SEP for Mac: Troubleshooting

Marc Lowe on January 28, 2020

SEP for Mac provides Anti-virus/Anti-malware (AV) protection and network intrustion prevention technologies (IPS), along with added central management and reporting. Its protection technology may inhibit performance and/or seemingly disrupt any file/folder functionality of your computer. Most issues should subside after the particular SEP protection technology has accomplished its tasks in searching for, and/or remedying, potential risks.

The SEP for Mac FAQ page [1], tries to cover common/known issues and is a good place to start if you suspect SEP may be misbehaving.

This document will walk you through SEP for Mac's typical behaviors and basic troubleshooting guidelines, as well as how to temporarily disable SEP protection technologies and how get log information that may be needed when calling the Service Desk for further assistance.

Common Behaviour from the SEP for Mac Client

Generally, the UCSF SEP client policies are set to allow end-users to temporarily disable the SEP protection technologies to help troubleshoot issues. Before we discuss that option, as well as other work-arounds, here are some common behaviors to help determine if SEP is just doing its job, or if SEP may be the cause of anomolous issues.

SEP for Mac contains anti-virus/anti-malware protection technologies. Typically, the most resource intensive task that SEP for Mac performs is running a full scan of a volume. Potential side effects during file scanning may include:

- increased cpu usage

- slow disk access
- locked out by a file caused by quarantining actions
- block internet traffic deemed to be an attack/risk to the network

To determine if SEP for Mac is in the middle of a scanning operation, you can check the status by:

1. Go to Applications -> Symantec Solutions -> Symantec Endpoint Protection
2. the Status screen should note any active tasks being perform by SEP

Other things to note about scheduled scans:

- The first scan of any volume may take a long time to complete
- After a successfully completed scan, subsequent scheduled scans will take less time since the client should skip files that have not modified since the last scan
- Scheduled scan(s), defined in policy, are typically set for times that will cause the least amount of impact to the work day (i.e. in the middle of the night or really early in the morning)
- If a machine was powered down during a scheduled scan, the scan will resume once the computer is powered on again

A note regarding Time Machine volumes:

- a Time Machine volume containing a long history will take a really long time to complete because each time interval on the backup will be scanned as though it were an entire system
- to mitigate the issue, we recommend:
    - only mounting Time Machine volumes when needed
      -or-
    - starting a new Time Machine volume *after* installing the SEP for Mac client
      -or-
    - maintaining Time Machine on a smaller volume

Temporarily disabling the SEP client

Though **disabling SEP is not recommended**, the quickest way to determine if an issue is being caused by SEP's protection technologies, is to "disable" the client temporarily to see if an issue goes away.

In the next section, we will discuss how to examine logs to determine what SEP is doing, which is the preferred method to rule out SEP as the cause of unwanted behavior. However, the feature of allowing end-users to "disable SEP", provides an easy way to set the SEP client into a pass-through mode to determine if one of SEP's protection technologies is interfering with a task you need to accomplish and know to be benign.

To temporarily disable the Auto-Protect feature:

1. In the top menu bar, to the far right, click the Symantec QuickMenu icon.
2. From the drop-down list, select Symantec Endpoint Protection.
3. From the drop-down list, select Disable Virus and Spyware protection & repeat for Disable Network Threat Protection.
4. An authentication window will open.
5. In the "Name:" field, type a local account name that has administrator privileges.
6. In the "Password:" field, type the password for the administrator account.
7. Click OK.

To re-enable SEP Auto-Protect feature:

- wait for a few minutes (the central policy should force the client re-enable itself shortly)
  -or-
- follow the same procedures used to disable the feature, but in step 3, choose "Enable" for the protection type

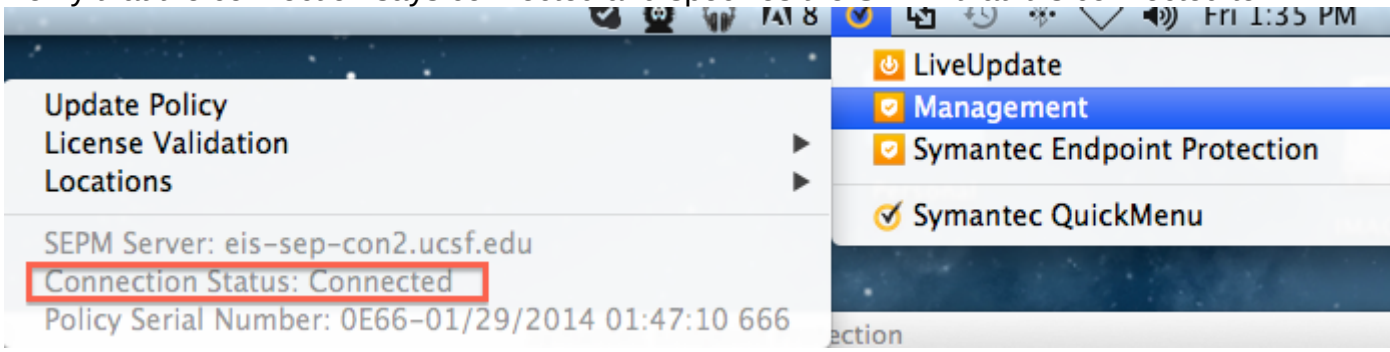
To stop an active scanning process:

