Symantec Endpoint Protection End-User Guide

For MacOS X

Symantec Endpoint Protection (SEP) is the evolutionary successor to Symantec Anti-Virus (SAV). SEP provides the anti-virus protection of SAV and will be Symantec's focus for future endpoint protection development on the MacOS X platform. New with version 12.1.4013.4013 is Network Threat Protection (NTP). NTP will block the network activity of over 2600 exploits (as of 7 Mar 2014).

This document will guide the user through the installation process and introduce the most basic components of the SEP interface and provide insight as to what to expect from SEP's behavior.

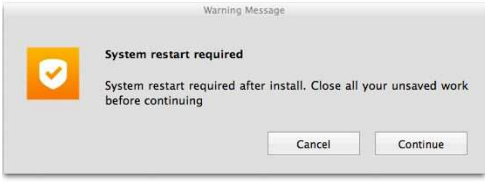
LLNL is providing SEP for home use as a no-cost benefit for its' employees, collaborators, and summer students. The SEP software is provided as-is and this document as the exclusive means of support. **DO NOT CONTACT 4-HELP or any other support organizations at LLNL for support of this software.** The ONLY exception will be the case where the user is having difficulty downloading the SEP installation files from access.llnl.gov . You may report download problems to 4-HELP.

Installation

The installation package of SEP from access.llnl.gov is compressed in a zip file.

Double click on the downloaded zip file to extract it into the native MacOS X installation package.

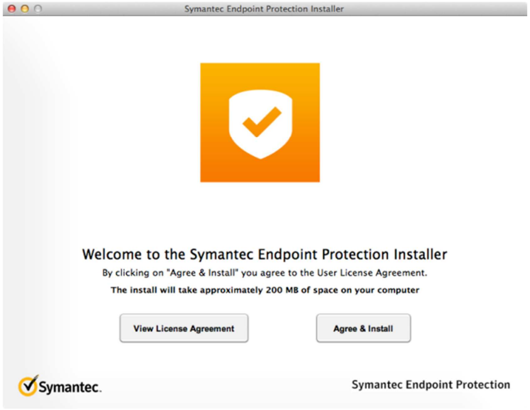
Double clicking on the Symantec Endpoint Protection Installer package will start the installation and bring up a user license acceptance window. A foreground window will notify you that a system reboot will be required.


Warning Message

System restart required

System restart required after install. Close all your unsaved work before continuing

Acknowledge reboot notification by selecting the "Continue" button


Symantec Endpoint Protection Installer

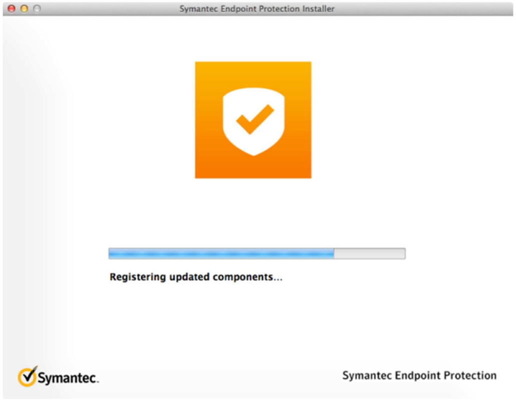
Welcome to the Symantec Endpoint Protection Installer

By clicking on "Agree & Install" you agree to the User License Agreement.

The install will take approximately 200 MB of space on your computer

View License Agreement
Agree & Install
Symantec.
Symantec Endpoint Protection

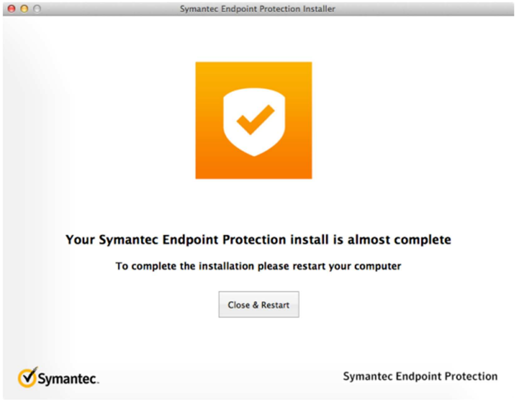
Select the "Agree & Install" button. Note that about 200MB of disk space is required.


Symantec Endpoint Protection Installer

Registering updated components...

Symantec.
Symantec Endpoint Protection

The installation will proceed with a progress indicator.


