控制台中的MAC内核和完整磁盘访问 — 面向终端的AMP

目录

简介

本文档介绍在面向终端的高级恶意软件防护(AMP)中进行故障排除的步骤，以处理两个Mac故障：完全磁盘访问(FDA)和内核模块未授权。

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

先决条件

要求

Cisco 建议您了解以下主题：

·Mac工具知识
·具有管理员权限的帐户

使用的组件

本文档中的信息基于面向MAC终端的思科AMP。

本文档中的信息是从特定环境中的设备创建的：

- MacOS高Sierra 10.13
- MacOS 10.14(Mojave)

限制

这是安装在OSV-10.4.X和连接器版本1.11.0上的OSX和AMP连接器上的修饰缺陷。AMP门户显示FDA的故障消息，主机显示允许FDA。
BugID:CSCvq98799

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

当请求加载KEXT但尚未批准时，加载请求将被拒绝。MacOS High Sierra 10.13引入了一项新功能，这意味着用户在加载新安装的第三方内核扩展(KEXT)之前需要获得批准，并且系统上只加载已批准的内核扩展。用户需要按照前面提到的步骤解决内核错误。
由于macOS 10.14(Mojave)引入了影响面向终端的AMP Mac连接器的新安全功能，因此您需要确保向AMP服务守护程序授予完全磁盘访问权限，但未经批准，AMP连接器无法为受macOS保护的文件系统的这些部分提供保护或可视性。

