Kernel MAC e acesso completo ao disco no console - AMP para endpoints

Contents

Introduction

Este documento descreve as etapas para solucionar problemas no AMP (Advanced Malware Protection, Proteção avançada contra malware) para endpoints para trabalhar com duas falhas Mac: FDA (Full Disk Access, acesso total ao disco) e módulo Kernel não autorizados.

Contribuído por Uriel Torres, Javier Jesus Martinez, engenheiro do TAC da Cisco.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

Conhecimento de ferramentas Mac
Conta com privilégios de administrador

Componentes Utilizados

As informações neste documento são baseadas no Cisco AMP para endpoints para MAC.

As informações neste documento foram criadas a partir dos dispositivos em um ambiente específico:

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Limitações

Este é um bug cosmético em conectores OSX e AMP instalados no OSV-10.4.X e no conector versão 1.11.0. O portal AMP mostra uma mensagem de falha para FDA e o host mostra que o FDA é permitido.
ID do bug: 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Quando uma solicitação é feita para carregar um KEXT, mas ainda não foi aprovada, a solicitação de carga é negada. O MacOS High Sierra 10.13 apresenta um novo recurso, o que significa que o usuário precisa de aprovação antes de carregar KEXTs (extensões de kernel de terceiros) recém-instaladas e que apenas as extensões de kernel aprovadas são carregadas em um sistema. O usuário precisa seguir as etapas mencionadas antes para resolver o erro de Kernel.
Como o macOS 10.14 (Mojave) introduz novos recursos de segurança que afetam o AMP para Endpoints Mac Connectors, você precisa garantir que o Acesso Total ao Disco seja concedido ao daemon de serviço da AMP, sem aprovação, o conector da AMP é incapaz de fornecer proteção ou visibilidade para essas partes do sistema de arquivos que estão sendo protegidas pelo macOS.

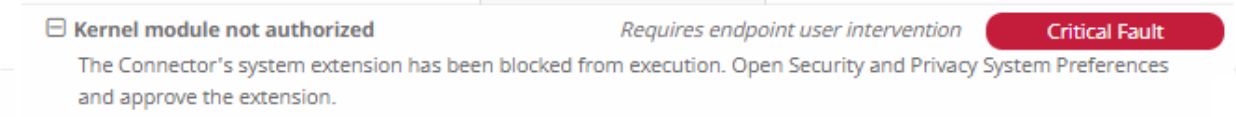
Troubleshoot

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Erros de console

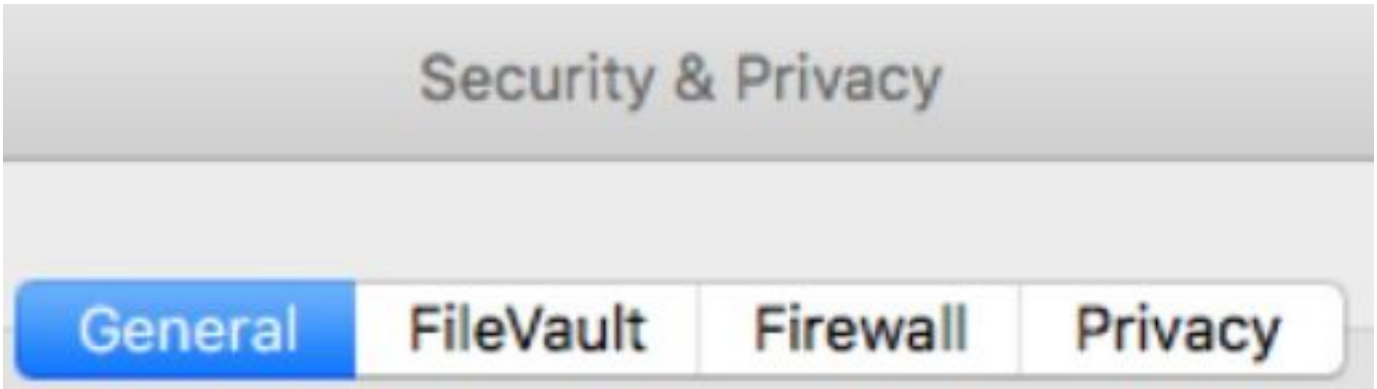
Falha de kernel

O console AMP mostra o erro "módulo Kernel não autorizado" quando uma solicitação é feita para carregar uma extensão Kernel (KEXT) e ela não é aprovada, a solicitação de carga é negada e macOS apresenta um alerta, como mostrado na imagem.