Symantec Endpoint Protection Installer

Your Symantec Endpoint Protection install is almost complete

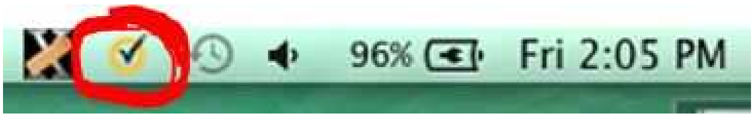
To complete the installation please restart your computer

Close & Restart
Symantec.
Symantec Endpoint Protection

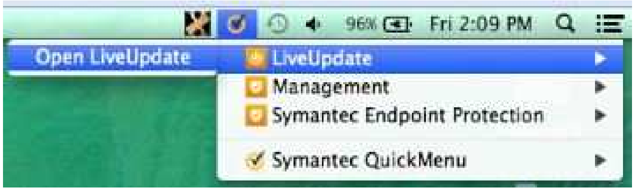
Upon completion of installation, you will be prompted for a reboot. Select the "Close & Restart" button.

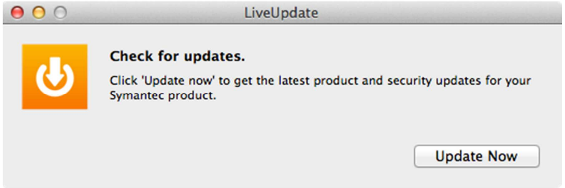
After the Reboot and Upon Logon

You will want to update your SEP product with the latest virus definitions and client updates. You can accomplish by going to the Apple Menu Bar and locating the Symantec icon (see below).



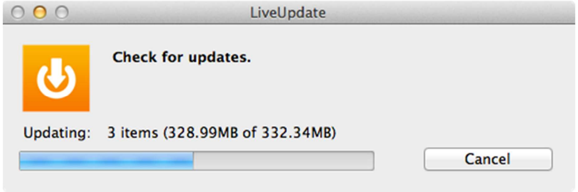
Select the **Open LiveUpdate** from the fly-out menu. A LiveUpdate window will display. Select the "Update Now" button.




LiveUpdate

Check for updates.

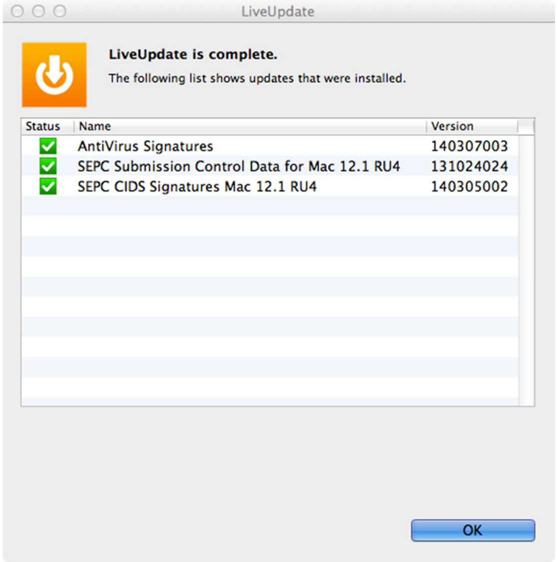
Click 'Update now' to get the latest product and security updates for your Symantec product.


LiveUpdate

Check for updates.

Updating: 3 items (328.99MB of 332.34MB)

A download and installation progress indicator will appear. Several minutes may be required for the download and installation even with a fast internet connection.


LiveUpdate

LiveUpdate is complete.

The following list shows updates that were installed.

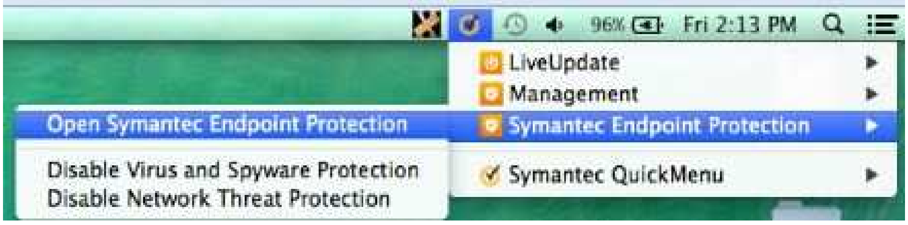
Status	Name	Version
✓	AntiVirus Signatures	140307003
✓	SEPC Submission Control Data for Mac 12.1 RU4	131024024
✓	SEPC CIDS Signatures Mac 12.1 RU4	140305002

All Symantec Endpoint components that were updated will be displayed. Click "Ok".