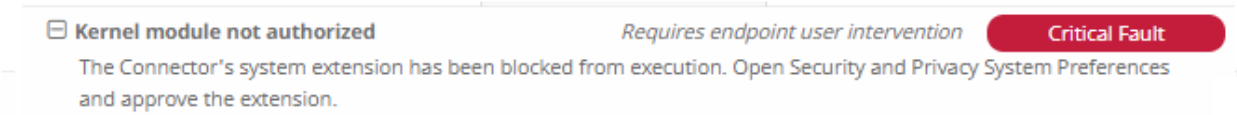
故障排除

本部分提供的信息可用于对配置进行故障排除。

控制台错误

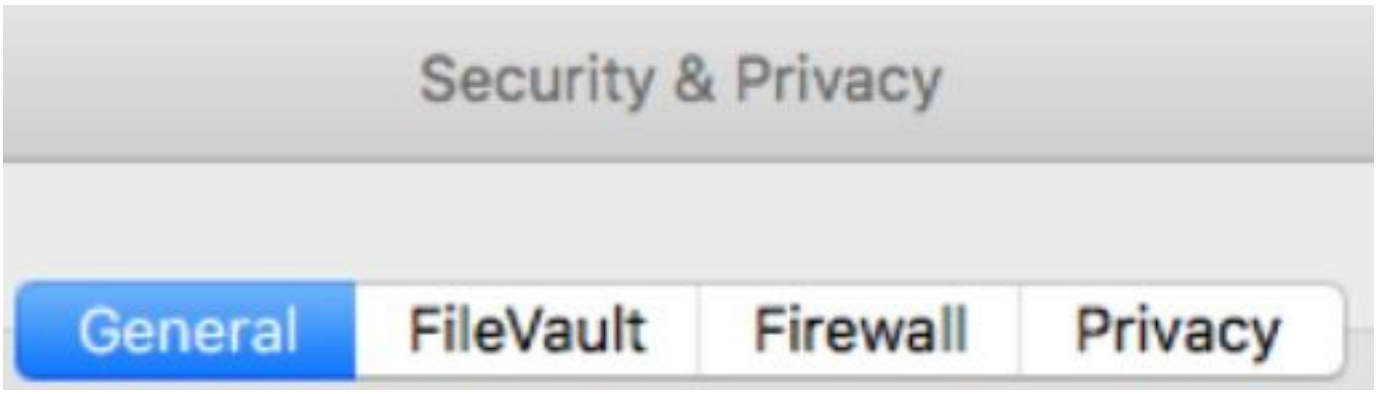
内核错误

AMP控制台显示错误“内核模块未授权”，当请求加载内核扩展(KEXT)且未获批准、加载请求被拒绝且macOS显示警报，如图所示。

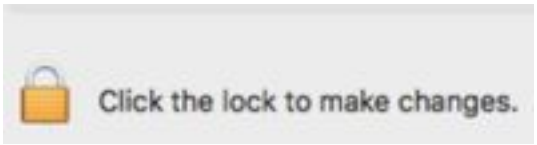


Apple macOS升级后，发布了有关内核批准的正式公告，如图所示。

要允许连接器扩展，请导航到**系统首选项>安全和隐私>**常规，如图所示。



单击“锁定”(Lock)以批准KEXT（仅系统上加载由用户批准的内核扩展），如图所示。

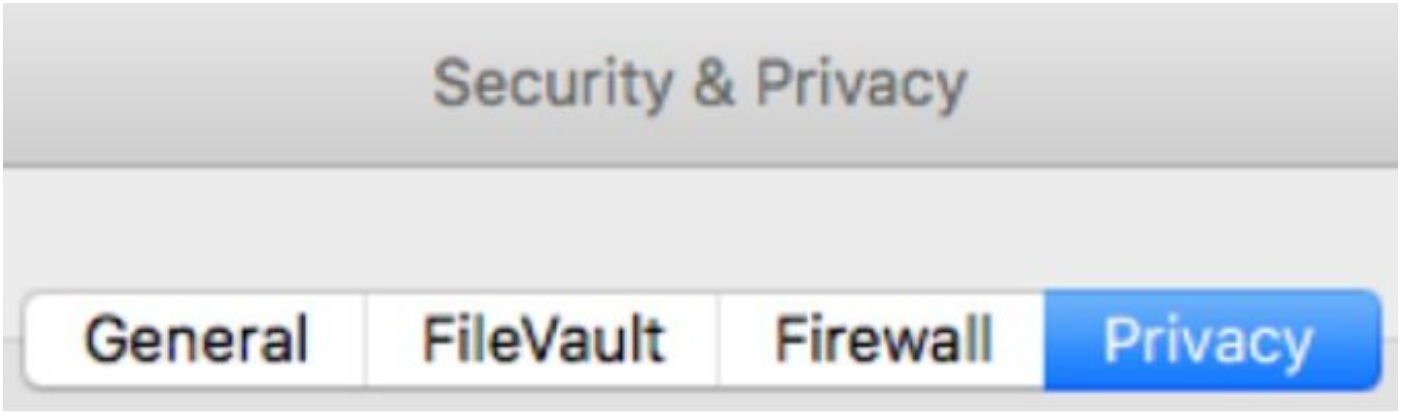


> **注意**：在警报后30分钟内，用户审批会显示在“安全和隐私首选项”窗格中。当KEXT获得批准后，将来的加载尝试会导致批准用户界面重新出现，但不会触发其他用户警报。

