Núcleo MAC y acceso completo al disco en la consola - AMP para terminales

Contenido

Introducción

Este documento describe los pasos para resolver problemas de protección frente a malware avanzado (AMP) para que los terminales funcionen con dos fallos de Mac: No están autorizados el acceso completo al disco (FDA) y el módulo del núcleo.

Colaborado por Uriel Torres, Javier Jesus Martinez, Ingenieros del TAC de Cisco.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

Conocimiento de herramientas · Mac
Cuenta · con privilegios de administrador

Componentes Utilizados

La información de este documento se basa en Cisco AMP para terminales para MAC.

La información de este documento se creó a partir de los dispositivos en un entorno específico:

- MacOS High Sierra 10.13

- MacOS 10.14 (Mojave)

Limitaciones

Este es un error cosmético en los conectores OSX y AMP instalados en OSV-10.4.X y en la versión 1.11.0 del conector. El portal de AMP muestra un mensaje de error para la FDA y el host muestra que la FDA está permitida.
ID de error: 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. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cuando se realiza una solicitud para cargar un KEXT, pero aún no se ha aprobado, se rechaza la solicitud de carga. MacOS High Sierra 10.13 introduce una nueva función, lo que significa que el usuario necesita aprobación antes de cargar las recién instaladas extensiones de kernel de terceros (KEXT) y solamente las extensiones de kernel aprobadas se cargan en un sistema. El usuario debe seguir los pasos mencionados anteriormente para resolver el error Kernel.
Dado que macOS 10.14 (Mojave) introduce nuevas funciones de seguridad que afectan a los conectores Mac de AMP para terminales, debe asegurarse de que se concede acceso de disco completo al demonio de servicio de AMP, sin aprobación, el conector de AMP no puede proporcionar protección ni visibilidad a estas partes del sistema de archivos protegido por macOS.

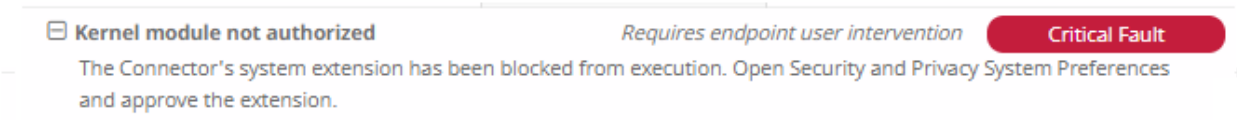
Troubleshoot

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Errores de consola

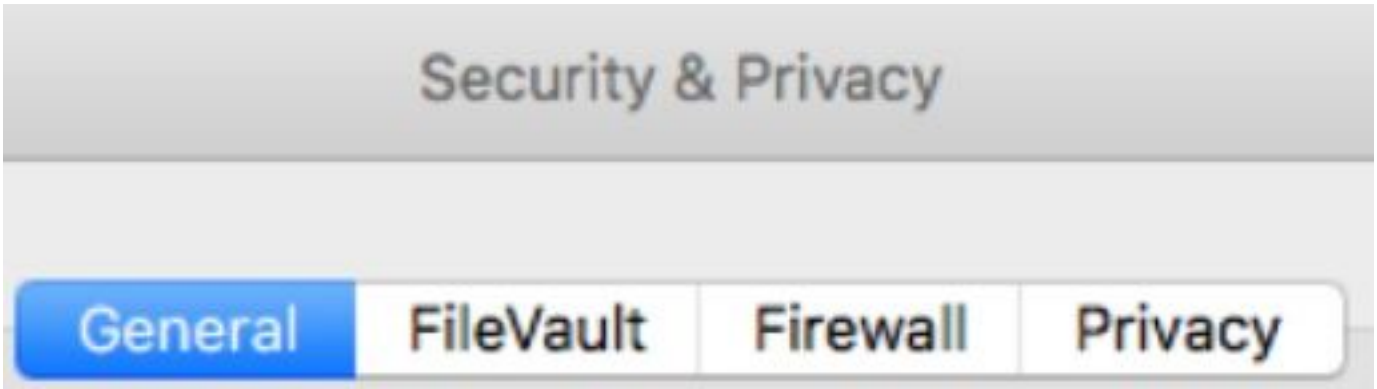
Falla del núcleo

La consola de AMP muestra el error "Módulo del núcleo no autorizado" cuando se realiza una solicitud para cargar una extensión del núcleo (KEXT) y no está aprobada, la solicitud de carga es denegada y macOS presenta una alerta, como se muestra en la imagen.