1. Go to Applications -> Symantec Solutions -> Symantec Endpoint Protection
2. If a scan is in progress, you should be presented with an option to postpone or cancel the scan

Communications issues for updates to definitions and policies

To ensure the client is communicating and is managed properly by the endpoint servers:

1. Select the Symantec client tray icon located at the top right corner of the screen.
2. Hover the mouse over the Management menu choice.
3. Verify that the connection says connected and specifies the SEPM that it is connected to.



Checking Logs on a Mac

1. Go to Applications -> Symantec Solutions -> Symantec Endpoint Protection
2. Click on 'View Log History'

Installation Logs

SEP for Mac installation logs are stored in the system's install logs:

- Review the file /private/var/log/install.log
- the phrase "Symantec Endpoint Protection Installation Log" will appear at the beginning of the installation cycle
- also accessible through the Console app utility.

Additional Logs

Information on exporting the logs mentioned above, can be found in the Symantec Knowledge Base Article TECH214527 [2]

Advanced users (tech savvy) can review more logs by following the instructions found on the Symantec Knowledge Base Article TECH134761 [3], which covers using the "GatherSymantecInfo" tool from Symantec.

Uninstalling a SEP client

A common troubleshooting step would be to uninstall and reinstall the SEP client.

Instructions for uninstalling the SEP client can be found on the SEP for Mac FAQ [4] documentation page.

After uninstalling, re-download a new client installer from https://software.ucsf.edu/content/endpoint-protection [5], and re-install the client.

Reporting issues and Getting Additional Help

1. Gather the "Troubleshooting" information found on the client
   (this will provide useful information regarding versions, communication settings, actions, updates, etc.)
    1. Go to Applications -> Symantec Solutions -> Symantec Endpoint Protection
    2. Click on 'View Log History'
    3. On the left colum, verify that "All" is highlighted
    4. Click on the button 'Export'
    5. Note the value in the "Where:" field, then click on the button "Save"
    6. Be prepared to provide this file when contacting the IT Service Desk
2. Contact the Service Desk by:

- visiting https://ucsf.service-now.com/ess/ [6]
  -or-
- calling them at (415) 514-4100

Advanced Troubleshooting for the tech-savvy

Most of Symantec's documentation (How-to articles, Knowledge base articles, and forum discussions) are fully open and accessible to anyone. Most of these are technical, but they can be very informative.

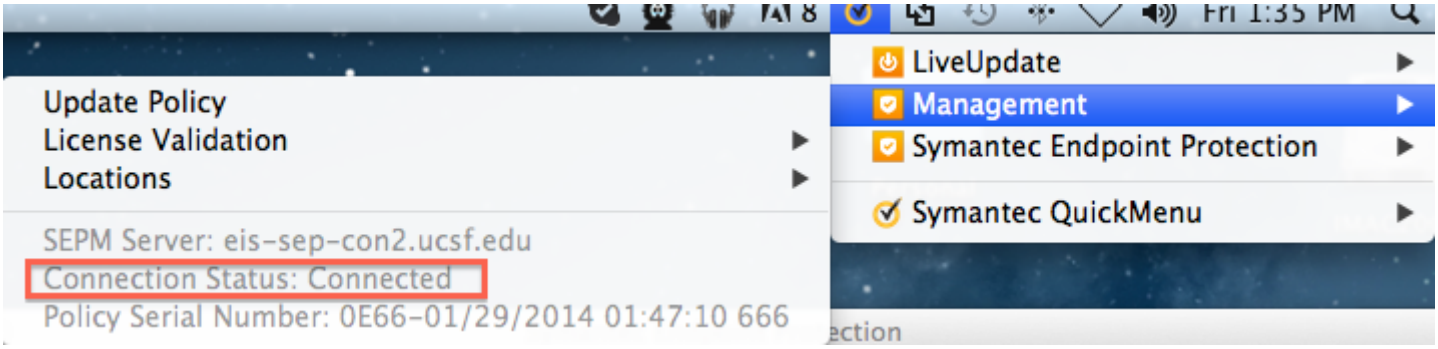
A good place to start for andvanced troubleshooting of SEP for Mac issues is Symantec's office "SEP for Mac FAQ" Knowledge Base article at:

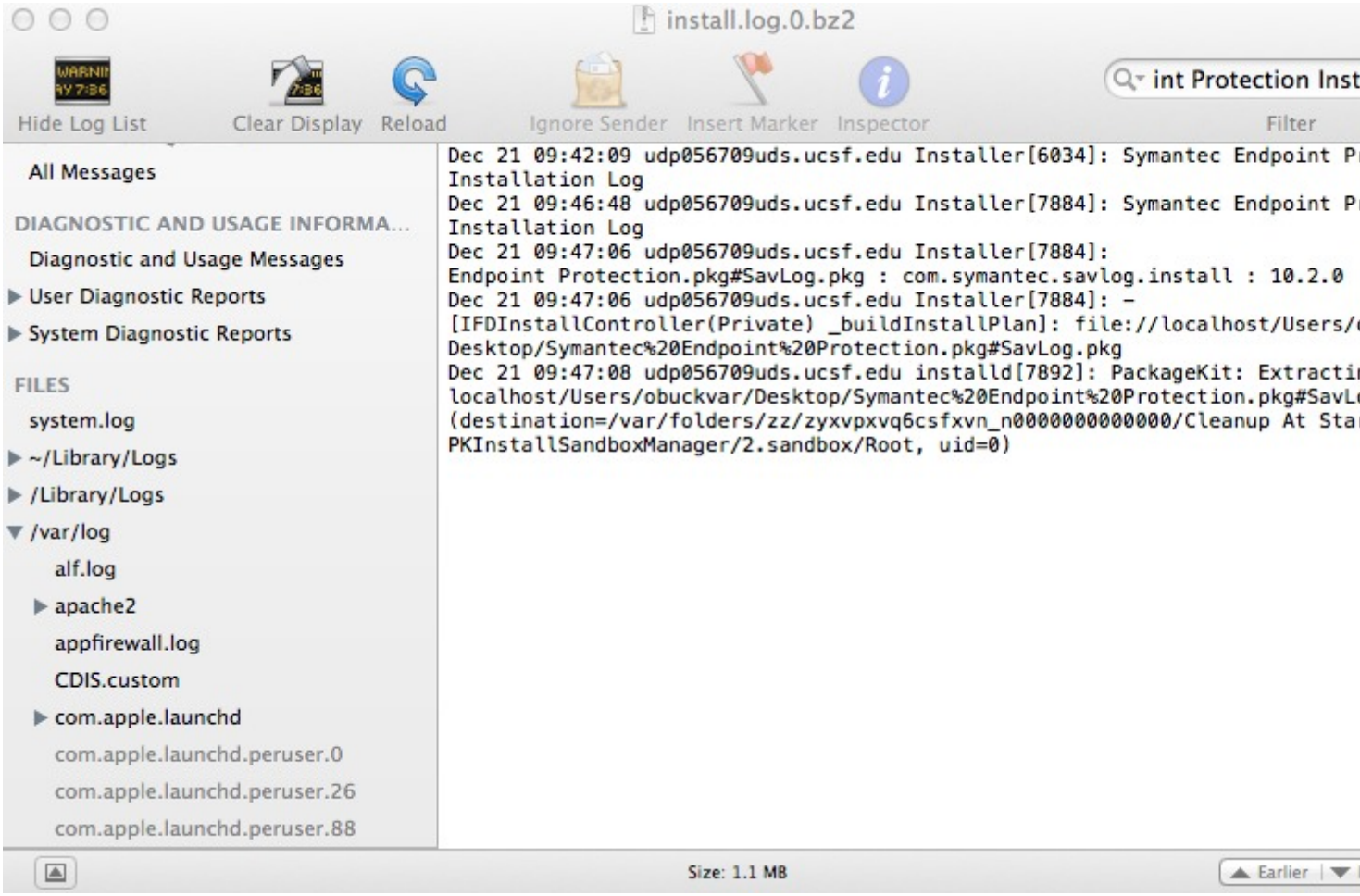
https://support.symantec.com/en_US/article.TECH240292.html [7]

Required Service Information

Symantec Endpoint Protection (SEP) [8]

Images





GET IT HELP. Contact the Service Desk online, or phone 415.514.4100

Site Login Site Index

Suggest an IT Improvement | © UC Regents

*/ //-->

Source URL: https://it.ucsf.edu/services/symantec-endpoint-protection-sep/tutorial/sep-mac-troubleshooting?page=8

Links
[1] https://it.ucsf.edu/services/symantec-endpoint-protection-sep/tutorial/sep-mac-faq
[2] https://support.symantec.com/en_US/article.TECH214527.html
[3] https://support.symantec.com/en_US/article.TECH134761.html
[4] https://it.ucsf.edu/services/symantec-endpoint-protection-sep/tutorial/sep-mac-faq?page=3
[5] https://software.ucsf.edu/content/endpoint-protection
[6] https://ucsf.service-now.com/ess/
[7] https://support.symantec.com/en_US/article.TECH240292.html
[8] https://it.ucsf.edu/services/symantec-endpoint-protection-sep