控制檯中的MAC核心和全磁碟訪問 — 面向終端的AMP

目錄

簡介

本檔案介紹用於終端機的進階惡意軟體防護(AMP)中排除故障的步驟，以有效解決兩個Mac故障：未授權全磁碟訪問(FDA)和核心模組。

作者：Uriel Torres、Javier Jesus Martinez，思科TAC工程師。

必要條件

需求

思科建議您瞭解以下主題：

·Mac工具知識
·具有管理員許可權的帳戶

採用元件

本檔案中的資訊是根據適用於MAC的終端思科AMP。

本檔案中的資訊是根據特定環境中的裝置所建立：

- MacOS High Sierra 10.13
- MacOS 10.14(Mojave)

限制

這是安裝在OSV-10.4.X和聯結器版本1.11.0上的OSX和AMP聯結器上的修飾性錯誤。AMP門戶顯示FDA的故障消息，主機顯示FDA被允許。
錯誤ID:CSCvq98799

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

當請求載入KEXT但尚未批准時，載入請求會被拒絕。MacOS High Sierra 10.13引入了一項新功能，這意味著使用者需要在載入新安裝的第三方核心擴展(KEXT)之前獲得批准，並且系統僅載入已批准的核心擴展。使用者需要執行前面提到的步驟來解決核心錯誤。
由於macOS 10.14(Mojave)引入了影響面向終端的AMP的Mac聯結器的新安全功能，您需要確保向AMP服務守護程式授予全磁碟訪問許可權，未經批准，AMP聯結器無法向受macOS保護的檔案系統的這些部分提供保護或可視性。

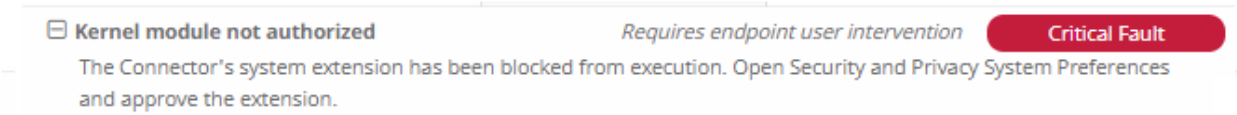
疑難排解

本節提供的資訊可用於對組態進行疑難排解。

控制檯錯誤

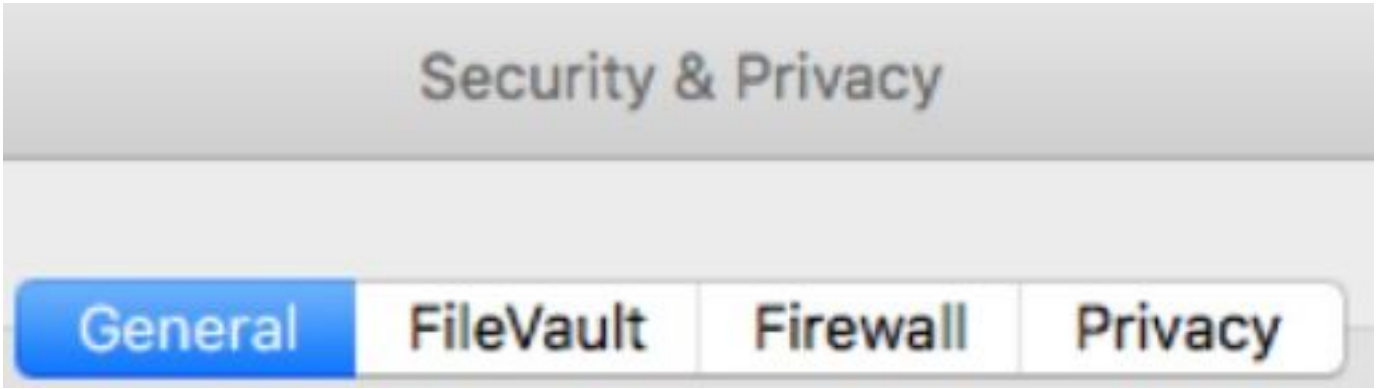
核心故障

AMP控制檯顯示錯誤「Kernel module not authorized」（核心模組未授權），當請求載入核心擴展(KEXT)時，該請求未獲批准、載入請求被拒絕且macOS顯示警報，如下圖所示。