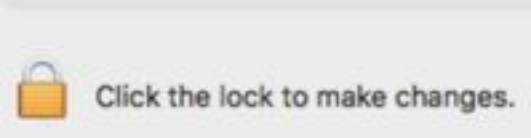


Después de la actualización de Apple MacOS, se lanzó un anuncio oficial sobre la aprobación del núcleo, como se muestra en la imagen.

Para permitir la extensión del conector, navegue hasta **Preferencias del sistema > Seguridad y privacidad > General** como se muestra en la imagen.



Haga clic en Bloquear para aprobar el KEXT (sólo las extensiones del núcleo aprobadas por el usuario se cargan en un sistema), como se muestra en la imagen.

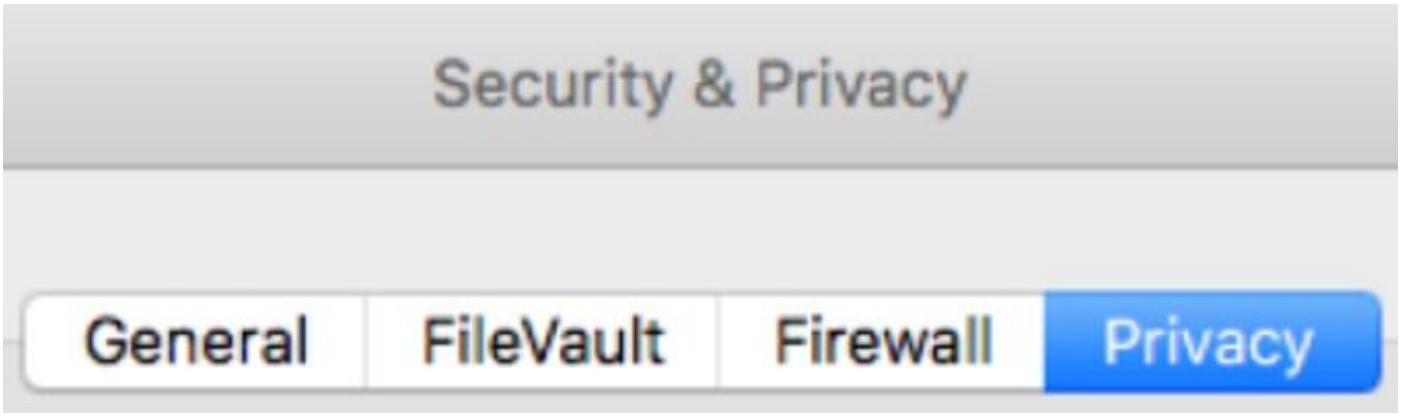


Nota: La aprobación del usuario se presenta en el panel Preferencias de seguridad y privacidad durante 30 minutos después de la alerta. Cuando se aprueba el KEXT, los futuros intentos de carga hacen que la interfaz de usuario de aprobación vuelva a aparecer, pero no activa otra alerta de usuario.