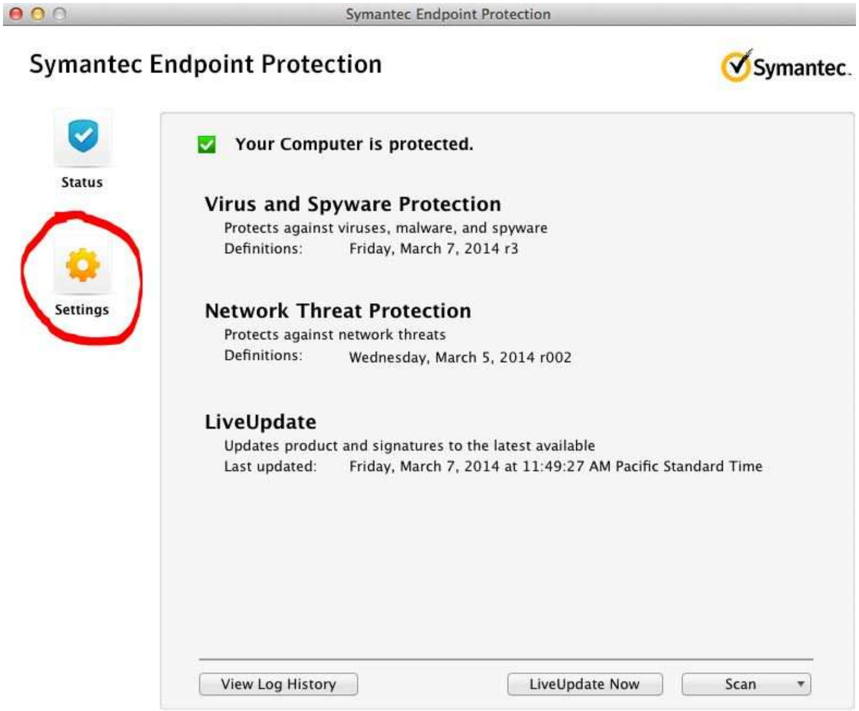
Scheduling LiveUpdate

In order to maximize SEP’s effectiveness, it is critically important to keep the product and its’ antivirus definitions up-to-date. The following guide will illustrate the process to schedule regular and periodic updates.

To schedule product updates, launch the SEP client by navigating the Apple Menu Bar


96%
Fri 2:13 PM
LiveUpdate
Management
Open Symantec Endpoint Protection
Symantec Endpoint Protection
Disable Virus and Spyware Protection
Disable Network Threat Protection
Symantec QuickMenu

The SEP status windows will launch



☑ Your Computer is protected.

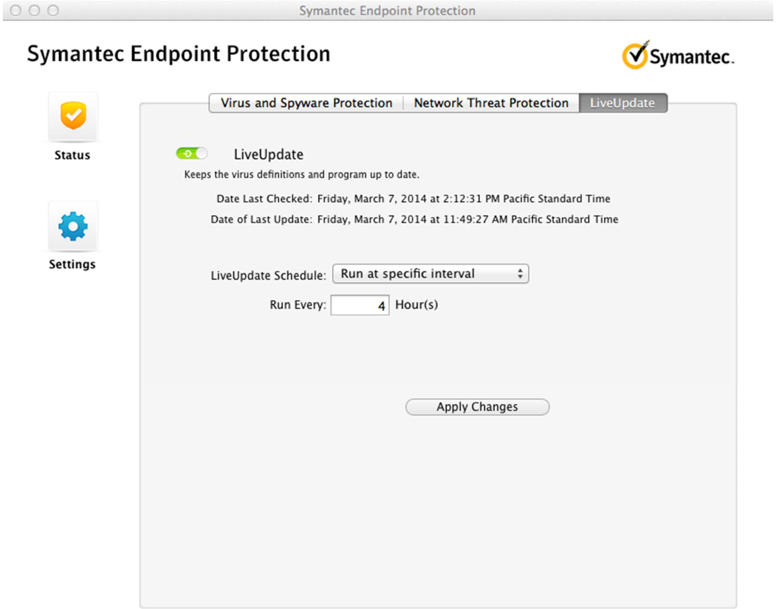
Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: Friday, March 7, 2014 r3

Network Threat Protection
Protects against network threats
Definitions: Wednesday, March 5, 2014 r002

LiveUpdate
Updates product and signatures to the latest available
Last updated: Friday, March 7, 2014 at 11:49:27 AM Pacific Standard Time

Select the “Settings” button.

In the settings pane, select the "LiveUpdate" tab to review the scheduling options.


Symantec Endpoint Protection
Symantec Endpoint Protection
Symantec.
Status
Settings
Virus and Spyware Protection
Network Threat Protection
LiveUpdate
Apply Changes

LiveUpdate

Keeps the virus definitions and program up to date.