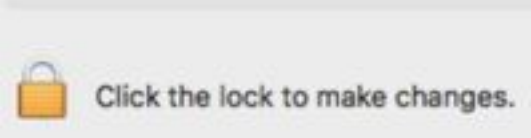


Após a atualização do Apple macOS, um anúncio oficial foi iniciado sobre a aprovação do kernel, como mostrado na imagem.

Para permitir a extensão do conector, navegue para **Preferências do sistema > Segurança e privacidade > Geral** como mostrado na imagem.



Clique no Bloqueio para aprovar o KEXT (somente as extensões de kernel aprovadas pelo usuário são carregadas em um sistema), como mostrado na imagem.

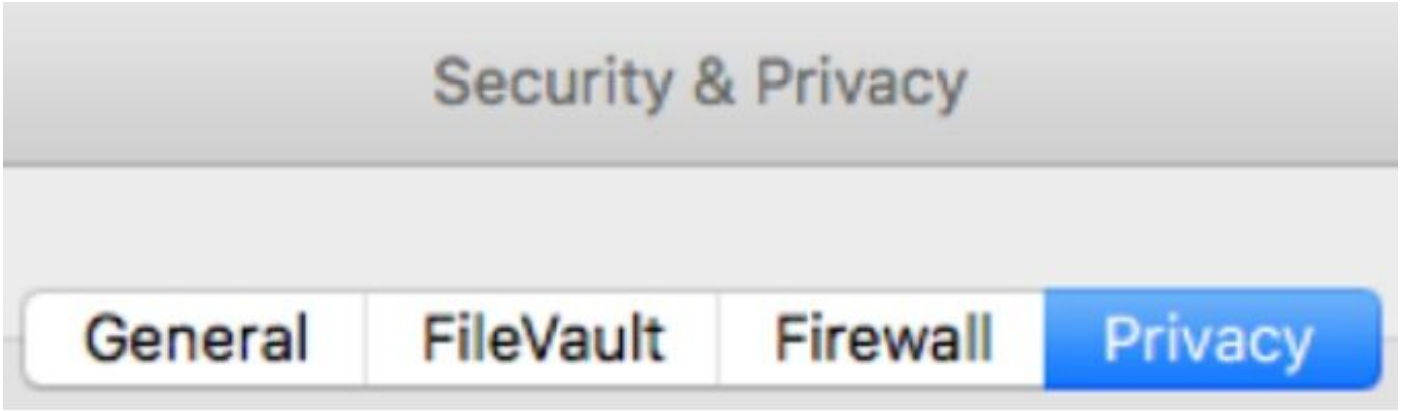


Observação: a aprovação do usuário é apresentada no painel de preferências de Segurança e privacidade por 30 minutos após o alerta. Quando o KEXT é aprovado, a carga futura tenta fazer com que a interface de usuário de aprovação reapareça, mas ela não aciona outro alerta de usuário.