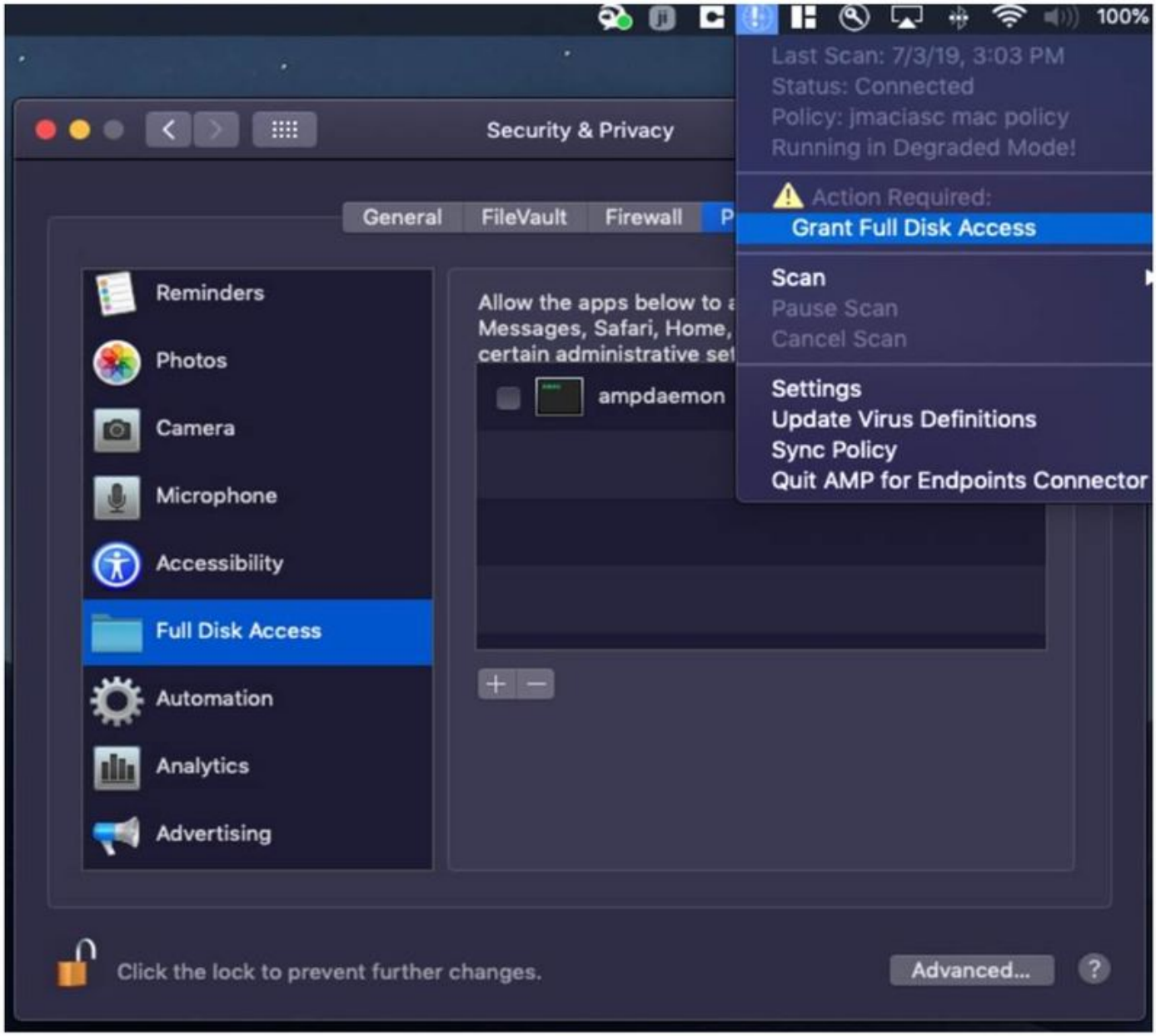
Falla de acceso al disco completo

La consola de AMP muestra "Disk Access not allowed" (El acceso al disco no se concede), como se muestra en la imagen.

