MAC Kernel en Full Disk Access in console - AMP voor endpoints

Inhoud

Inleiding

Dit document beschrijft de stappen naar probleemoplossing in Advanced Malware Protection (AMP) voor endpoints om twee Mac-fouten te werken: Full Disk Access (FDA) en Kernel-module is niet toegestaan.

Bijgedragen door Uriel Torres, Javier Jesus Martinez, Cisco TAC-ingenieurs.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- kennis over Mac
- Account met Administrator-rechten

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Advanced Malware Protection voor endpoints voor MAC.

De informatie in dit document is afkomstig van de apparatuur in een specifieke omgeving:

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Beperkingen

Dit is een cosmetische bug op OSX- en AMP-connectors die op OSV-10.4.X is geïnstalleerd en op connector versie 1.11.0. Het AMP-portaal geeft een foutbericht voor FDA en de host toont dat FDA is toegestaan.
BugID: CSCvq98799

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk levend is, zorg er dan voor dat u de mogelijke impact van om het even welke opdracht begrijpt.

Achtergrondinformatie

Wanneer een aanvraag is ingediend om een KEXT-document te laden, maar nog niet is goedgekeurd, wordt de aanvraag voor het laden afgewezen. MacOS High Sierra 10.13 introduceert een nieuwe optie, wat betekent dat de gebruiker goedkeuring vereist voordat hij de nieuw geïnstalleerde kernelextensies (KEXT's) van derden laadt en alleen de goedgekeurde kernelextensies op een systeem worden geladen. De gebruiker moet de eerder genoemde stappen volgen om de Kernel-fout op te lossen.
Aangezien macOS 10.14 (Mojave) nieuwe beveiligingsfuncties invoert die AMP voor Endpoints Mac Connectors beïnvloeden, dient u er zeker van te zijn dat de volledige Disk Access wordt verleend aan de AMP-servicedag zonder goedkeuring, kan de AMP-connector geen bescherming of zichtbaarheid bieden aan deze delen van het bestandssysteem die door macOS worden beschermd.

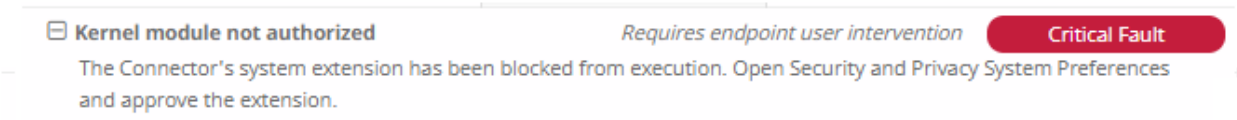
Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

Console-fouten

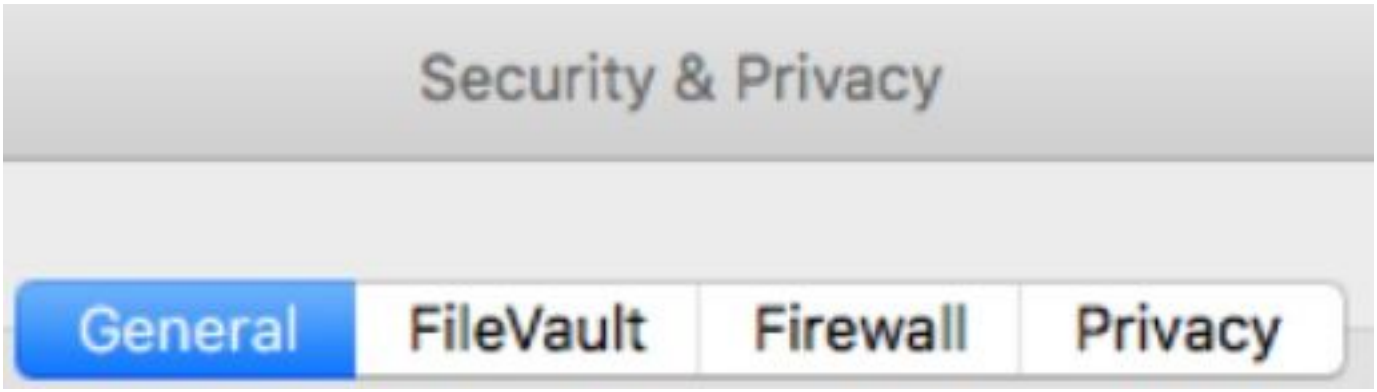
Kernel Fault

AMP Console laat de fout zien "Geen geautoriseerde module" wanneer een verzoek wordt ingediend om een Kernel Extension (KEXT) te laden en deze niet is goedgekeurd, wordt het verzoek om belasting afgewezen en meldt macOS een waarschuwing, zoals in de afbeelding wordt weergegeven.