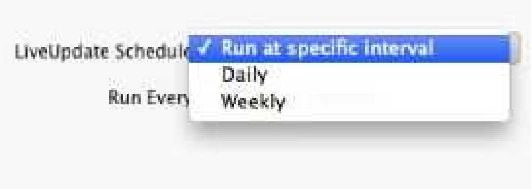
Date Last Checked: Friday, March 7, 2014 at 2:12:31 PM Pacific Standard Time

Date of Last Update: Friday, March 7, 2014 at 11:49:27 AM Pacific Standard Time

LiveUpdate Schedule: Run at specific interval

Run Every: 4 Hour(s)

A 4 hour reoccurring schedule is the default. You can change this up to 23 hours. Or if prefer a specific time of occurrence, you can choose settings for daily or weekly. Choosing either of these options will bring-up settings for the time and day of the week as appropriate.

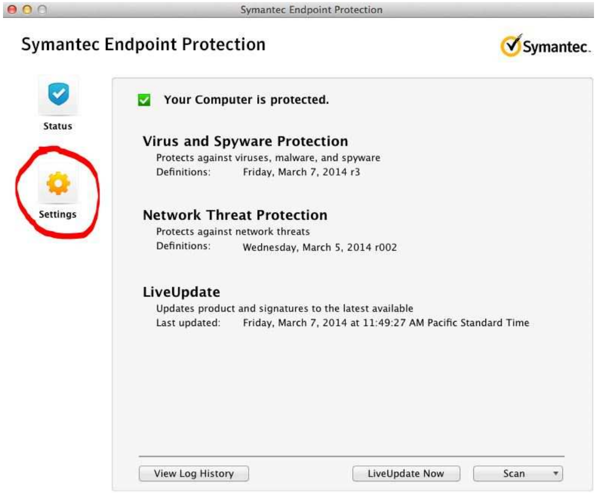


It's **highly recommended** that you set a schedule that occurs either daily at a convenient time or reoccurring. Keeping your virus definitions up-to-date is critically important.

Scheduling File Scans

While SEP's AutoProtect feature can scan new files as they are accessed by the user or operating system, it's still a good idea of perform periodic scans of the entire hard drive or at least user data (home directory). By default SEP will not schedule a full or partial drive scan; you'll need to schedule one if you want the additional protection. We recommend a monthly drive scan.

To schedule a scan, launch the SEP client and from the "Status" pane, select the "Settings" button

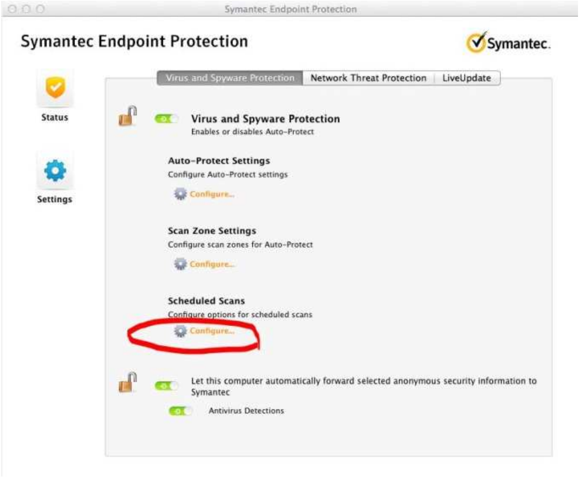


Your Computer is protected.

Virus and Spyware Protection
Protects against viruses, malware, and spyware
Definitions: Friday, March 7, 2014 r3

Network Threat Protection
Protects against network threats
Definitions: Wednesday, March 5, 2014 r002

LiveUpdate
Updates product and signatures to the latest available
Last updated: Friday, March 7, 2014 at 11:49:27 AM Pacific Standard Time


Symantec Endpoint Protection
Symantec Endpoint Protection
Symantec.
Virus and Spyware Protection
Network Threat Protection
LiveUpdate
Status
Settings
Configure...
Configure...
Configure...

Virus and Spyware Protection
Enables or disables Auto-Protect

Auto-Protect Settings
Configure Auto-Protect settings

Scan Zone Settings
Configure scan zones for Auto-Protect

Scheduled Scans
Configure options for scheduled scans

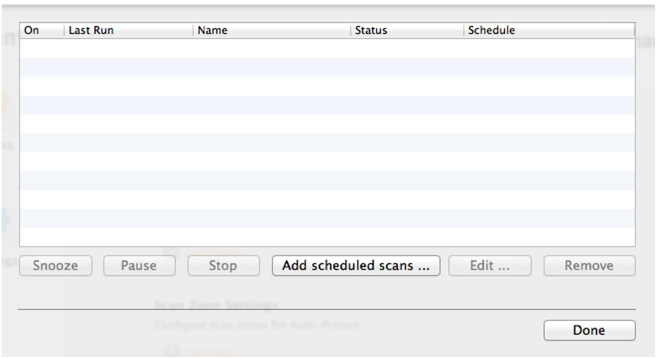
Let this computer automatically forward selected anonymous security information to Symantec