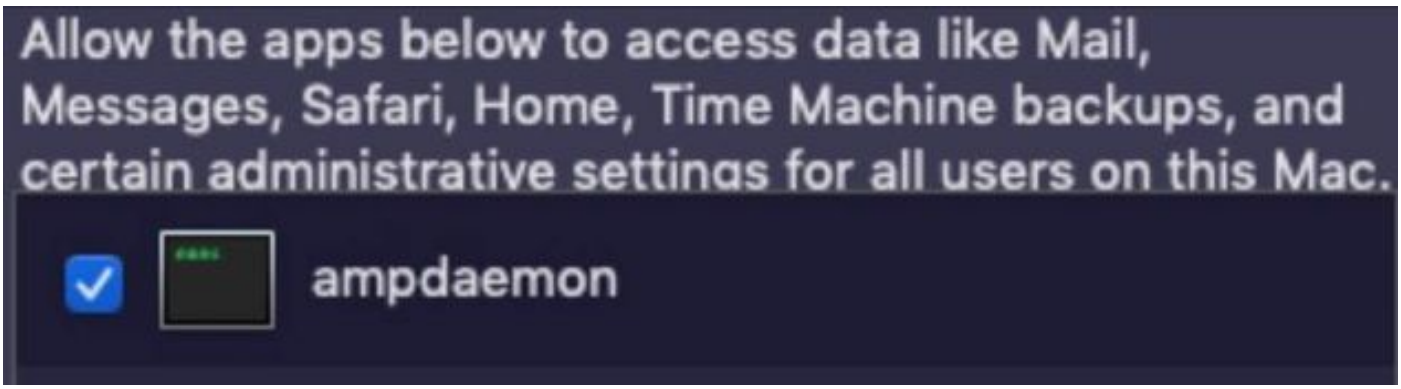
Verifique que no se permita el acceso completo al disco, navegue hasta **Preferencias del sistema > Seguridad y privacidad > Privacidad,** como se muestra en la imagen.



Para aprobar el acceso al disco completo del conector AMP, navegue hasta Acceso al disco completo y marque el proceso ampdaemon, como se muestra en la imagen.

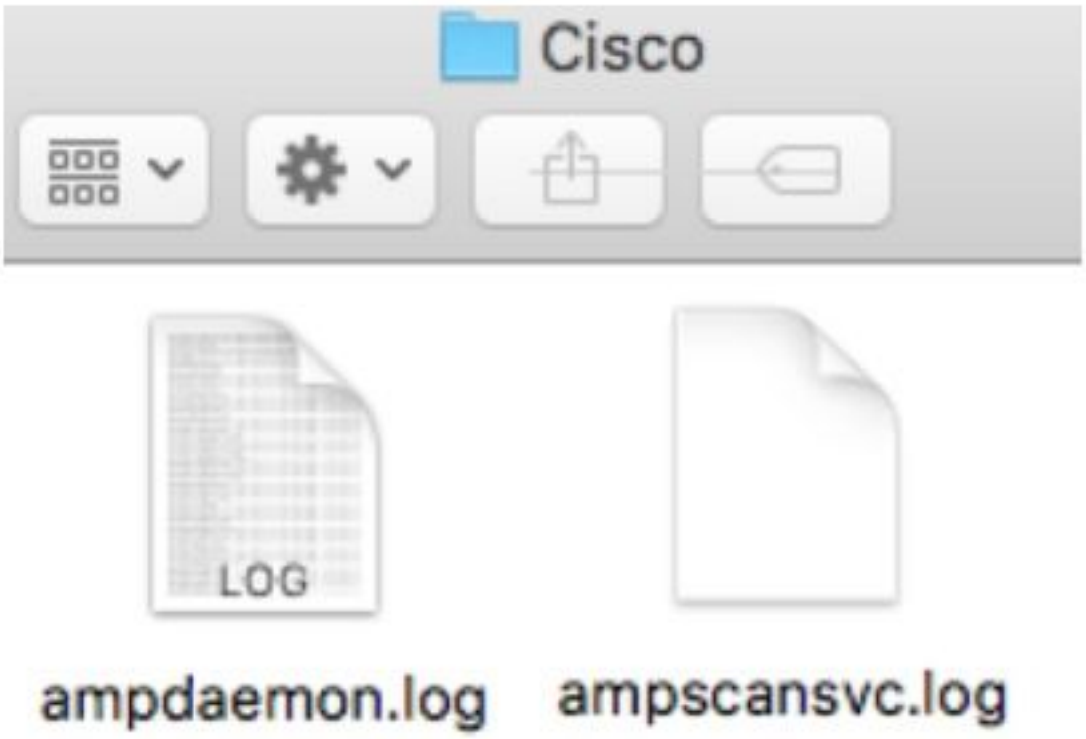


Abra un terminal y detenga el servicio AMP y ejecute el siguiente comando: **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** marque la casilla de verificación, como se muestra en la imagen.



