MAC Kernel and Full Disk Access in the Console - AMP for Endpoints

Contents

Introduction

This document describes the steps to troubleshoot in Advanced Malware Protection (AMP) for Endpoints to work two Mac Faults: Full Disk Access (FDA) and Kernel module not authorized.

Contributed by Uriel Torres, Javier Jesus Martinez, Cisco TAC Engineers.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Mac tools knowledge
- Account with administrator privileges

Components Used

The information in this document is based on Cisco AMP for Endpoints for MAC.

The information in this document was created from the devices in a specific environment:

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Limitations

This is a cosmetic bug on OSX and AMP Connectors installed on OSV-10.4.X and connector version 1.11.0. The AMP portal shows a Fault message for FDA and the host shows FDA is allowed.
BugID: CSCvq98799

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

When a request is made to load a KEXT, but not yet approved, the load request is denied. MacOS High Sierra 10.13 introduces a new feature, which means the user requires approval before loading newly-installed third-party kernel extensions (KEXTs) and only kernel extensions approved are loaded on a system. The user needs to follow the steps mentioned before to solve the Kernel error.
Since macOS 10.14 (Mojave) introduces new security features that affect AMP for Endpoints Mac Connectors, you require to ensure Full Disk Access is granted to the AMP service daemon, without approval, the AMP Connector is unable to provide protection or visibility to these parts of the file system being protected by macOS.

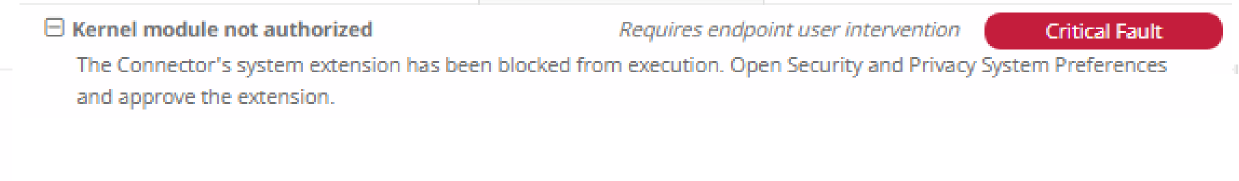
Troubleshoot

This section provides information you can use to troubleshoot your configuration.

Console errors

Kernel Fault

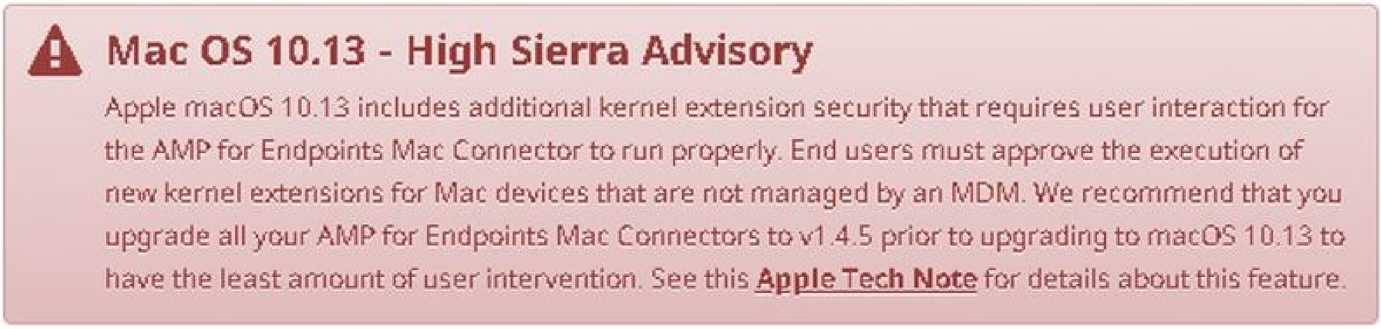
AMP Console shows the error “Kernel module not authorized” when a request is made to load a Kernel Extension (KEXT) and it is not approved, the load request is denied and macOS presents an alert, as shown in the image.



⊟ **Kernel module not authorized** *Requires endpoint user intervention* Critical Fault

The Connector's system extension has been blocked from execution. Open Security and Privacy System Preferences and approve the extension.