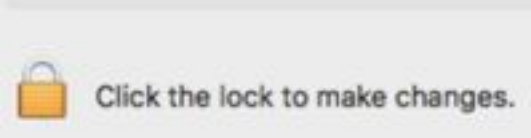


Na de upgrade van Apple was er een officiële aankondiging over de goedkeuring van de tunnel, zoals in de afbeelding te zien is.

Raadpleeg voor de connector-extensie **systeemvoorkeuren > Security & Privacy > General** zoals in de afbeelding.



Klik op in het slot om de KEXT goed te keuren (alleen de kanaaluitbreidingen die door de gebruiker zijn goedgekeurd, worden op een systeem geladen), zoals in de afbeelding weergegeven wordt.

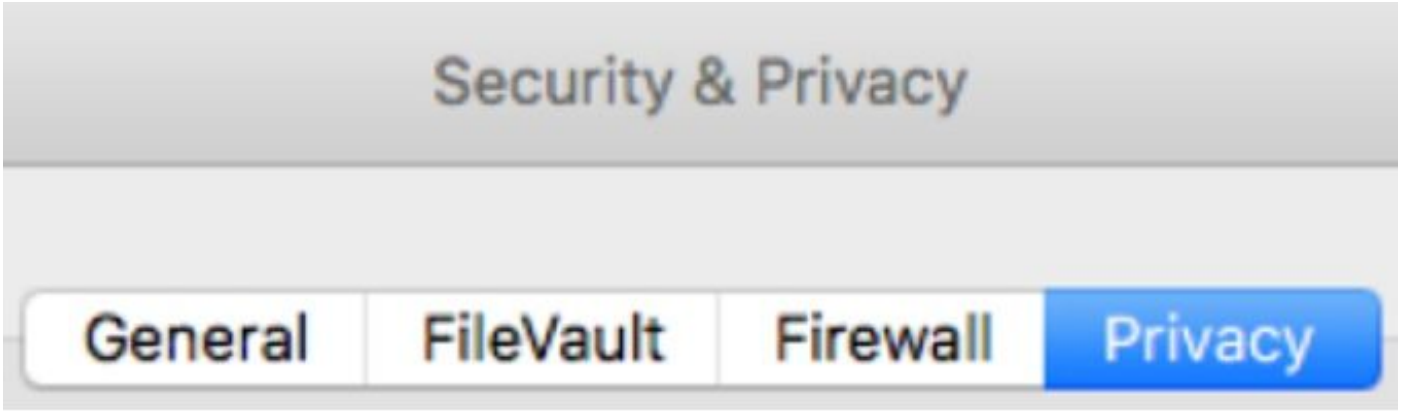


Opmerking: de gebruikersgoedkeuring wordt gedurende 30 minuten na de melding in het venster Security & Privacy prefab weergegeven. Wanneer de KEXT is goedgekeurd, probeert u de gebruikersinterface van de goedkeuring opnieuw te laten verschijnen, maar er wordt geen ander gebruikersalarm geactiveerd.