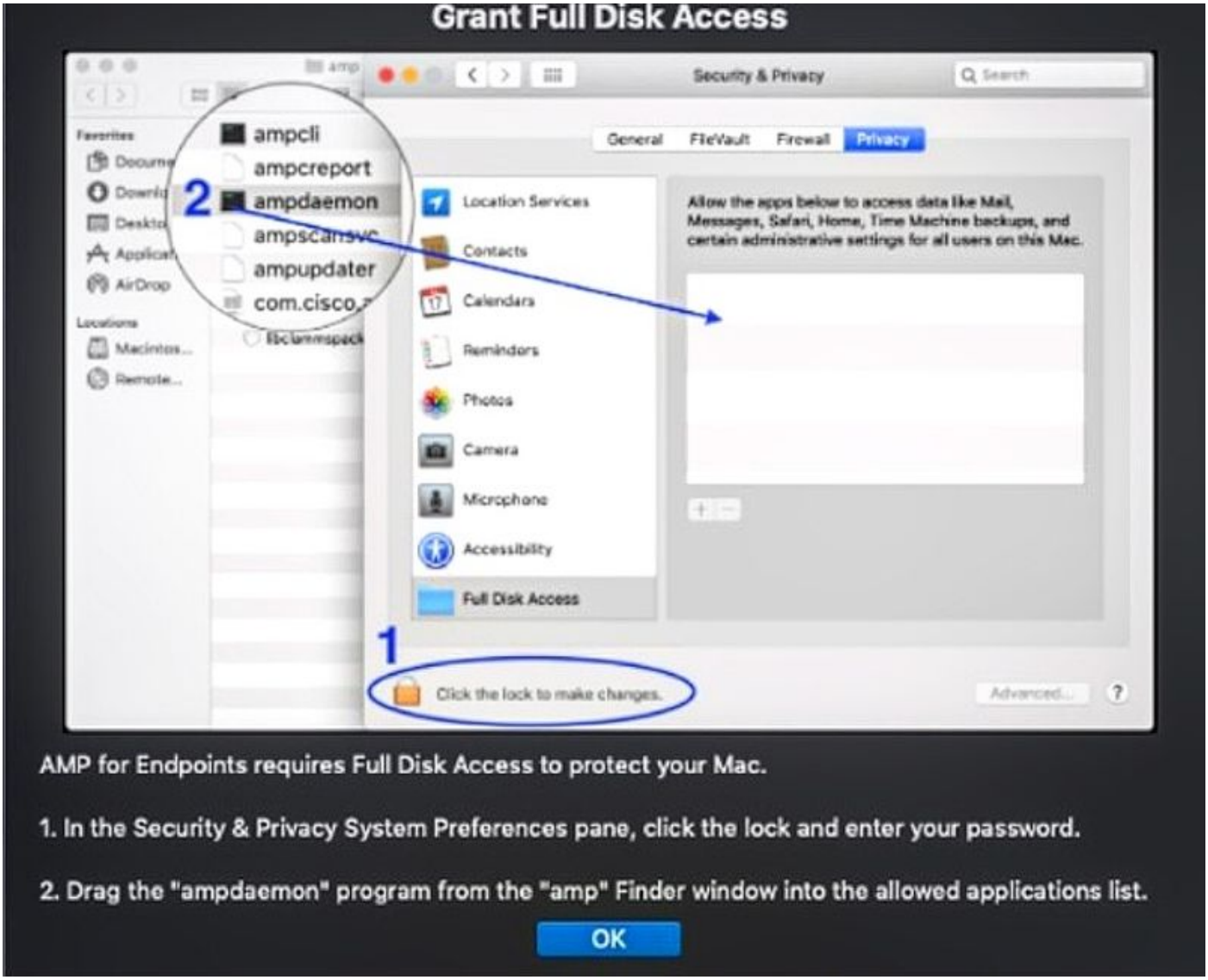
Para evitar problemas de caché, navegue hasta **/library/logs/cisco** y borre los siguientes archivos, como se muestra en la imagen.