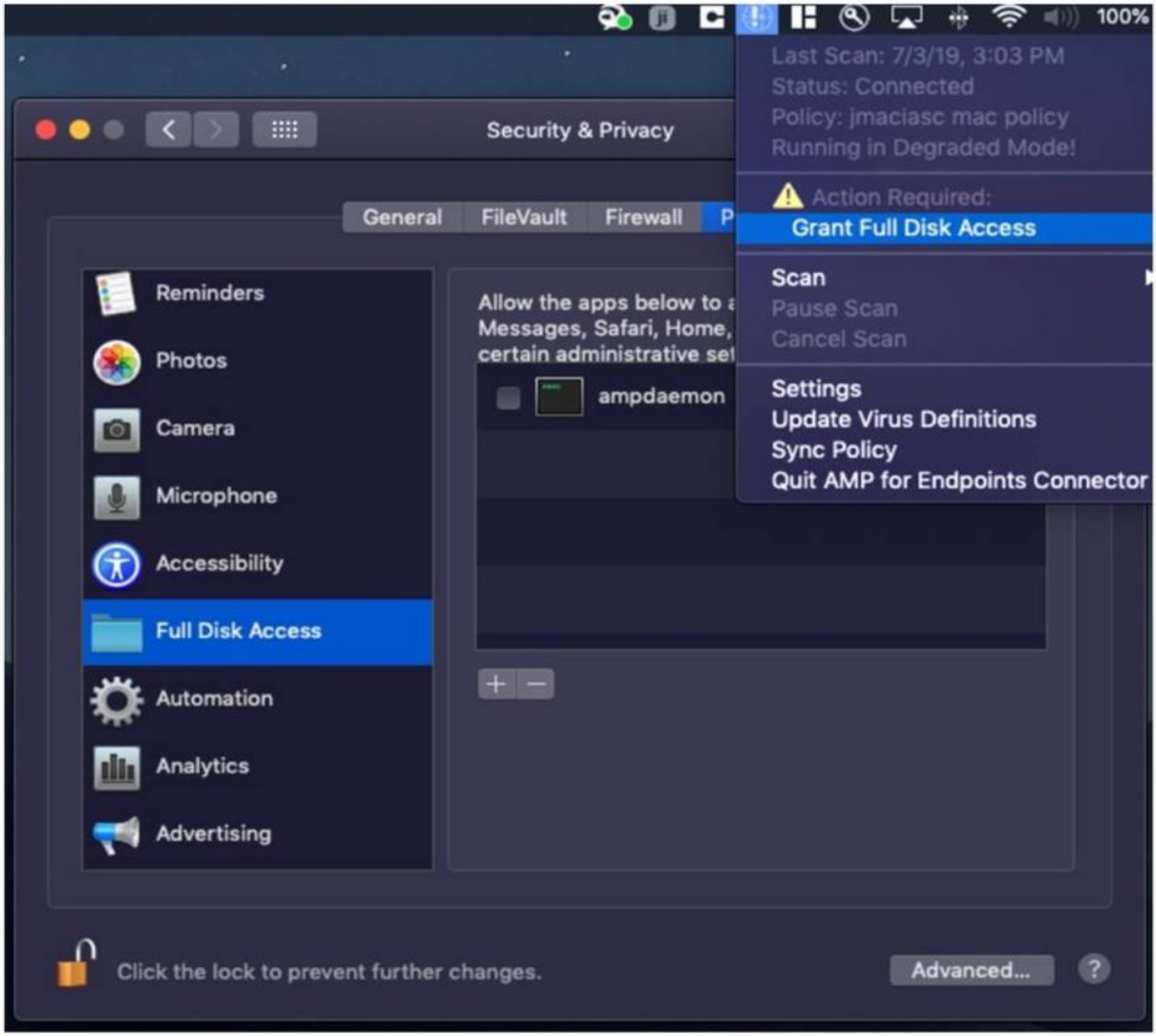
Falha total de acesso ao disco

O console AMP mostra "Acesso ao disco não concedido", como mostrado na imagem.