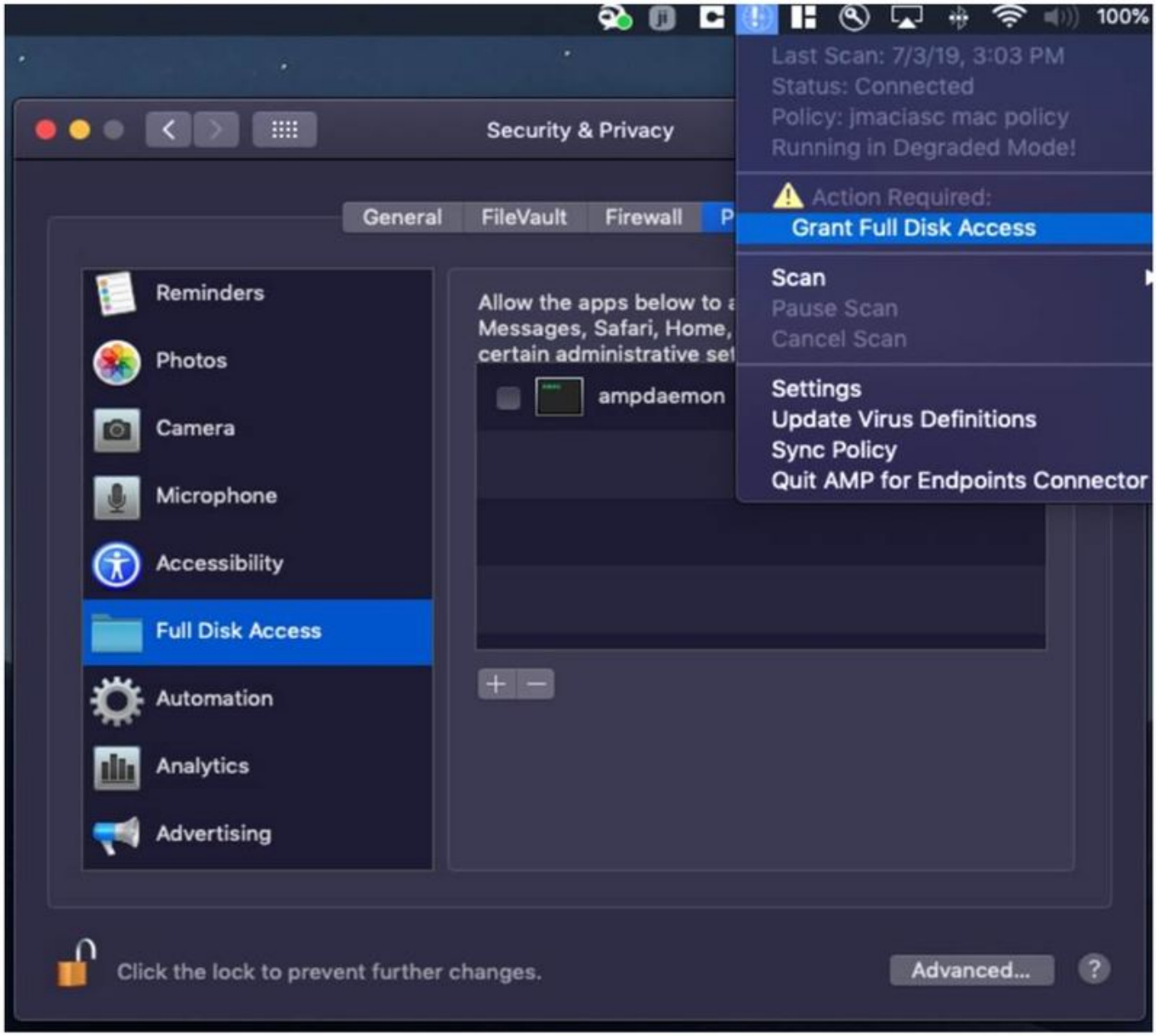
Volledig schijf-toegangsfout

AMP-console toont "Disk Access not Grant" zoals in de afbeelding wordt getoond.