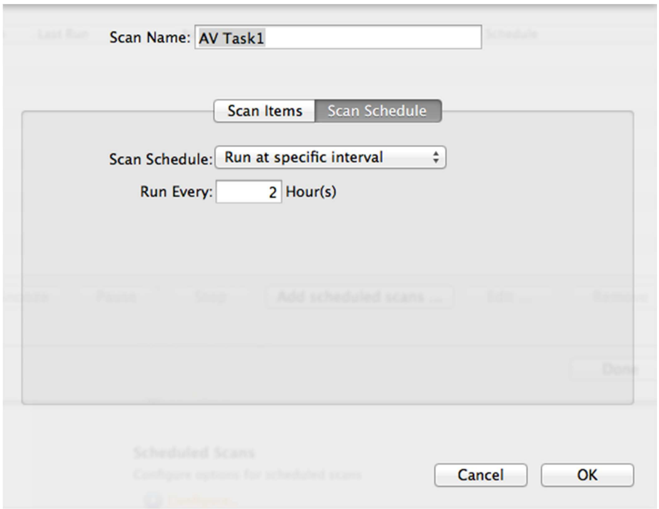
Antivirus Detections

Click on the "Virus and Spyware Protection" tab to reveal all the feature options.

Under the "Schedule Scans" header, click on the "Configure…" link

A pane listing scheduled scans (will be blank after a recent SEP install) will display. Select the "Add scheduled scans…" button.

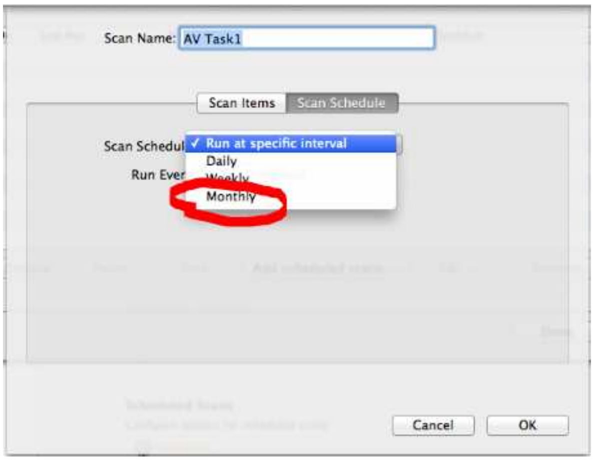



Scan Name: AV Task1

Scan Schedule: Run at specific interval

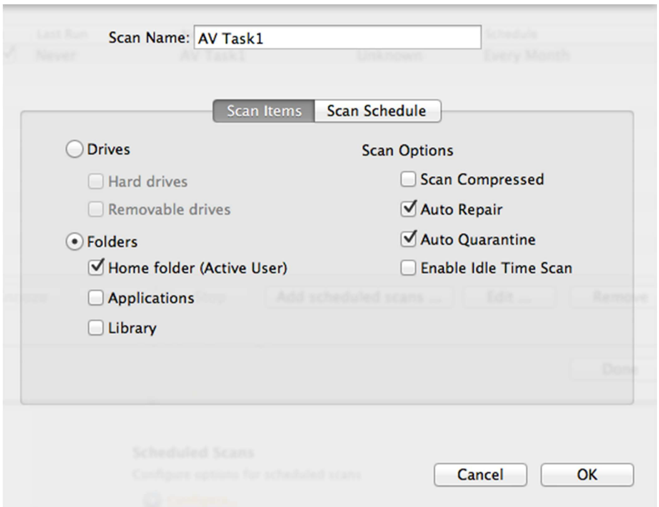
Run Every: 2 Hour(s)

The scan engine for SEP has been improved greatly over previous versions; still, the default 2 two-hour reoccurrence is just a bit too frequent.


Scan Name: AV Task1

We recommend a monthly schedule. Select monthly from the pull-down menu. Additional day-of-the-month and time options will appear. Select a convenient time, typically late at night or early morning.

After you’ve choosen *when* to scan, next you want to select *what* to scan. Selet the “Scan Items” button and review the options.



Scan Name: AV Task1

○ Drives

□ Hard drives

□ Removable drives

● Folders

☑ Home folder (Active User)

□ Applications

□ Library

Scan Options

□ Scan Compressed

☑ Auto Repair

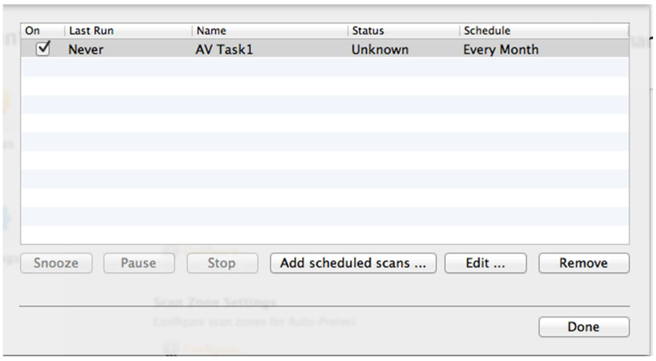
☑ Auto Quarantine

□ Enable Idle Time Scan

It’s HIGHLY RECOMMENDED that you select at least the defaults as shown.