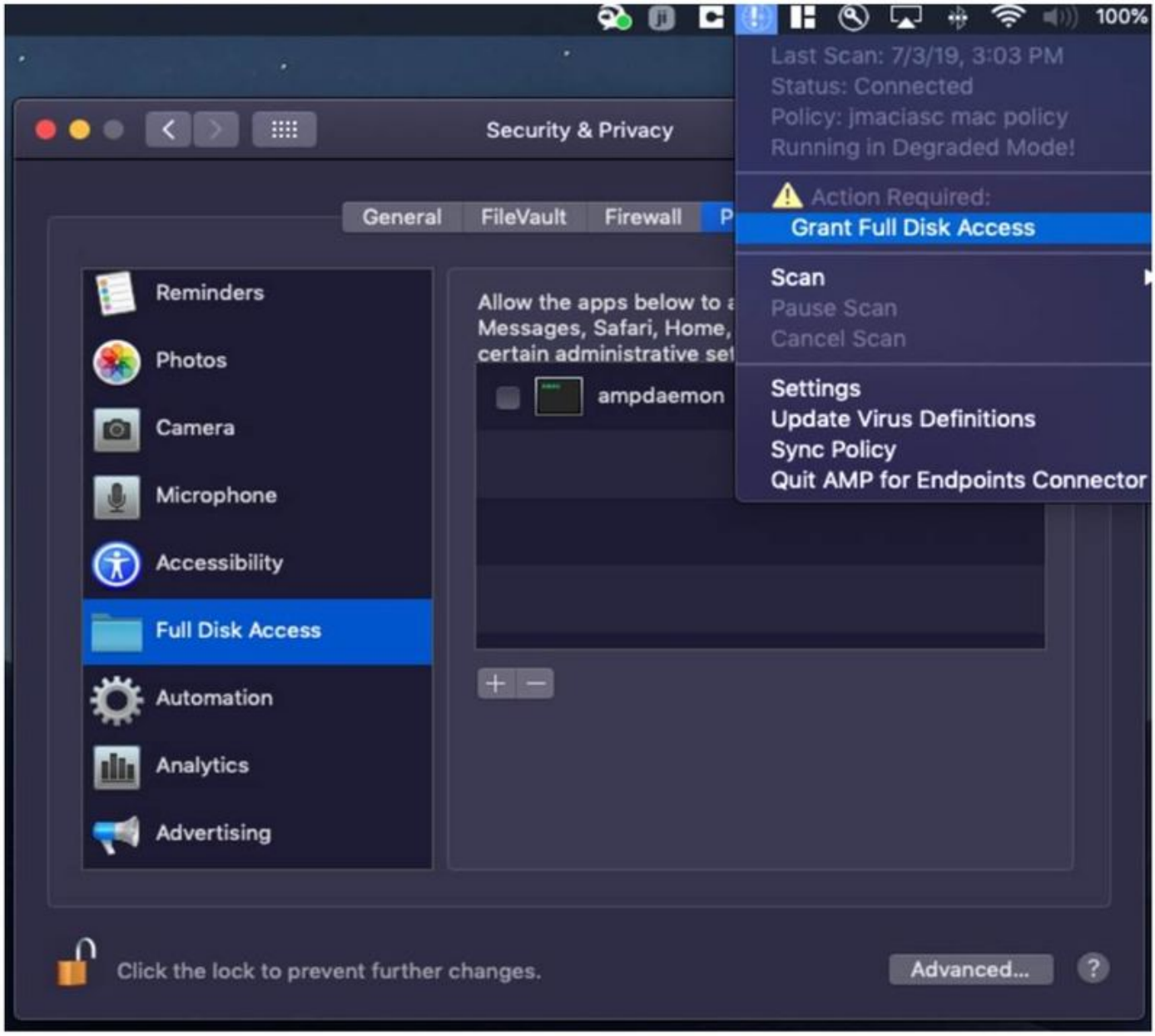
完全磁盘访问故障

AMP控制台显示“未授予磁盘访问权限”，如图所示。

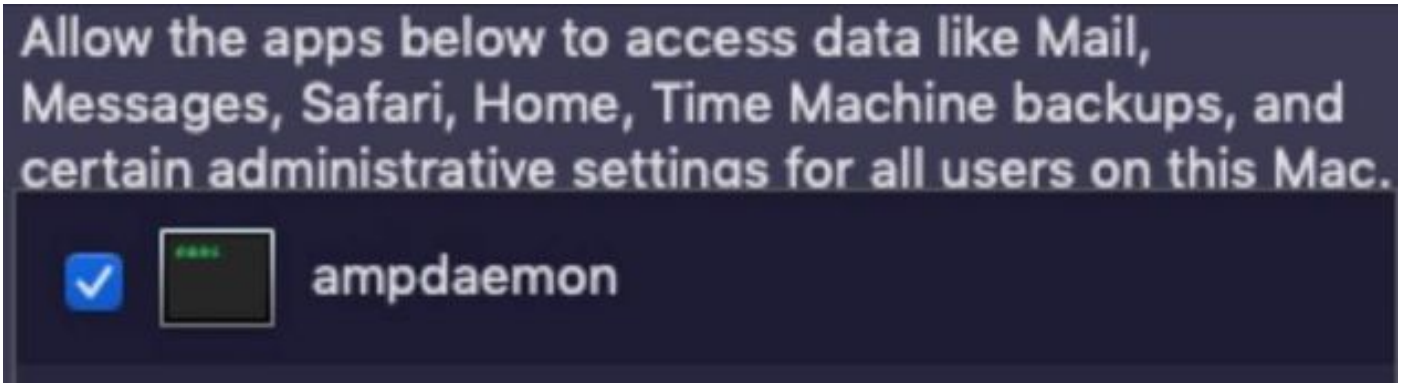
如图所示，请导航至“系统首选项”**>“安全和隐私”>“隐**私”，验证是否不允许完全磁盘访问。