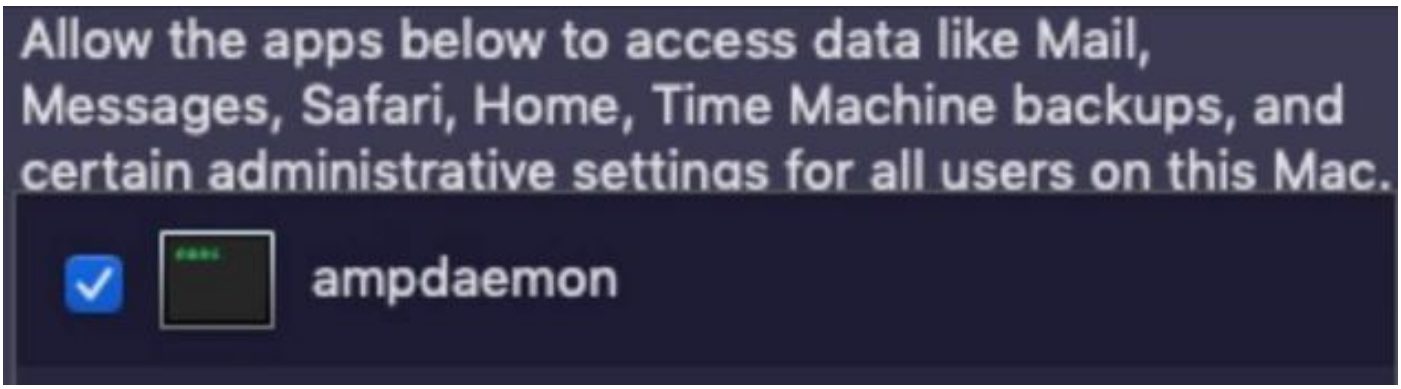
Verifique se o acesso total ao disco não é permitido, navegue para **Preferências do sistema > Segurança e privacidade > Privacidade,** conforme mostrado na imagem.



Para aprovar o acesso total ao disco do conector AMP, navegue até Full Disk Access e marque o processo de ampdaemon, como mostrado na imagem.

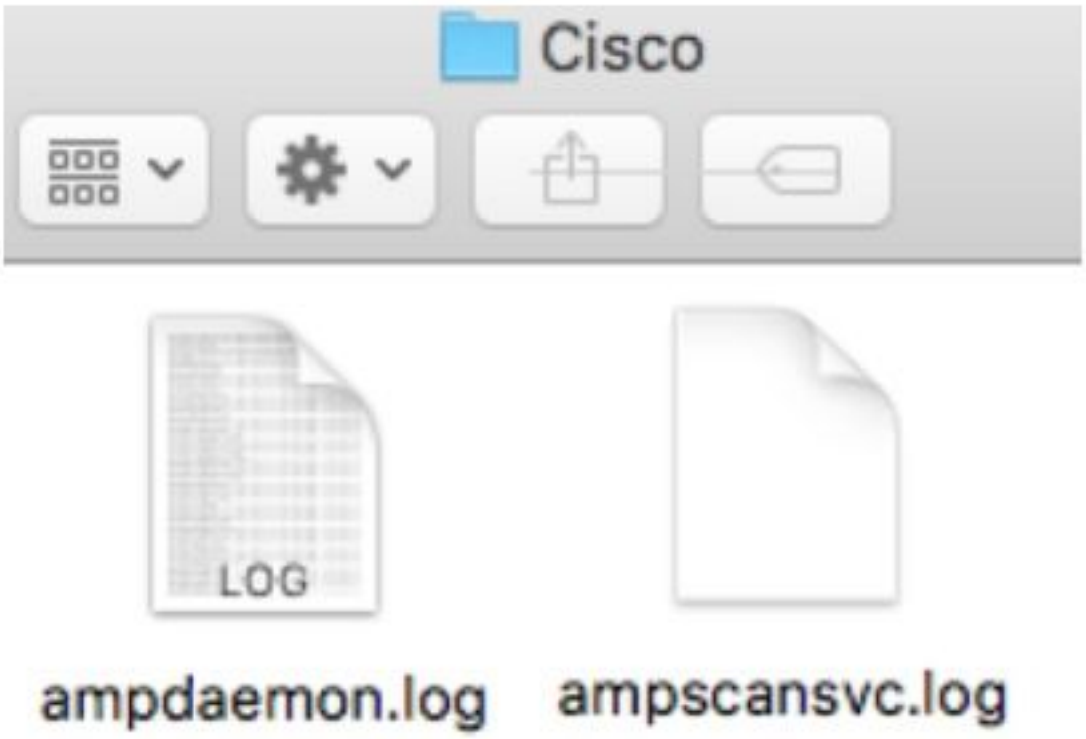


Abra um terminal e pare o serviço AMP e execute o próximo comando: **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** marque a caixa de seleção, como mostrado na imagem.