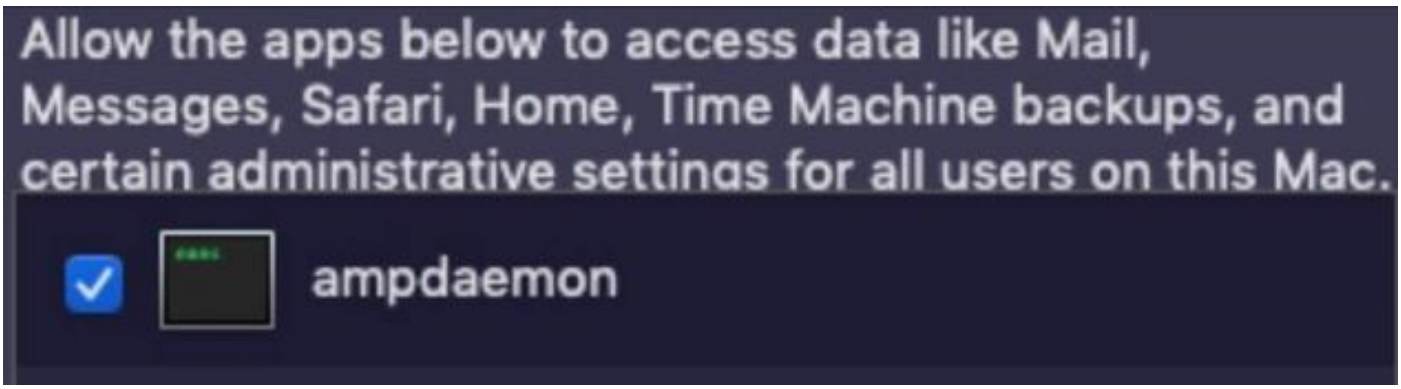
Controleer of de volledige toegang tot de schijf niet is toegestaan, navigeer dan naar **systeemvoorkeuren > Beveiliging en Privacy > Privacy,** zoals in de afbeelding getoond.



Om de volledige toegang tot de schijf van de AMP-connector goed te keuren, navigeer naar de Full Disk Access en controleer het ampdaemonproces, zoals in de afbeelding wordt getoond.

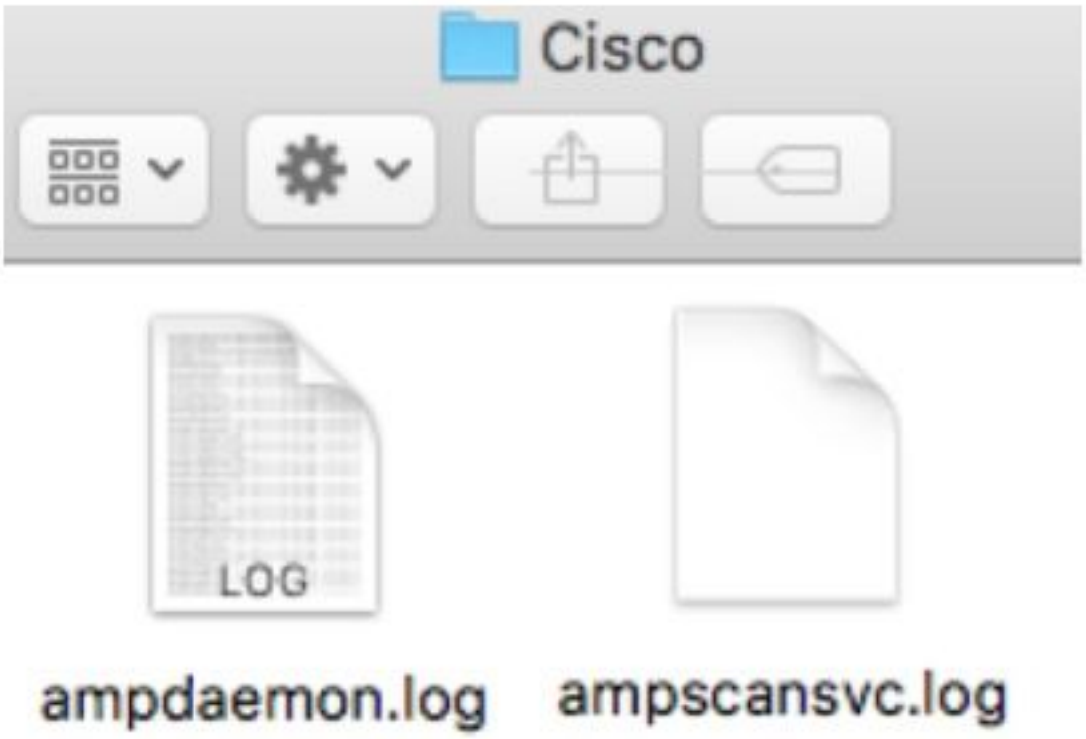


Open een terminal en stop de AMP-service en voer de volgende opdracht uit: **sudo/bin/lancering lossen /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** vinkt het selectieteken aan, zoals in de afbeelding wordt getoond.