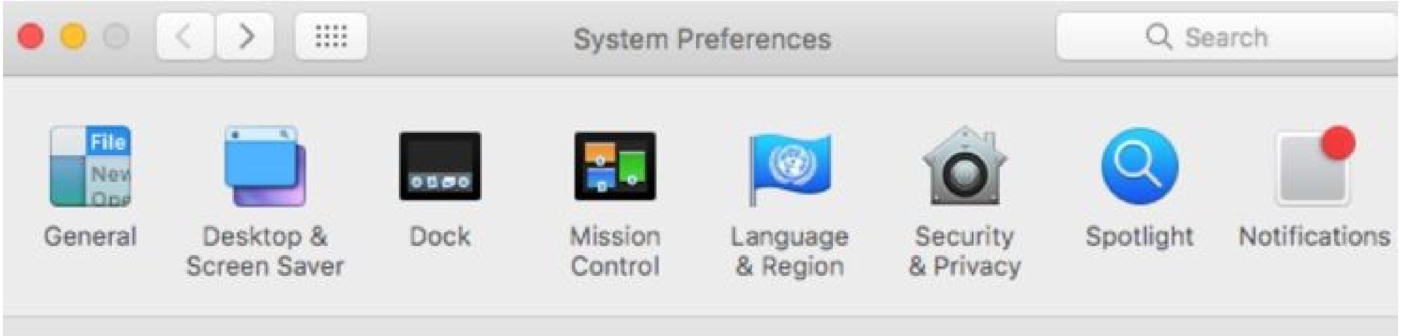
After the Apple macOS upgrade, an official announcement was launched about the kernel approval, as shown in the image.

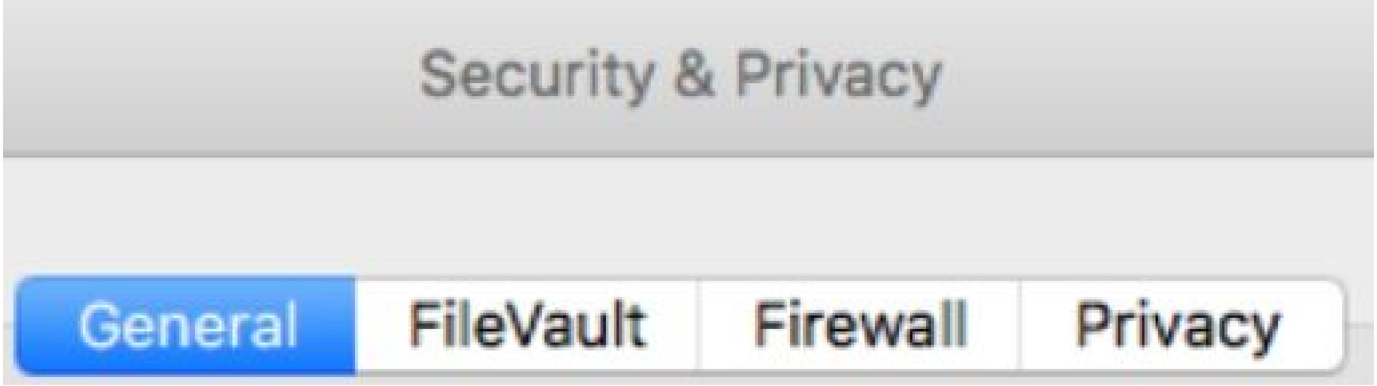


Mac OS 10.13 - High Sierra Advisory

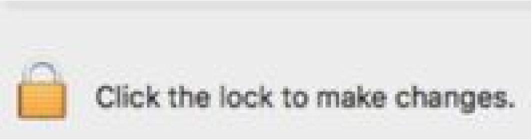
Apple macOS 10.13 includes additional kernel extension security that requires user interaction for the AMP for Endpoints Mac Connector to run properly. End users must approve the execution of new kernel extensions for Mac devices that are not managed by an MDM. We recommend that you upgrade all your AMP for Endpoints Mac Connectors to v1.4.5 prior to upgrading to macOS 10.13 to have the least amount of user intervention. See this Apple Tech Note for details about this feature.