Pay particular attention to the “Auto Repair” and “Auto Quarantine” checks. Both must be checked if you want viruses and malware to be moved to quarantine or a repair attempt made. Checking “Auto Quarantine” only will NOT move virus and malware to the quarantine.

Click “Ok” when satisfied with options.



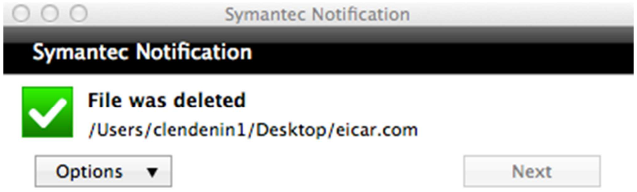
On	Last Run	Name	Status	Schedule
☑	Never	AV Task1	Unknown	Every Month

Your scheduled scan should now be displayed in the scan listing pane.

Select the “Done” button to complete.

Responding to SEP Virus Detection:

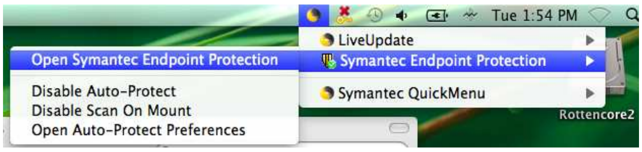
SEP will typically discover viruses on your system automatically as they are introduced. SEP's notifications and prompts are straightforward to understand. The following will document the process of virus detection.



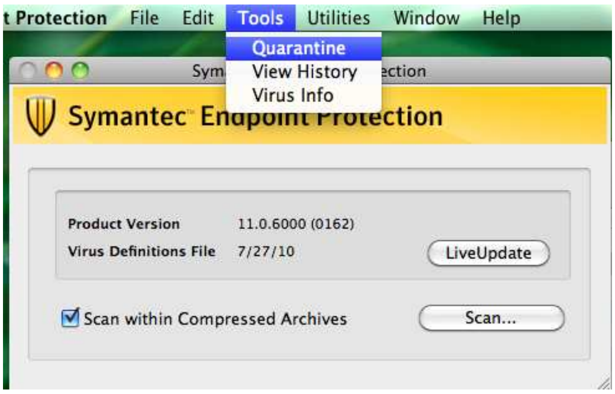
Symantec Notification

File was deleted
/Users/clendenin1/Desktop/eicar.com

SEP has discovered a virus on the desktop named "eicar.com" that was copied from a network location. The file was deleted because it could not be automatically repaired.



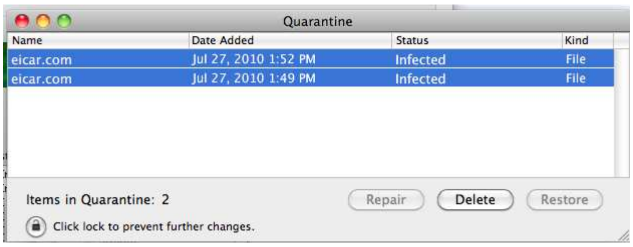
To access SEP's quarantine, go to the Apple Menu Bar, click on the Symantec icon, choose **Symantec EndPoint Protection**, and then **Open Symantec Endpoint Protection**.



Product Version 11.0.6000 (0162)
Virus Definitions File 7/27/10

☑ Scan within Compressed Archives

From the SEP menu, select **Tools** and **Quarantine**.



Quarantine

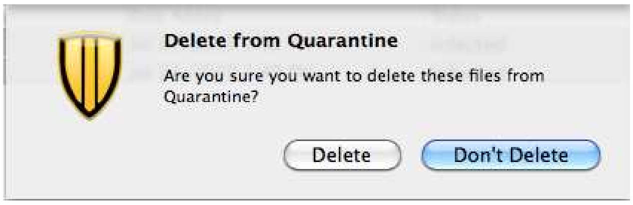
Name	Date Added	Status	Kind
eicar.com	Jul 27, 2010 1:52 PM	Infected	File
eicar.com	Jul 27, 2010 1:49 PM	Infected	File

Items in Quarantine: 2

Click lock to prevent further changes.