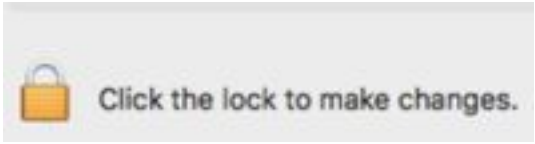


在Apple macOS升級後，有關核心批准的正式公告發佈，如下圖所示。

若要允許聯結器擴充模組，請導覽至**System Preferences > Security & Privacy > General**，如下圖所示。



按一下鎖定以批准KEXT（系統上只載入使用者批准的核心擴展），如下圖所示。

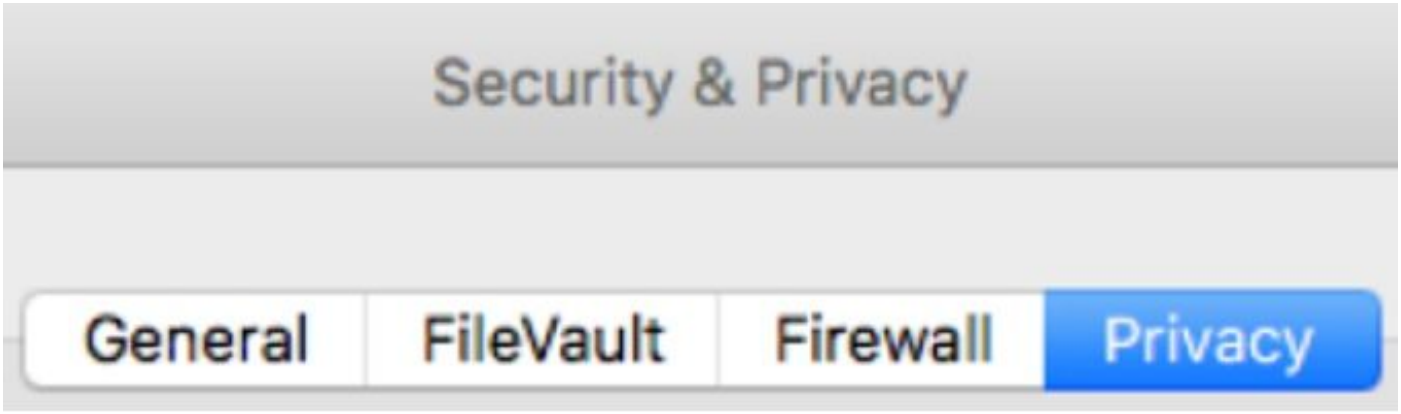