In order to allow the Connector extension, navigate to **System Preferences > Security & Privacy > General** as shown in the image.





Click on the Lock to approve the KEXT (Only kernel extensions approved by the user are loaded on a system), as shown in the image.

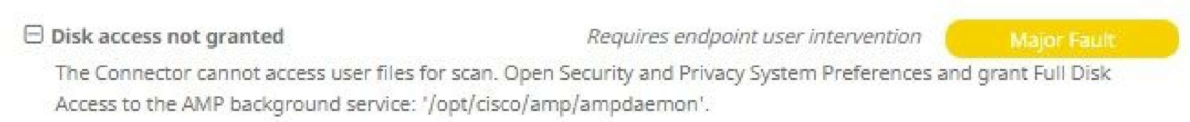


Click the lock to make changes.

> **Note**: The user approval is presented in the Security & Privacy preferences pane for 30 minutes after the alert. When the KEXT is approved future load attempts cause the approval user interface to reappear but it does not trigger another user alert.

Full Disk Access Fault

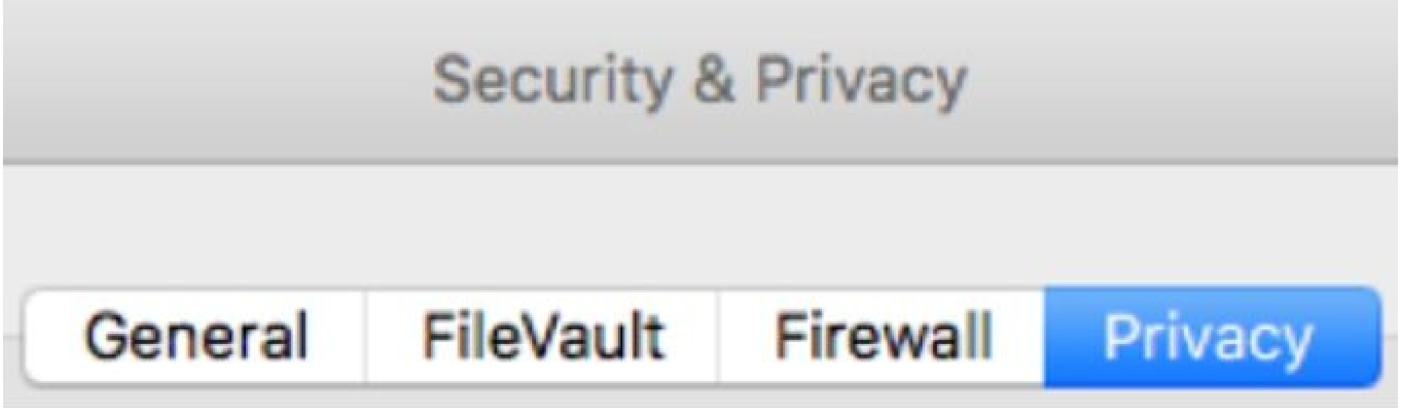
AMP console shows “Disk Access not granted” as shown in the image.