要批准AMP连接器的全磁盘访问，请导航至全磁盘访问并选中ampdaemon进程，如图所示。

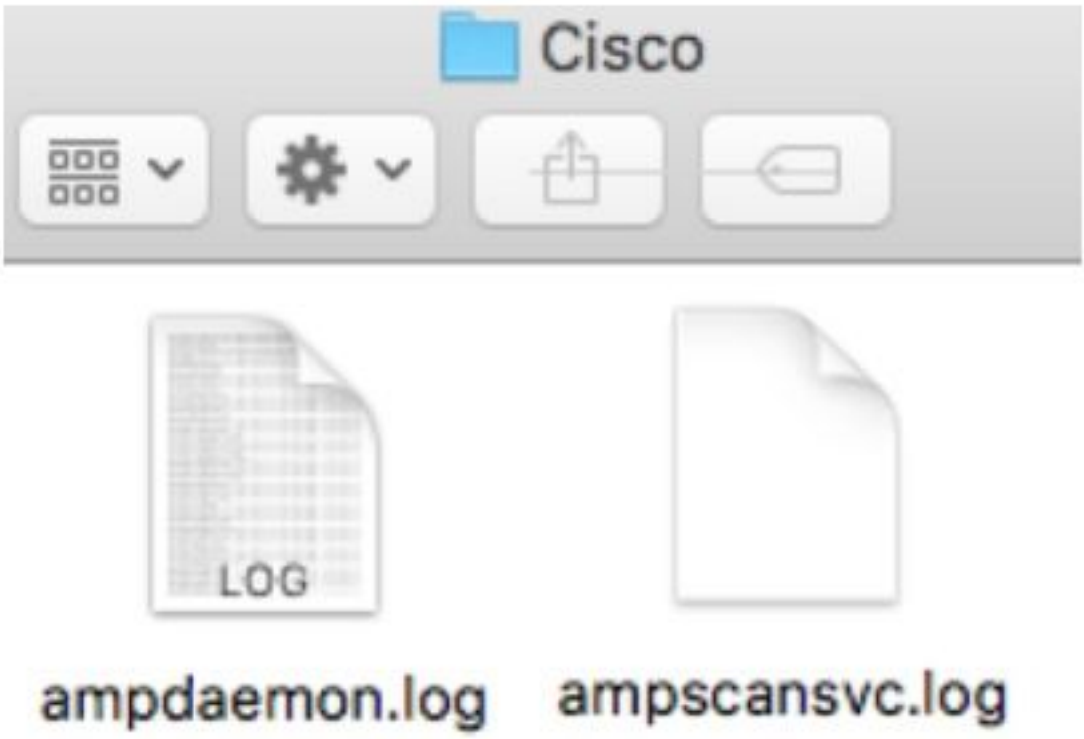


打开终端并停止AMP服务并运行下一个命令：**sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist**，如图所示标记复选框。