注意：警報後30分鐘，使用者批准將顯示在「安全和隱私首選項」窗格中。當KEXT被批准時，將來載入嘗試會導致批准使用者介面重新出現，但不會觸發其他使用者警報。

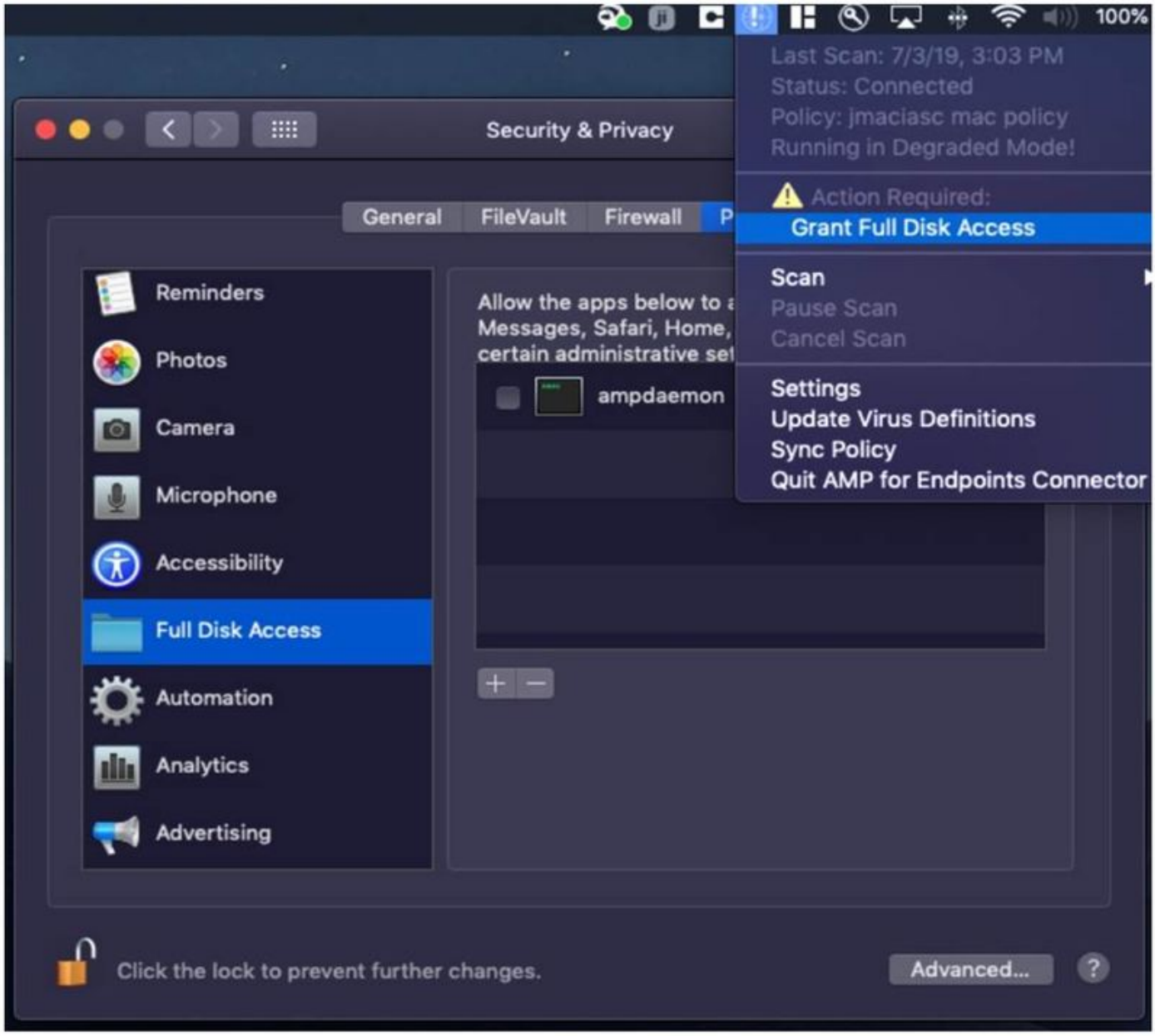
全磁碟訪問故障

AMP控制檯顯示「Disk Access not granted」（未授予磁碟訪問許可權），如下圖所示。

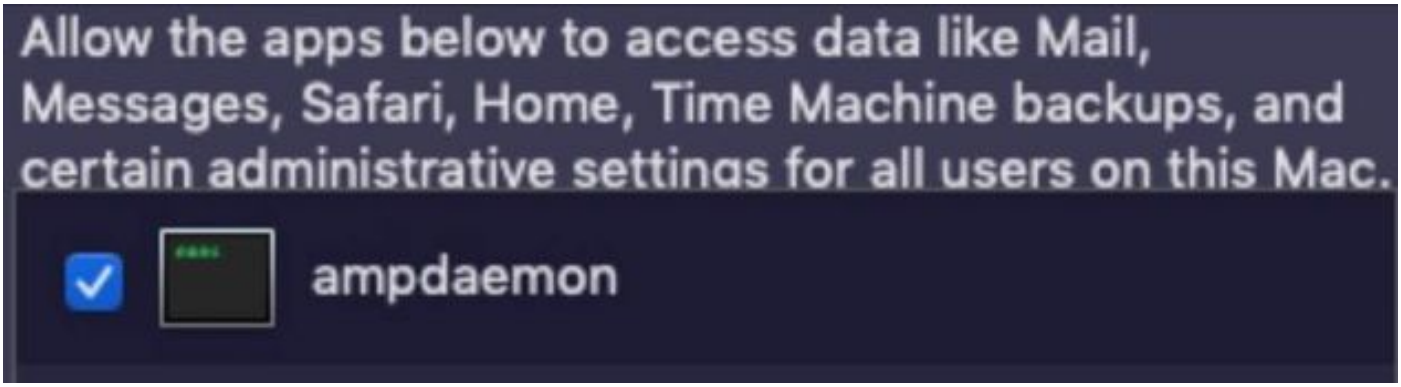
驗證是否不允許全盤訪問，請導航至**系統首選項>安全和隱私>隱私**，如下圖所示。