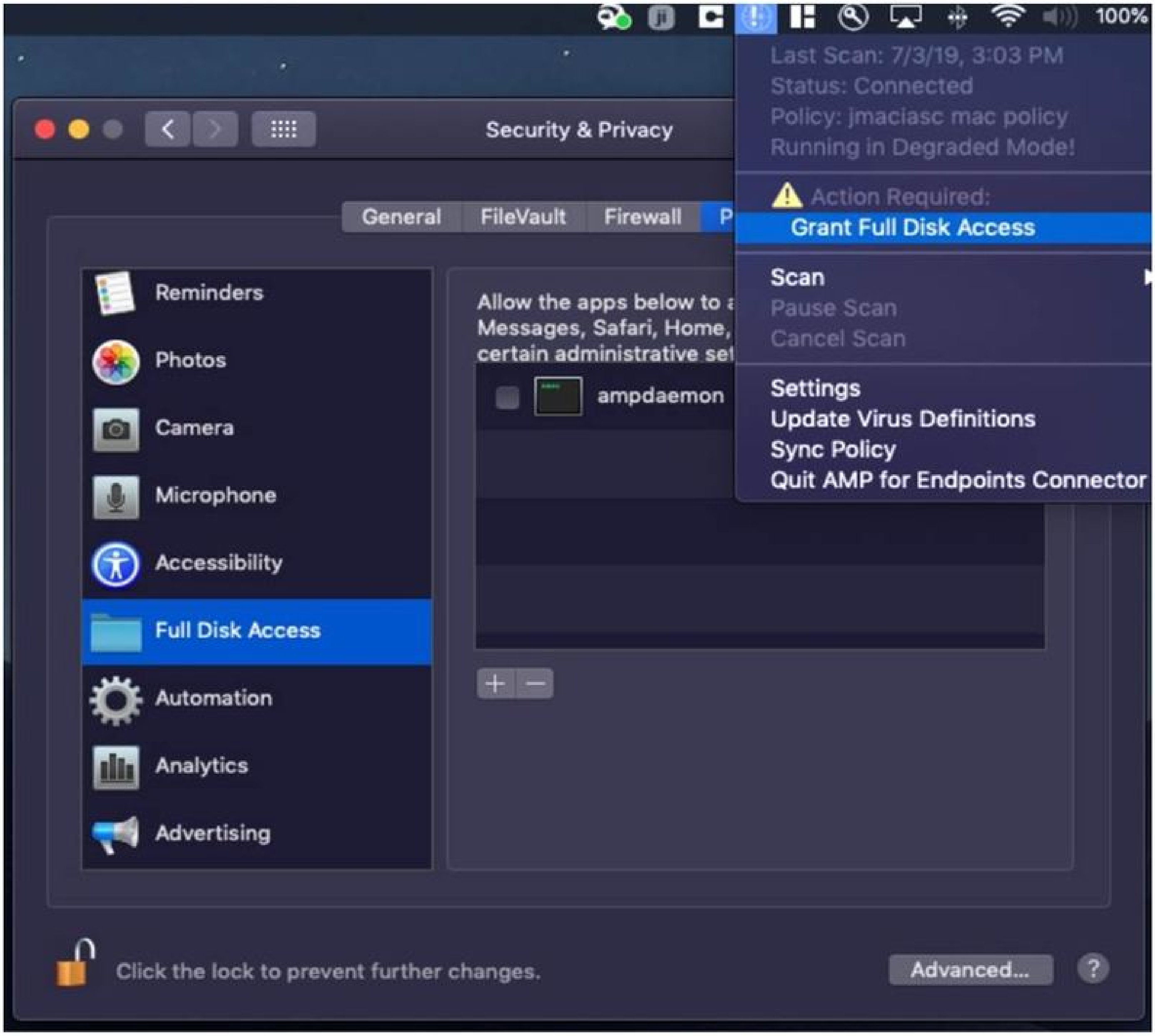
⊟ Disk access not granted *Requires endpoint user intervention* Major Fault

The Connector cannot access user files for scan. Open Security and Privacy System Preferences and grant Full Disk Access to the AMP background service: '/opt/cisco/amp/ampdaemon'.

Verify Full Disk access is not allowed, navigate to **System Preferences > Security & Privacy > Privacy,** as shown in the image.



In order to approve Ful disk access of the AMP connector, navigate to Full Disk Access and checkmark the ampdaemon process, as shown in the image.