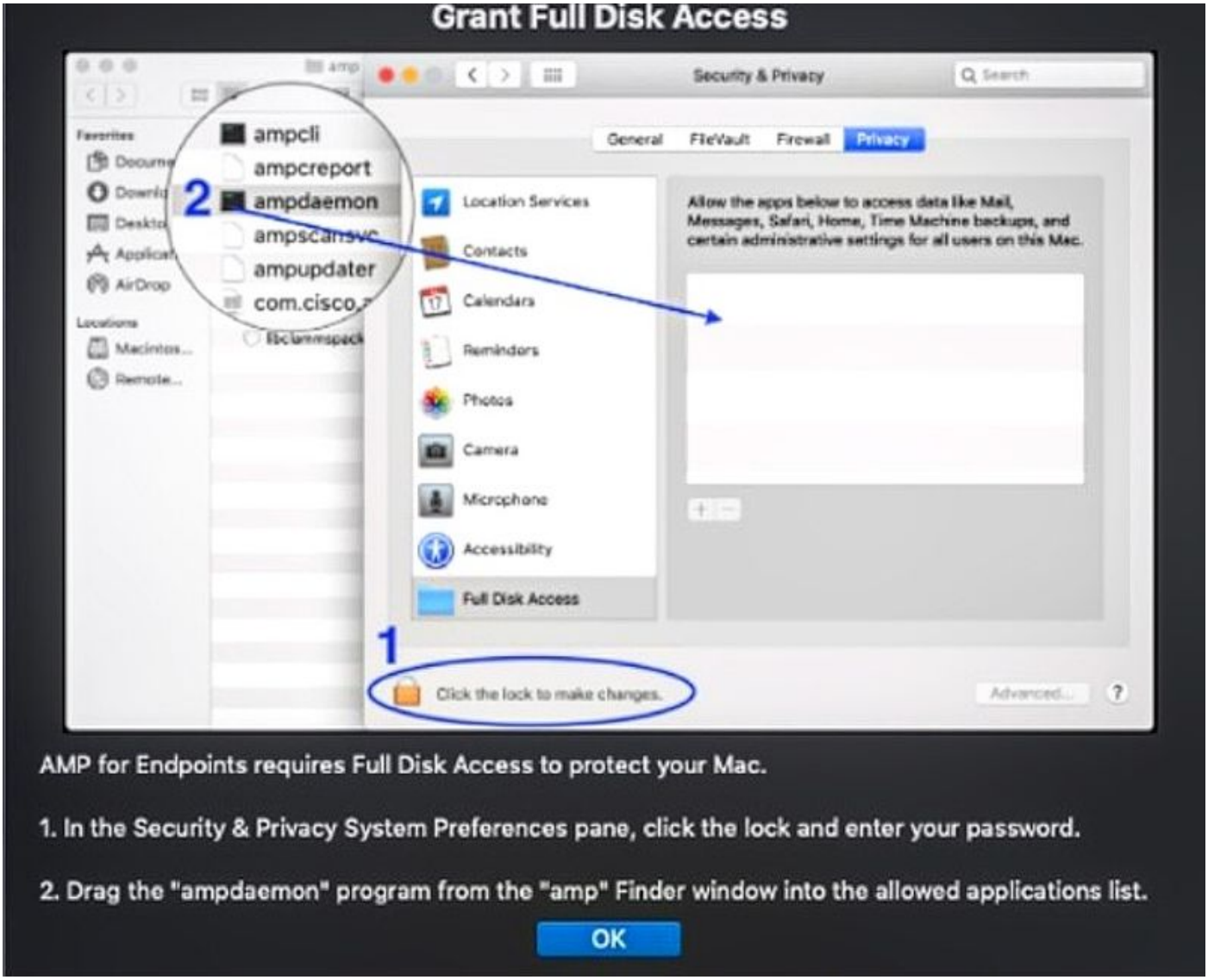
Om cacheproblemen te voorkomen, navigeer dan naar **/bibliotheek/logs/cisco** en verwijder de volgende bestanden, zoals in de afbeelding.