要批准AMP聯結器的Full磁碟訪問，請導航到Full Disk Access並複選ampdaemon進程，如下圖所示。

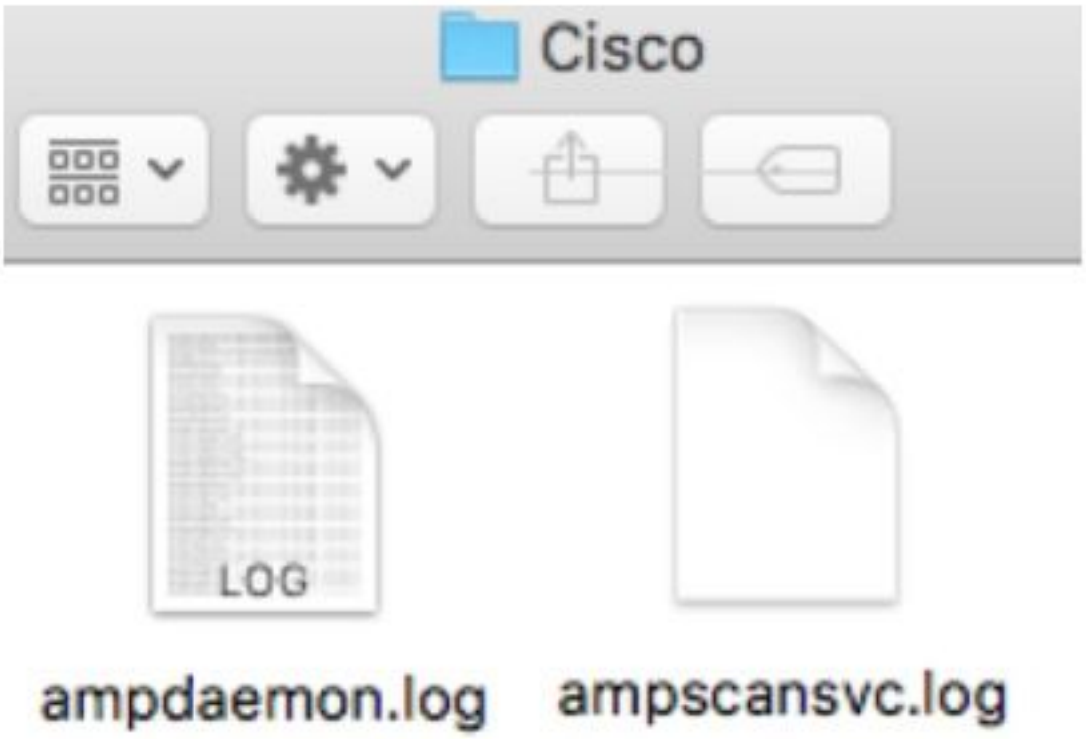


開啟終端機並停止AMP服務，然後運行下一個命令：**sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist**，選中覈取方塊，如下圖所示。