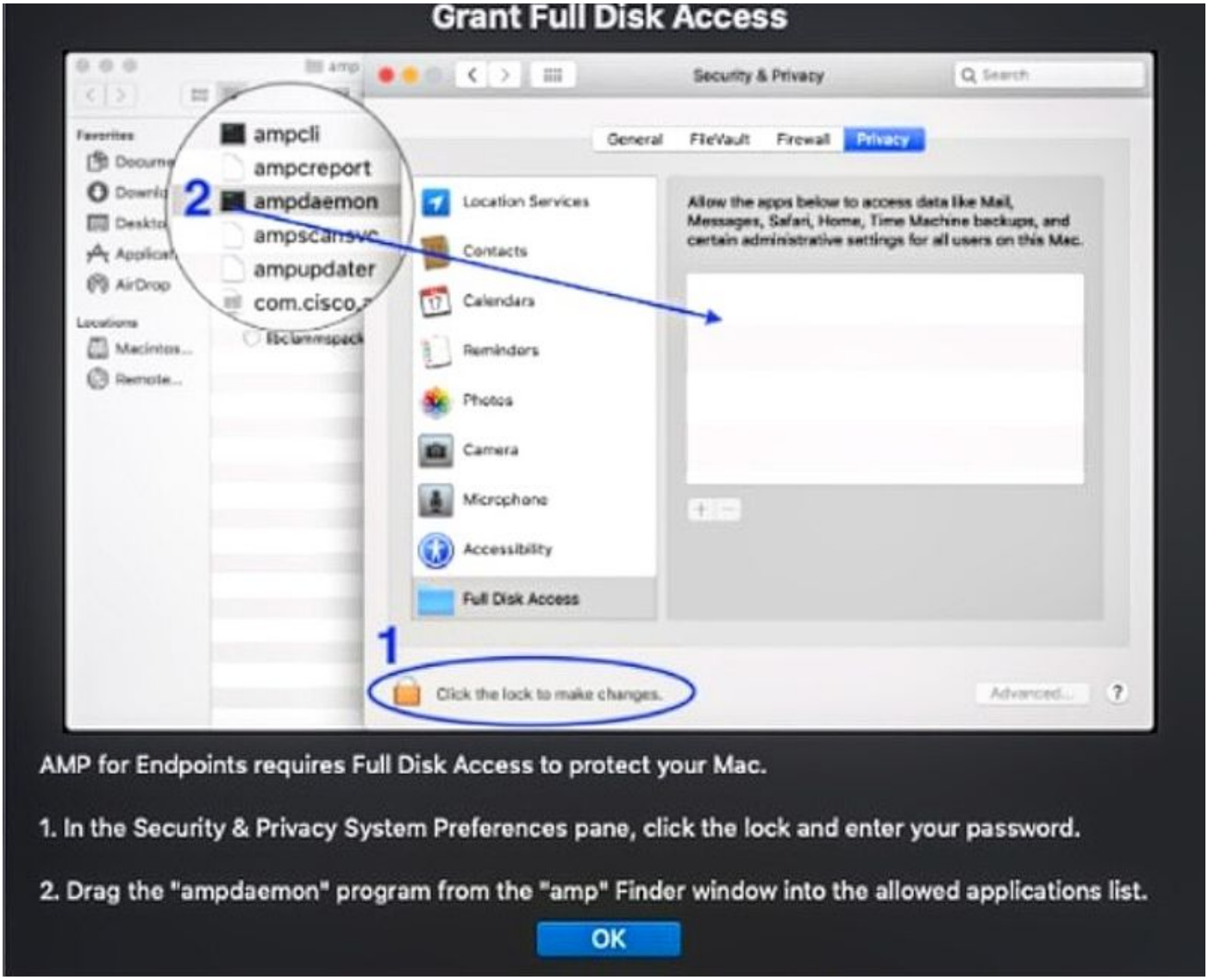
Para evitar problemas de cache, navegue até **/library/logs/cisco** e apague os próximos arquivos, como mostrado na imagem.

