when notifying users**.

See “Managing intrusion prevention” on page 32.

See “Managing firewall protection for the Mac client” on page 33.

Index