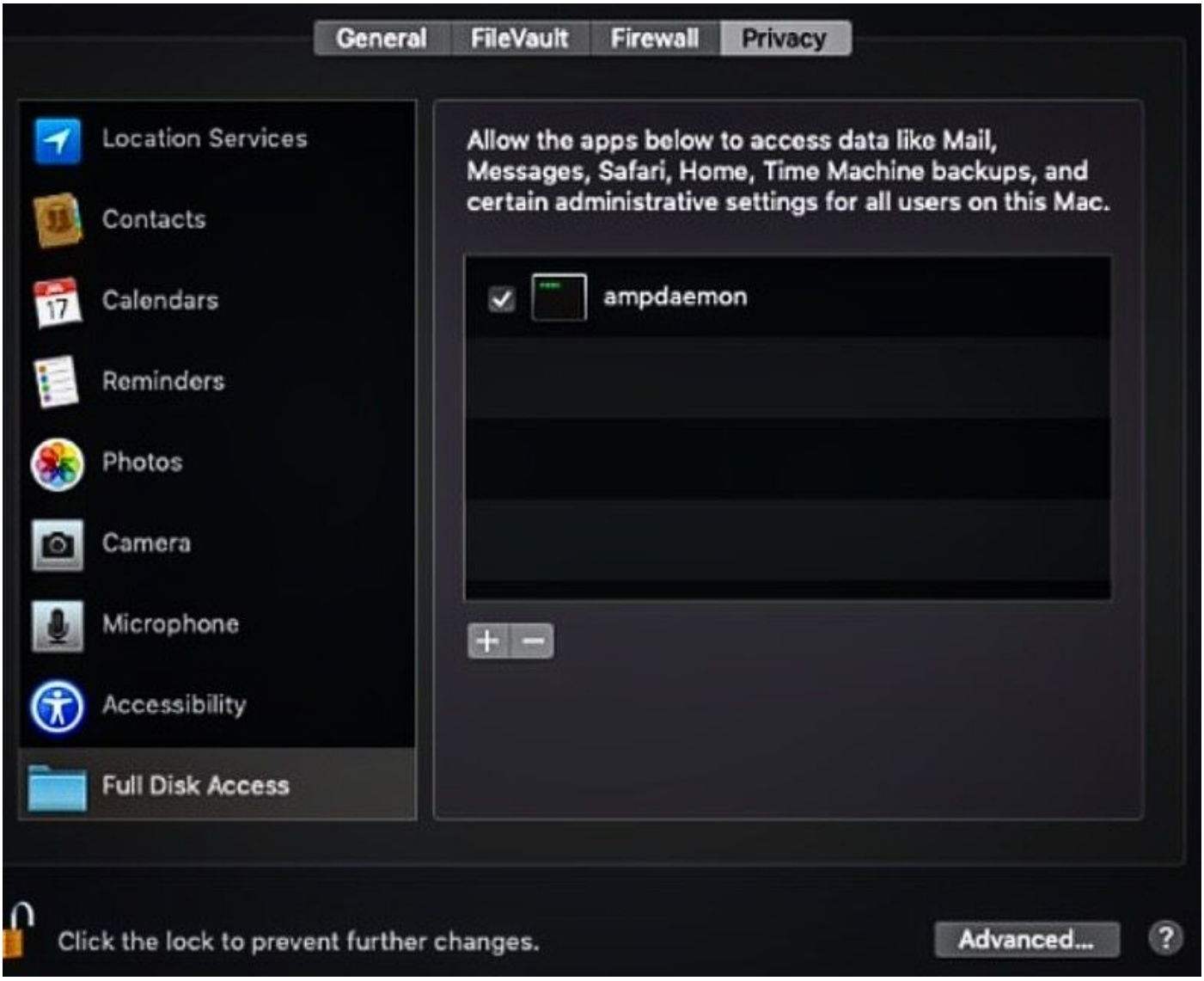
- ampdaemon.log
- ampscansvc.log



Start de service met behulp van de opdracht: **sudo/bin/wash load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

Opmerking: Mocht u het ampèrebestand niet vinden, sleep het dan in de lijst Full Disk Access, zorg er dan voor dat het selectieteken gemarkeerd is zoals in de afbeelding.


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



Om volledige schijftoegang te verlenen, geef de Kernels toestemmingen en een aanbevolen herstart van de apparaten van MAC, in het volgende hartslag interval het gerapporteerde bericht van de console weg.