Infected files are listed in the quarantine. Highlight the files by selecting them and then choose the "**Delete**" button to empty the quarantine.

Note: You may need to click on the admin "lock" and provide admin credentials to access the "**Delete**" button



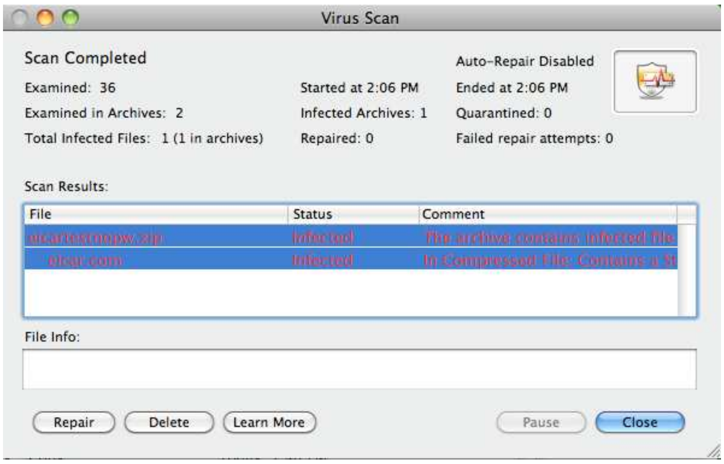
Delete from Quarantine

Are you sure you want to delete these files from Quarantine?

Select the “Delete” button in the confirmation display.

SEP’s File Scan Detects Virus

While rare, at times, SEP won’t discover a virus until a file scan is performed. The notification and remediation process is similar to the process described earlier.



Scan Completed

Examined: 36

Examined in Archives: 2

Total Infected Files: 1 (1 in archives)

Started at 2:06 PM

Infected Archives: 1

Repaired: 0

Auto-Repair Disabled

Ended at 2:06 PM

Quarantined: 0

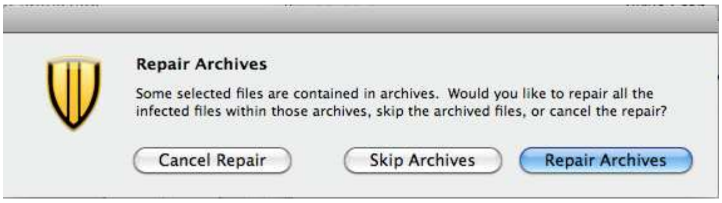
Failed repair attempts: 0

Scan Results:

File	Status	Comment
eicartestnopw.zip	Infected	The archive contains infected file
eicar.com	Infected	In Compressed File: Contains a S

File Info:

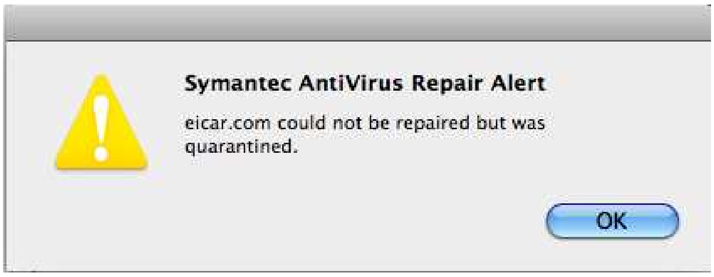
SEP has discovered two infected files, a compressed file and its’ contents. Select the “Delete” button to remove the file. You can attempt to “Repair” the file. A “Repair” often removes the file or places it on the quarantine.



Repair Archives

Some selected files are contained in archives. Would you like to repair all the infected files within those archives, skip the archived files, or cancel the repair?

Since the file is embedded in an archived file, SEP is asking whether it should repair the archive. In this case, you should select “Repair Archives”.