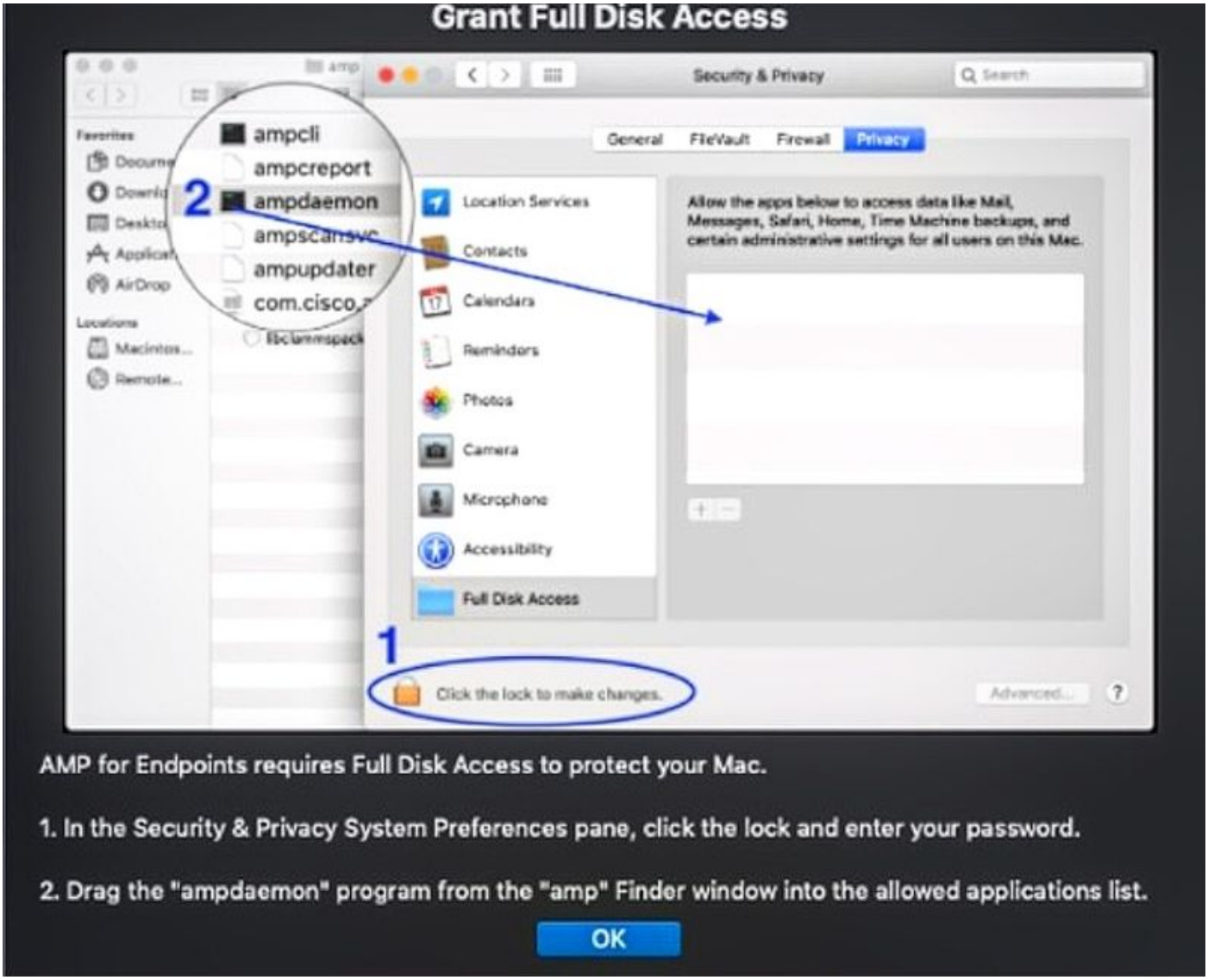
为避免缓存问题，请导航至**/library/logs/cisco**并清除下一个文件，如图所示。