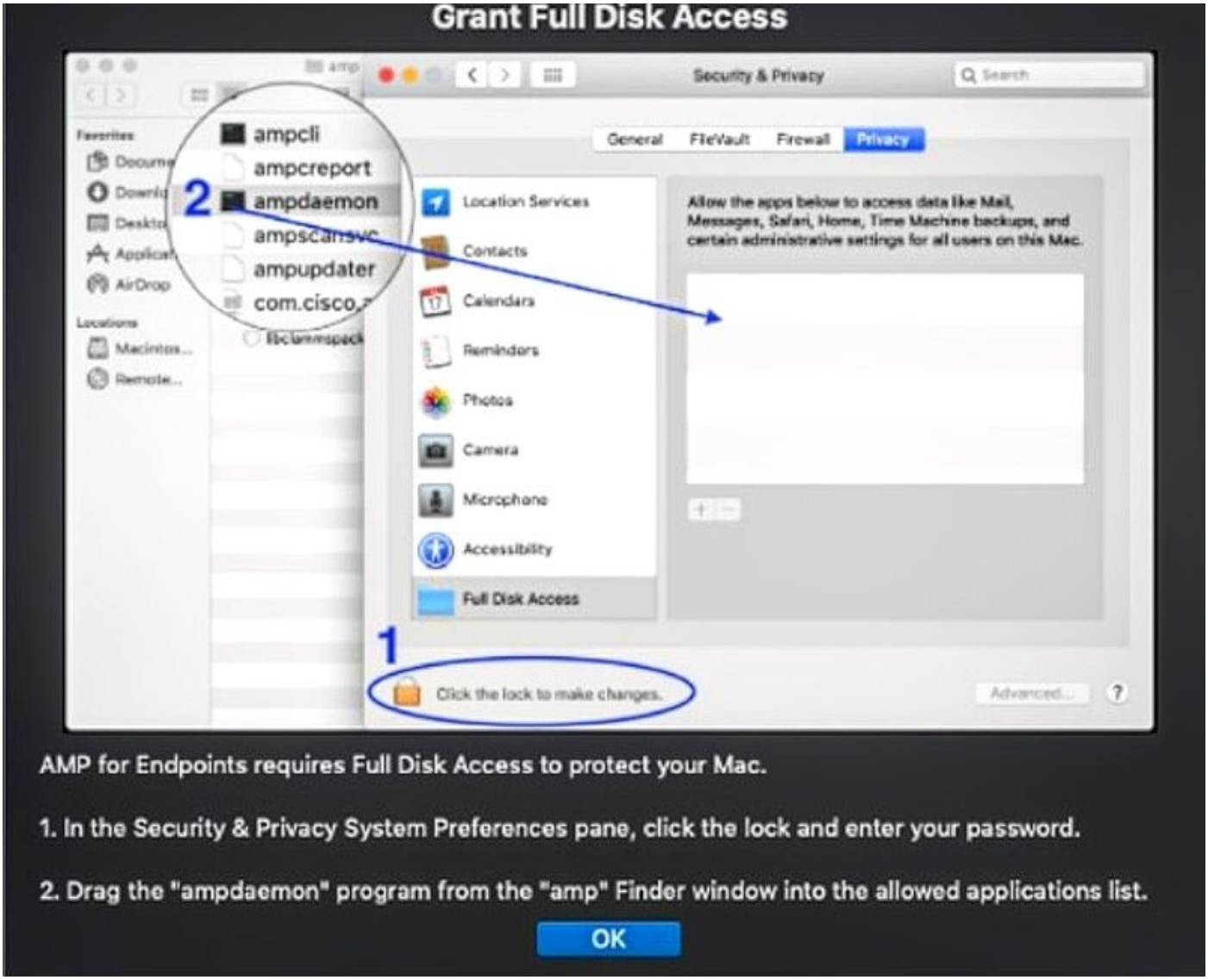
若要避免快取問題，請導覽至**/library/logs/cisco**，然後清除下一個檔案，如下圖所示。