Symantec AntiVirus Repair Alert

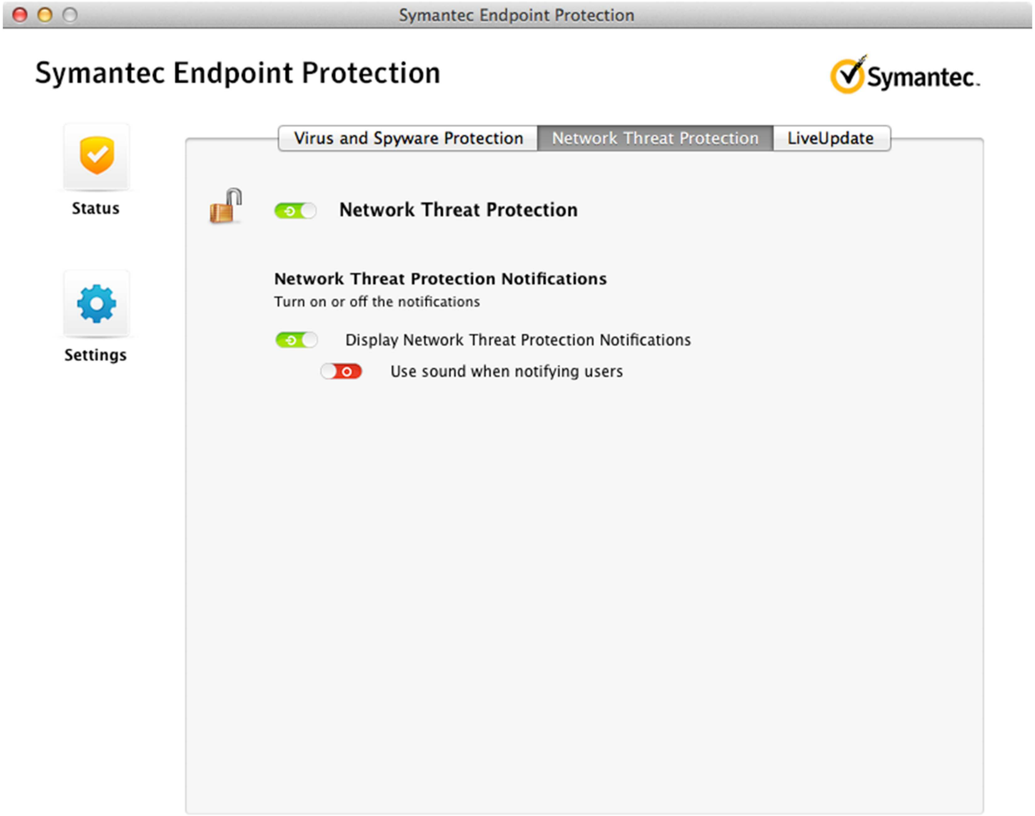
eicar.com could not be repaired but was quarantined.

If the file can't be repaired, SEP will notify you and place the file in quarantine.

Empty the quarantine as described earlier.

Network Threat Protection (NTP)

Network Threat Protection (NTP) is a new feature with this release of SEP on the Mac OS X platform. As of the date of the document (3/2014) NTP protects against more than 2600 known exploits and the list continues to grow. In the unmanaged client there is not much user control over the feature other than to disable it or to turn off sound notification when an exploit is intercepted.


Symantec Endpoint Protection
Symantec Endpoint Protection
Symantec.
Status
Settings
Virus and Spyware Protection
Network Threat Protection
LiveUpdate

☑ Network Threat Protection

Network Threat Protection Notifications

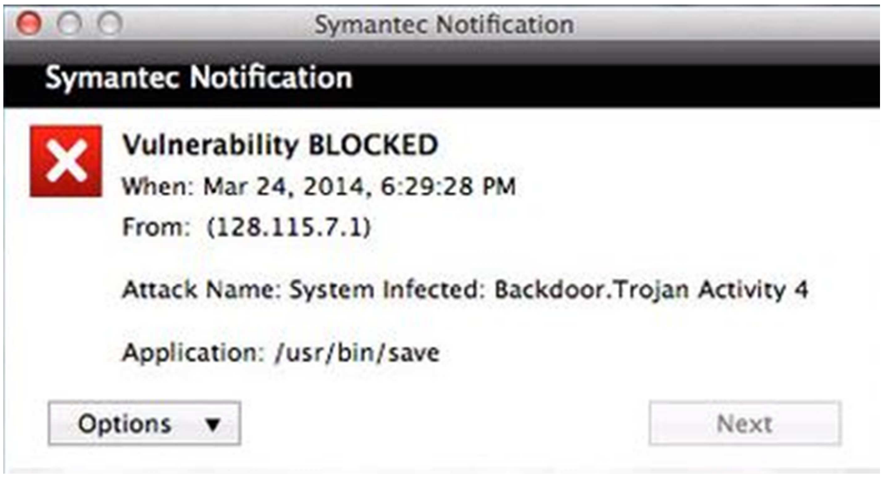
Turn on or off the notifications

☑ Display Network Threat Protection Notifications

☐ Use sound when notifying users

It is HIGHLY recommended that you leave NTP enabled unless you are experiencing networking issues and you suspect that SEP might be the problem.

Should SEP intercept an exploit, it will notify you with a dialogue pop-up. Typically the exploit will be listed, the source of the exploit, and what action was taken (usually blocked).



Symantec Notification

Vulnerability BLOCKED

When: Mar 24, 2014, 6:29:28 PM

From: (128.115.7.1)

Attack Name: System Infected: Backdoor.Trojan Activity 4

Application: /usr/bin/save

This concludes this tutorial. You will find additional information in SEP’s built in help system should you need to know more about this product.