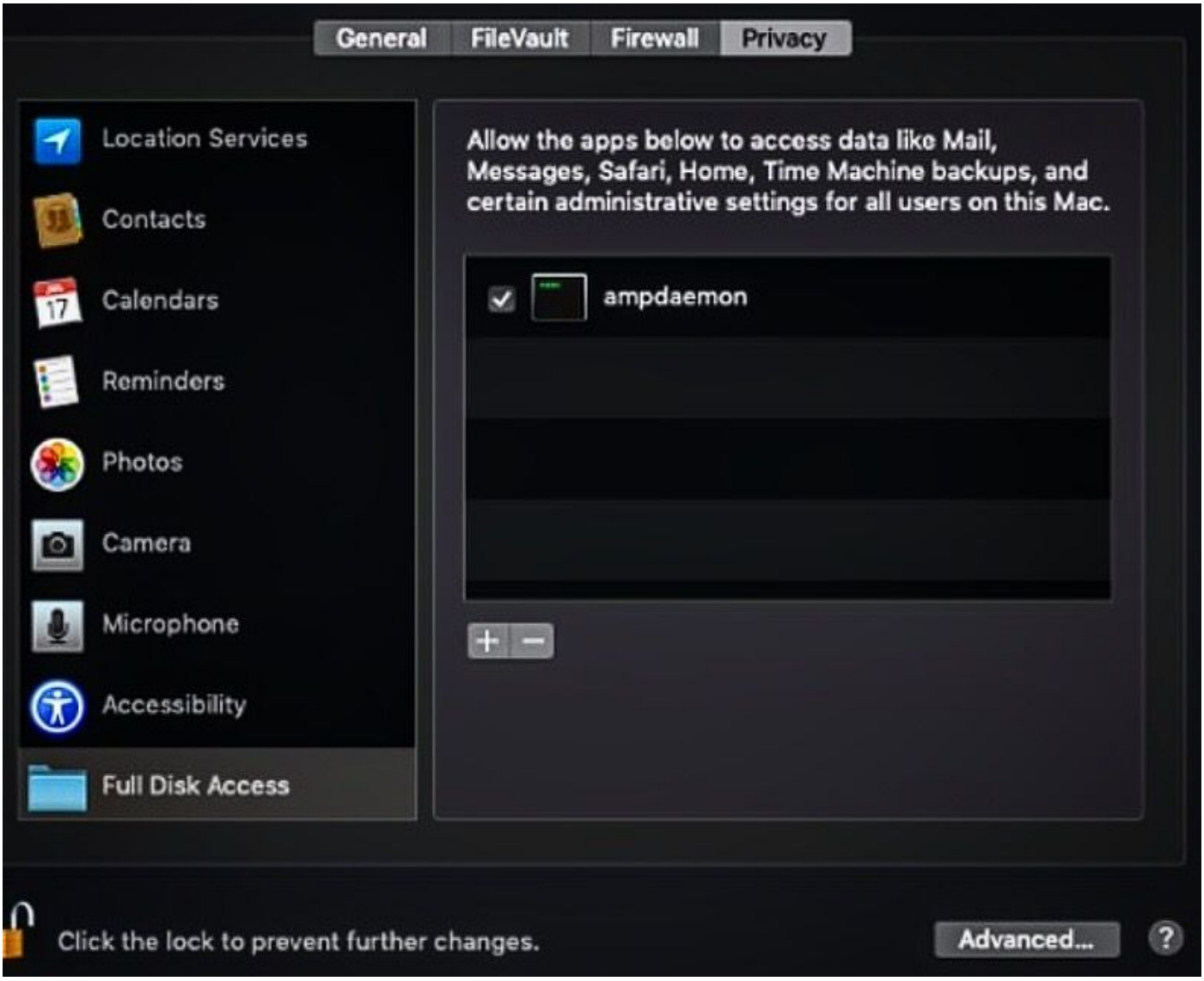
- ampdaemon.log
- ampscansvc.log



使用以下命令启动服务：**sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**。

注意： 如果找不到ampdeamon文件，请将其拖放到“允许完全磁盘访问”列表中，确保选中该复选框，如图所示。


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



为了授予完全磁盘访问权限，请授予内核权限并建议重新启动MAC设备，在下一个心跳间隔内，报告的消息从控制台消失。