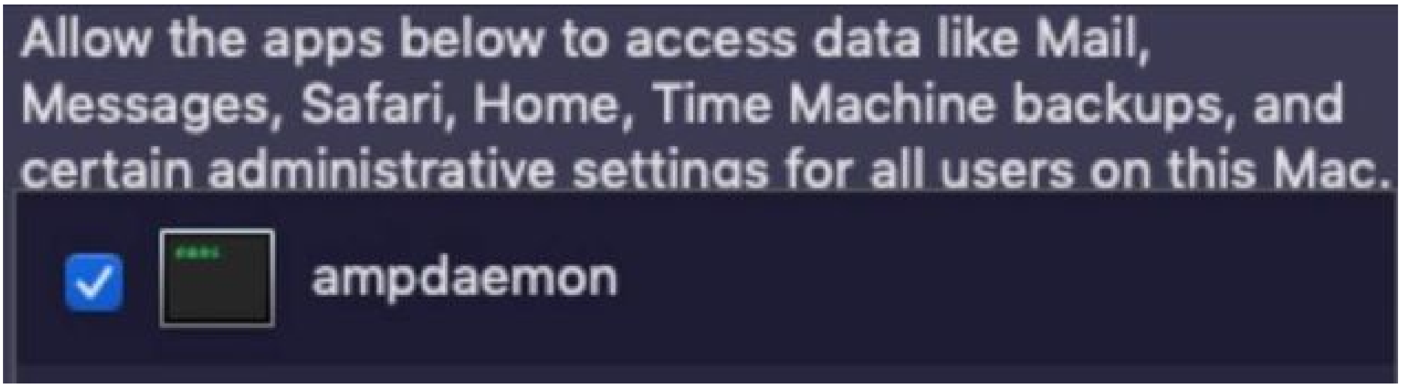
Last Scan: 7/3/19, 3:03 PM
Status: Connected
Policy: jmaciasc mac policy
Running in Degraded Mode!

Action Required:
Grant Full Disk Access

Allow the apps below to a
Messages, Safari, Home,
certain administrative set

Click the lock to prevent further changes.

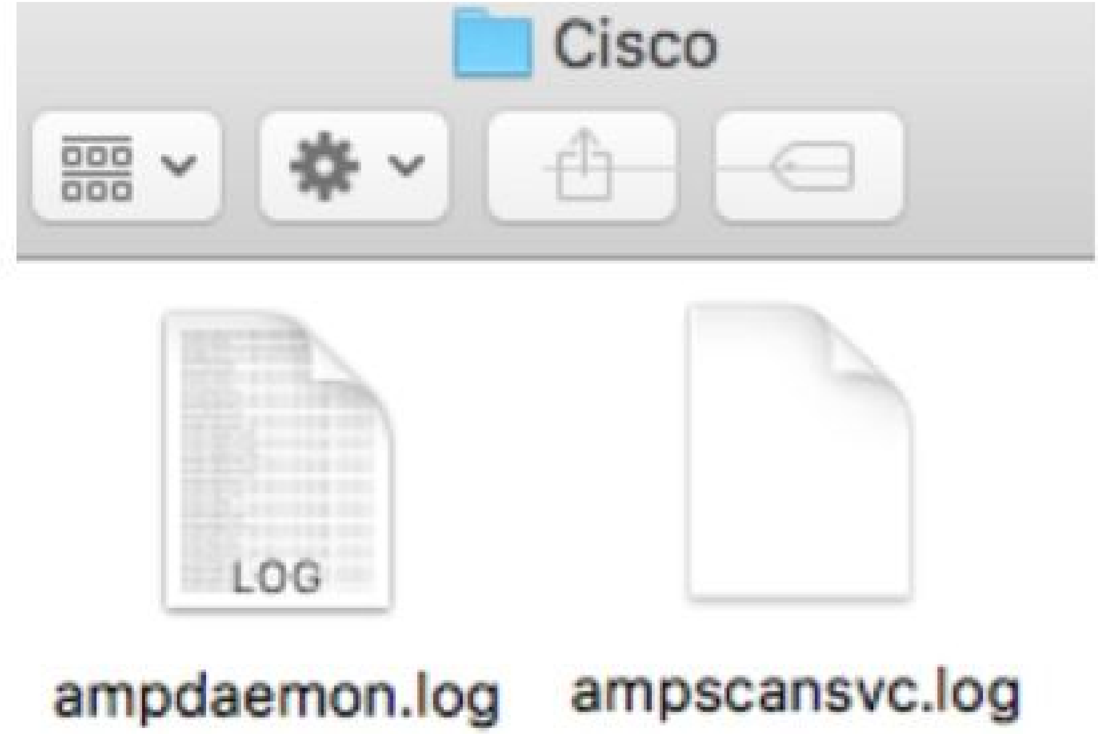
Open a terminal and stop the AMP service and run the next command: **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** mark the checkbox, as shown in the image.



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.