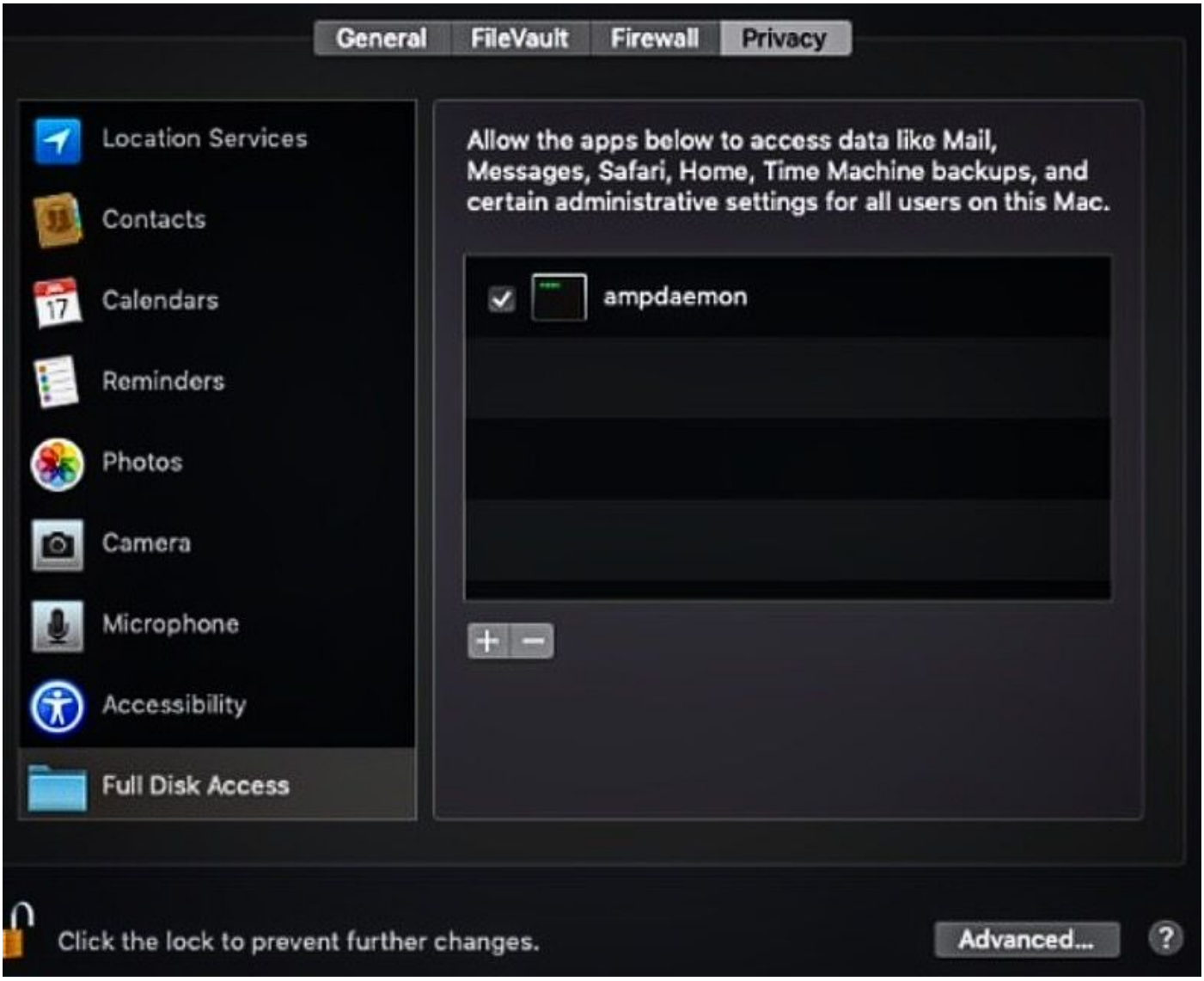
- ampdaemon.log
- ampscansvc.log



使用命令sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist啟動服務。

附註： 如果您找不到安瓿檔案，請將其拖放到「允許全磁碟訪問」清單中，確保選中該霰取方塊，如下圖所示。


Grant Full Disk Access
Security & Privacy
General
FileVault
Firewall
Privacy
ampcli
ampcreport
ampdaemon
ampscansvc
ampupdater
2
Location Services
Contacts
Calendars
Reminders
Photos
Camera
Microphone
Accessibility
Full Disk Access
Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.
1
Click the lock to make changes.
Advanced...
AMP for Endpoints requires Full Disk Access to protect your Mac.
1. In the Security & Privacy System Preferences pane, click the lock and enter your password.
2. Drag the "ampdaemon" program from the "amp" Finder window into the allowed applications list.
OK



為了授予磁碟完全訪問許可權，請授予核心許可權並建議MAC裝置重新啟動，在下一個檢測訊號間隔內，報告消息將從控制檯中消失。