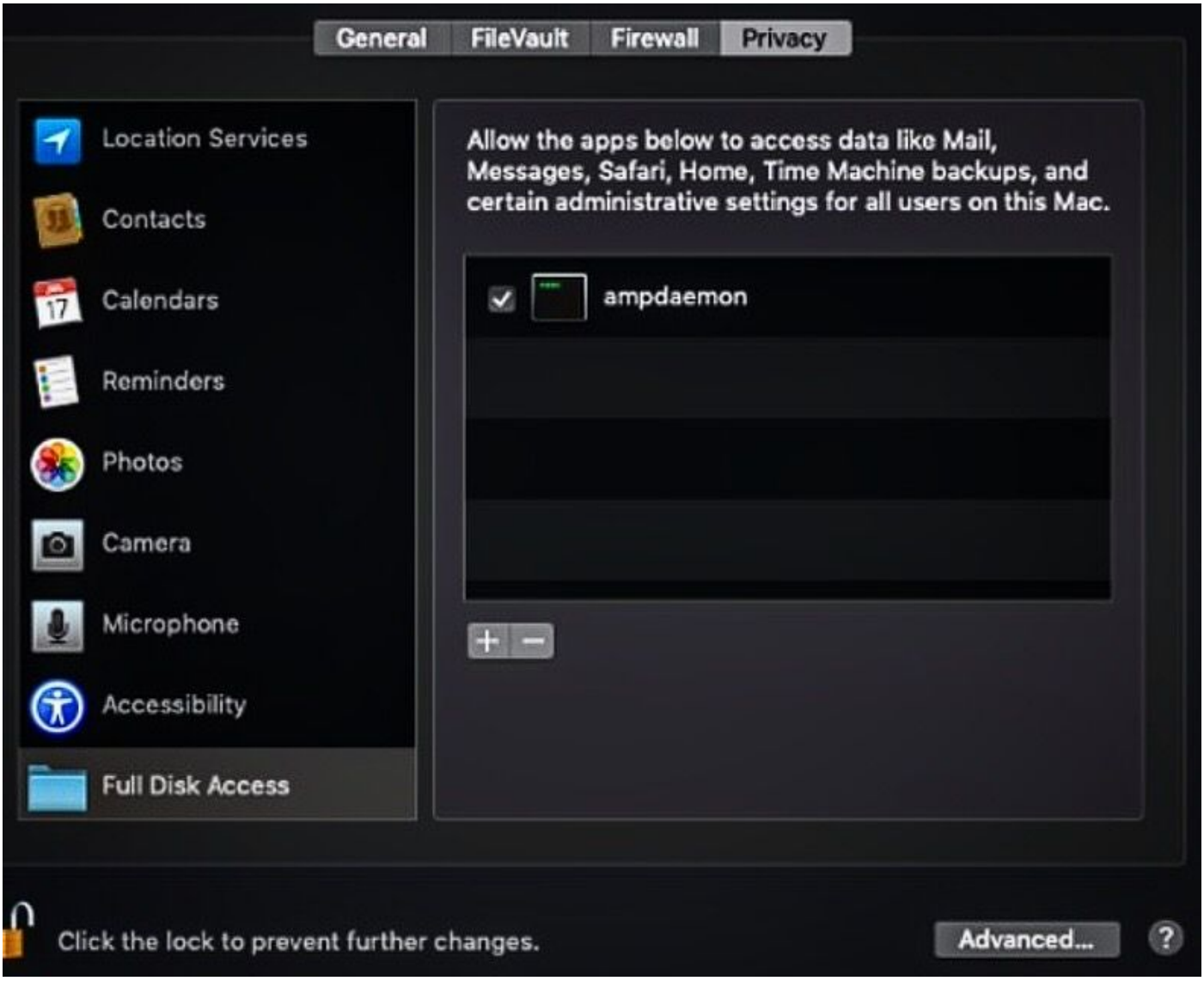
- ampdaemon.log
- ampscansvc.log



Inicie el servicio con el comando: **sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

> **Nota**: En caso de que no pueda encontrar el archivo de amantón, arrástrelo y suéltelo a la lista Permitir acceso al disco completo, asegúrese de que la casilla de verificación está marcada, como se muestra en la imagen.


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



Para conceder acceso completo al disco, otorgue a los Kernels permisos y un reinicio recomendado de los dispositivos MAC, en el siguiente intervalo de latido el mensaje informado desaparece de la consola.