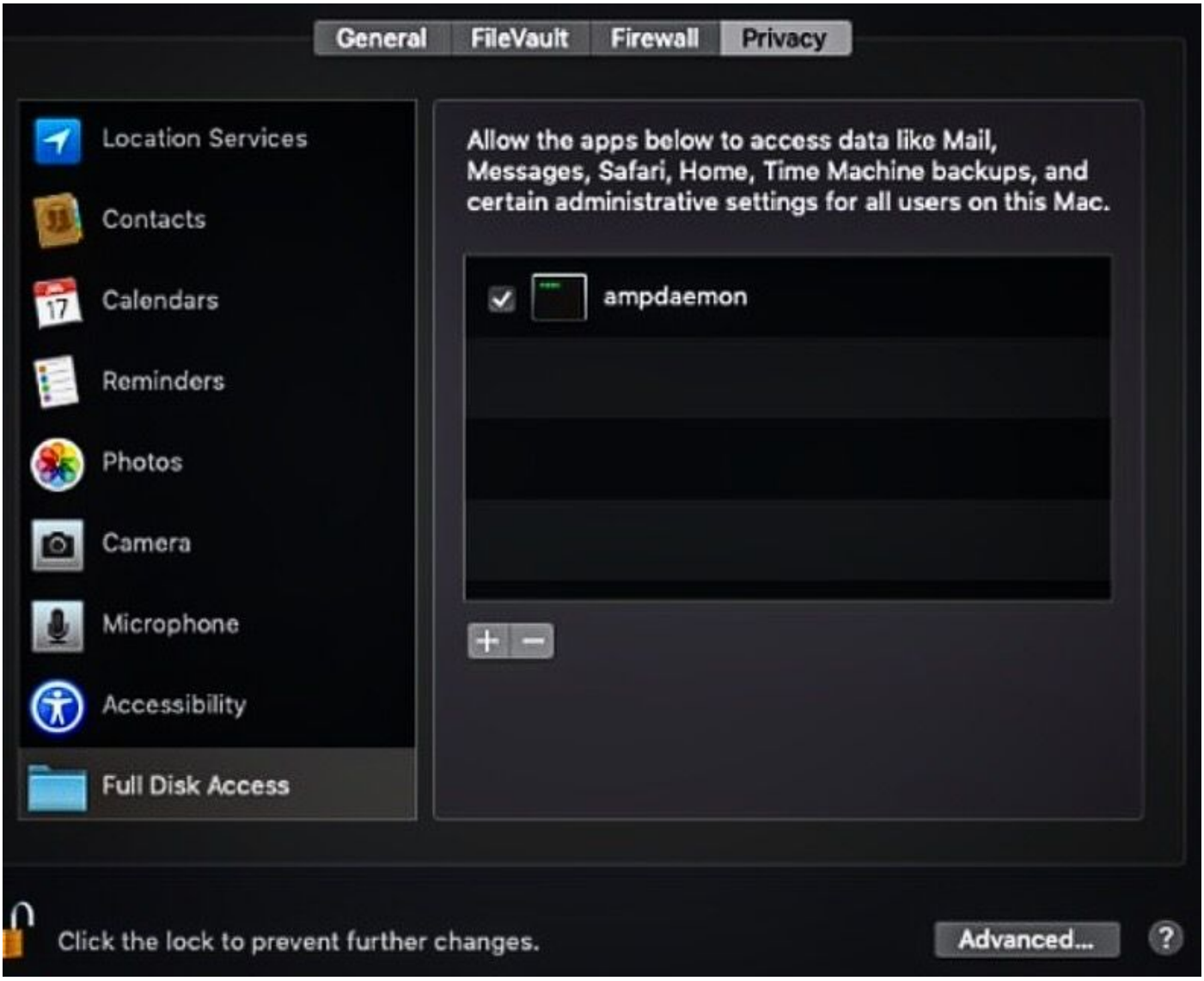
- ampdaemon.log
- ampscansvc.log



Inicie o serviço com o comando: **sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

> **Observação**: caso você não consiga encontrar o arquivo ampdeamon, arraste e solte-o na lista permitir Acesso Total ao Disco, verifique se a caixa de seleção está marcada, como mostrado na imagem.


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 acesso total ao disco, conceder aos Kernels permissões e uma reinicialização recomendada dos dispositivos MAC, no próximo intervalo de pulsação a mensagem relatada desaparece do console.