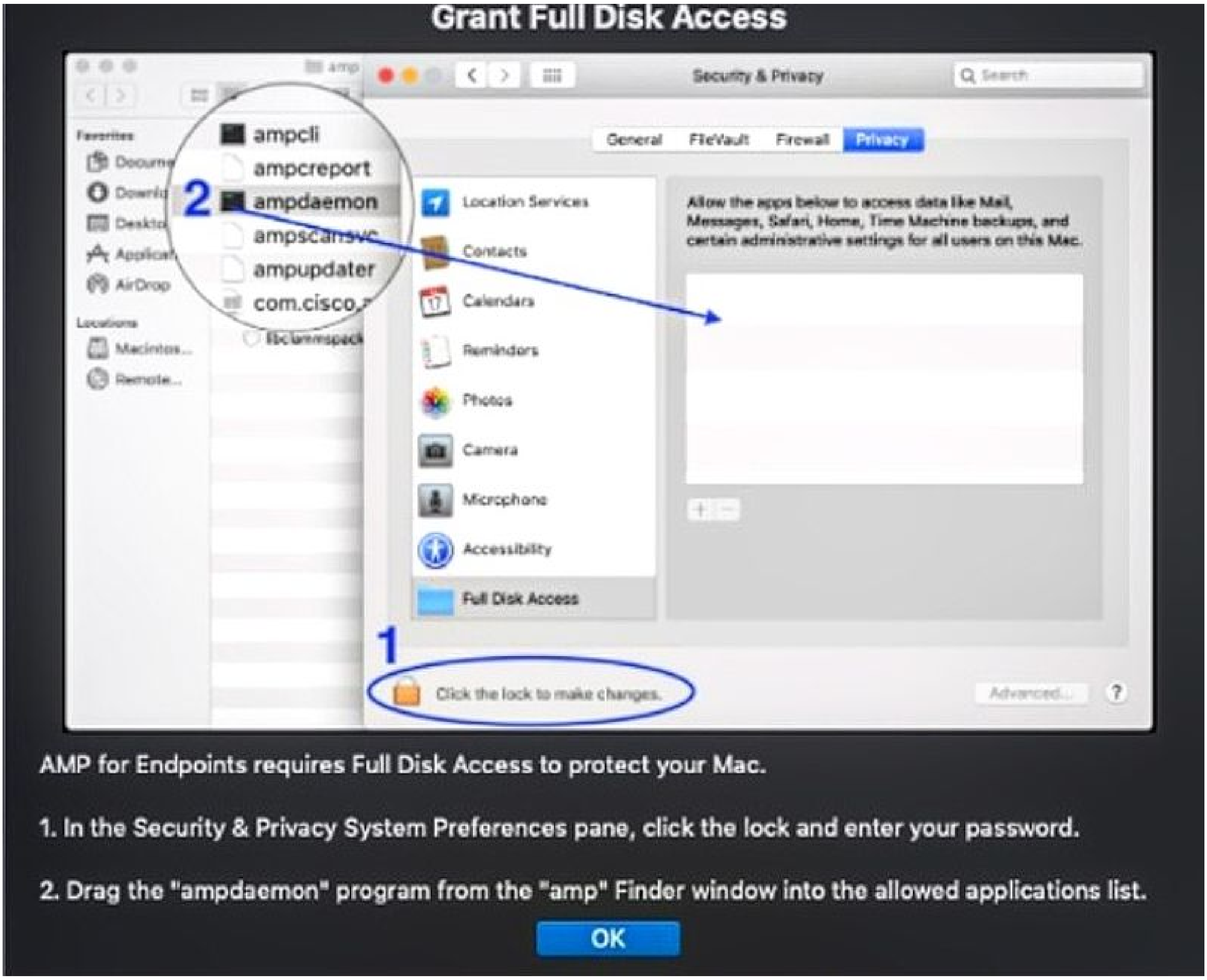
In order to avoid cache issues, navigate to **/library/logs/cisco** and erase the next files, as shown in the image.

- ampdaemon.log
- ampscansvc.log



Start the service with the command: **sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

> **Note**: In case you can’t find the ampdeamon file, drag & drop it into the allow Full Disk Access list, ensure that the checkbox is marked, as shown in the image.



Grant Full Disk Access

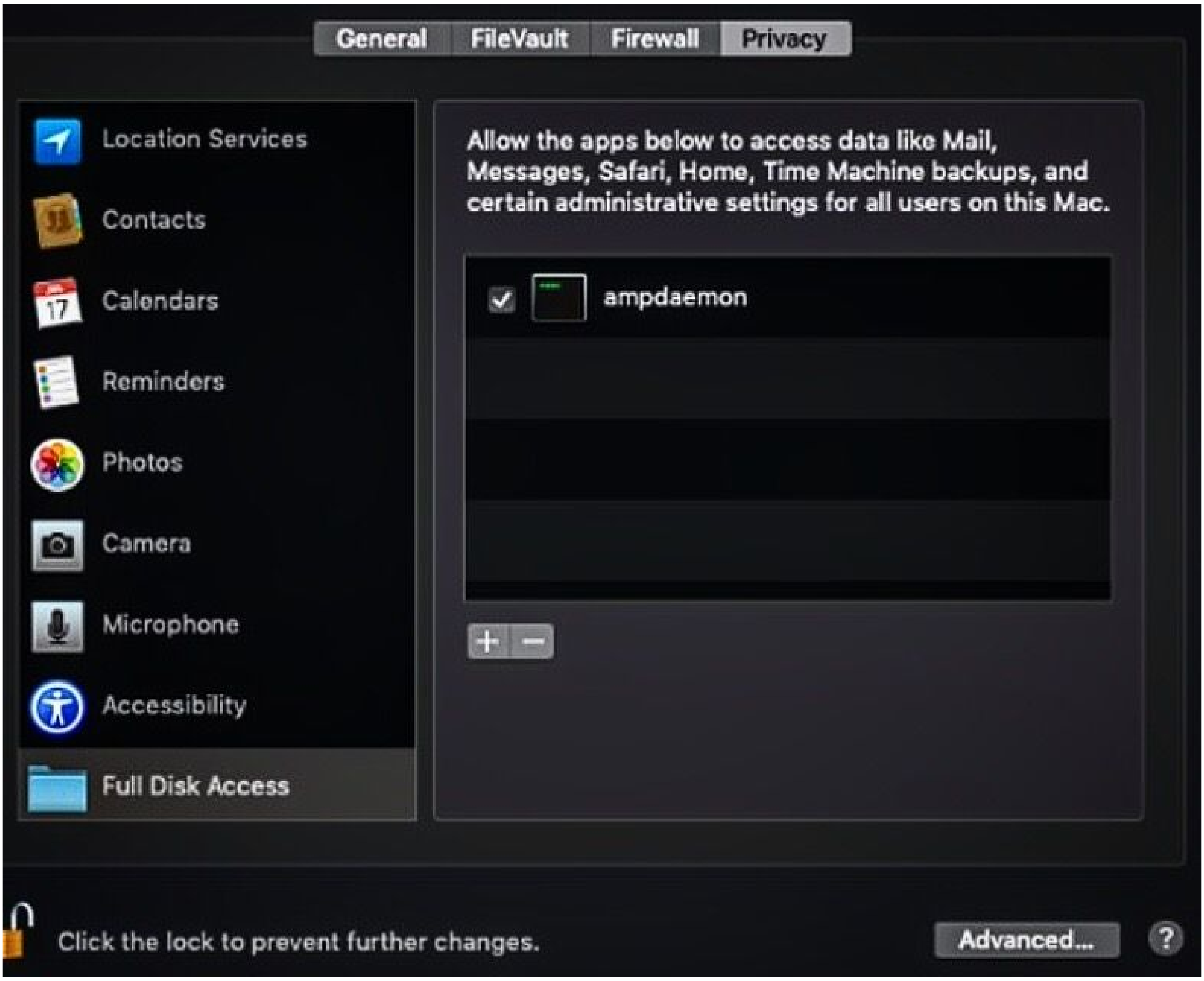
Allow the apps below to access data like Mail, Messages, Safari, Home, Time Machine backups, and certain administrative settings for all users on this Mac.

Click the lock to make changes.

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.



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.

☑ ampdaemon

Click the lock to prevent further changes.

In order to grant full disk Access, give the Kernels permissions and a recommended reboot of the MAC devices, in the next heartbeat interval the reported message disappears from the console.