Núcleo MAC e acesso a disco completo no console - AMP para valores-limite

Índice

Introdução

Este original descreve as etapas para pesquisar defeitos na proteção avançada do malware (AMP) para que os valores-limite trabalhem duas falhas do Mac: Acesso a disco completo (FDA) e módulo de núcleo não autorizado.

Contribuído por Uriel Torres, Javier Jesus Marti'nez, engenheiros de TAC da Cisco.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

• O Mac utiliza ferramentas o conhecimento
• Conta com privilégios do administrado

Componentes Utilizados

A informação neste documento é baseada em Cisco AMP para valores-limite para o MAC.

A informação neste documento foi criada dos dispositivos em um ambiente específico:

- Serra alta 10.13 MacOS

- MacOS 10.14 (Mojave)

Limitações

Este é um erro cosmético nos conectores OSX e AMP instalados em OSV-10.4.X e em versão 1.11.0 do conector. O portal AMP mostra que uma mensagem de falha para FDA e as mostras FDA do host está permitida.
BugID: CSCvq98799

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Quando um pedido é feito para carregar um KEXT, mas não ainda aprovado, o pedido da carga está negado. A serra alta 10.13 MacOS introduz uns novos recursos, que signifiquem que o usuário exige a aprovação antes que Ramais da terceira novo-instalados de carregamento do núcleo (KEXTs) e somente os Ramais do núcleo aprovados são carregados em um sistema. O usuário precisa de seguir as etapas mencionadas antes para resolver o erro do núcleo.
Desde que o macOS 10.14 (Mojave) introduz os recursos de segurança novos que afetam o AMP para conectores do Mac dos valores-limite, você exige para assegurar-se de que o acesso a disco completo esteja concedido ao demônio do serviço AMP, sem aprovação, o conector AMP seja incapaz de fornecer a proteção ou a visibilidade a estas peças do sistema de arquivos que está sendo protegido pelo macOS.

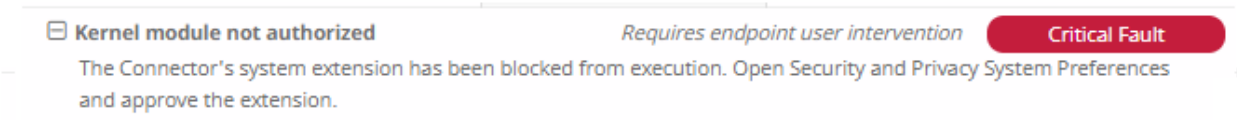
Troubleshooting

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

Erros de console

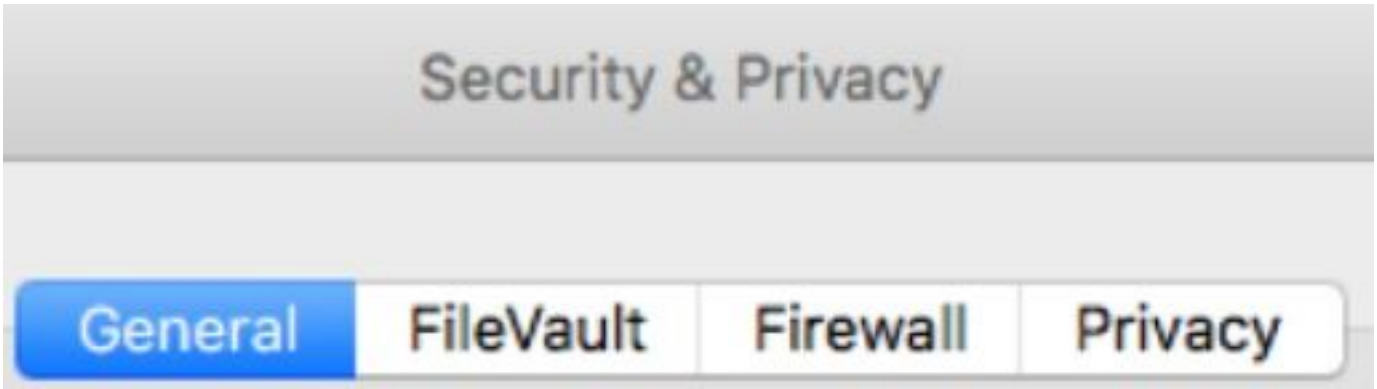
Falha do núcleo

O console AMP mostra o erro “módulo de núcleo não autorizado” quando um pedido é feito para carregar uma extensão do núcleo (KEXT) e não é aprovado, o pedido da carga é negado e o macOS apresenta um alerta, segundo as indicações da imagem.

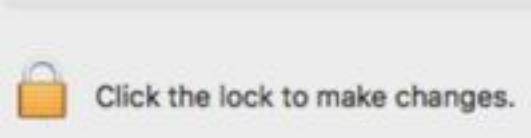


Depois que a elevação macOS de Apple, um anúncio oficial foi lançada sobre a aprovação do núcleo, segundo as indicações da imagem.

A fim permitir a extensão do conector, navegue ao **> segurança & à privacidade > ao general das preferências do sistema** segundo as indicações da imagem.



Clique sobre o fechamento para aprovar o KEXT (somente os Ramais do núcleo aprovados pelo usuário são carregados em um sistema), segundo as indicações da imagem.

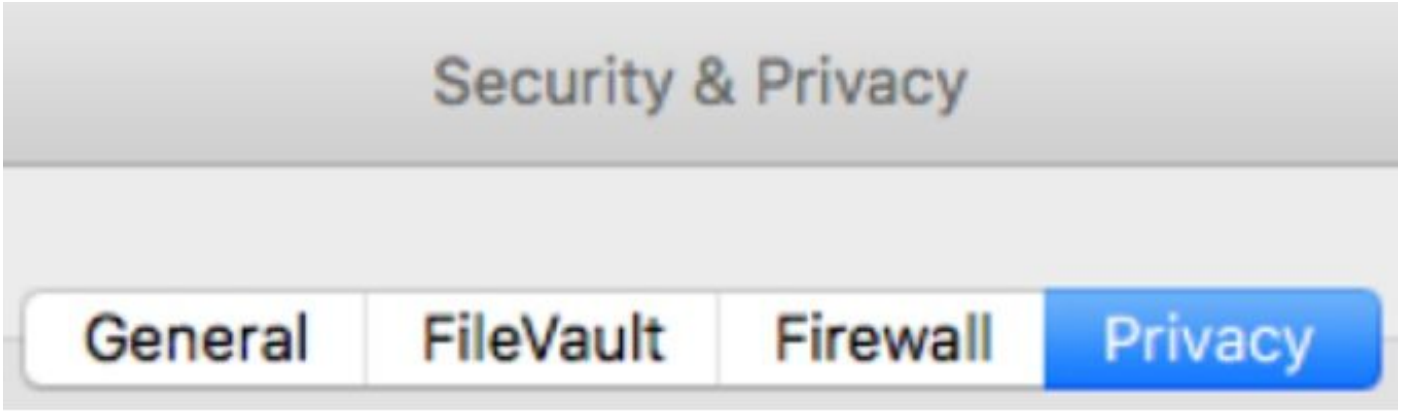


Nota: A aprovação do usuário é apresentada placa nas preferências da Segurança & da privacidade por 30 minutos após o alerta. Quando o KEXT é tentativas futuras aprovadas da carga faz com que a interface do utilizador da aprovação reapareça mas não provoca um outro alerta do usuário.

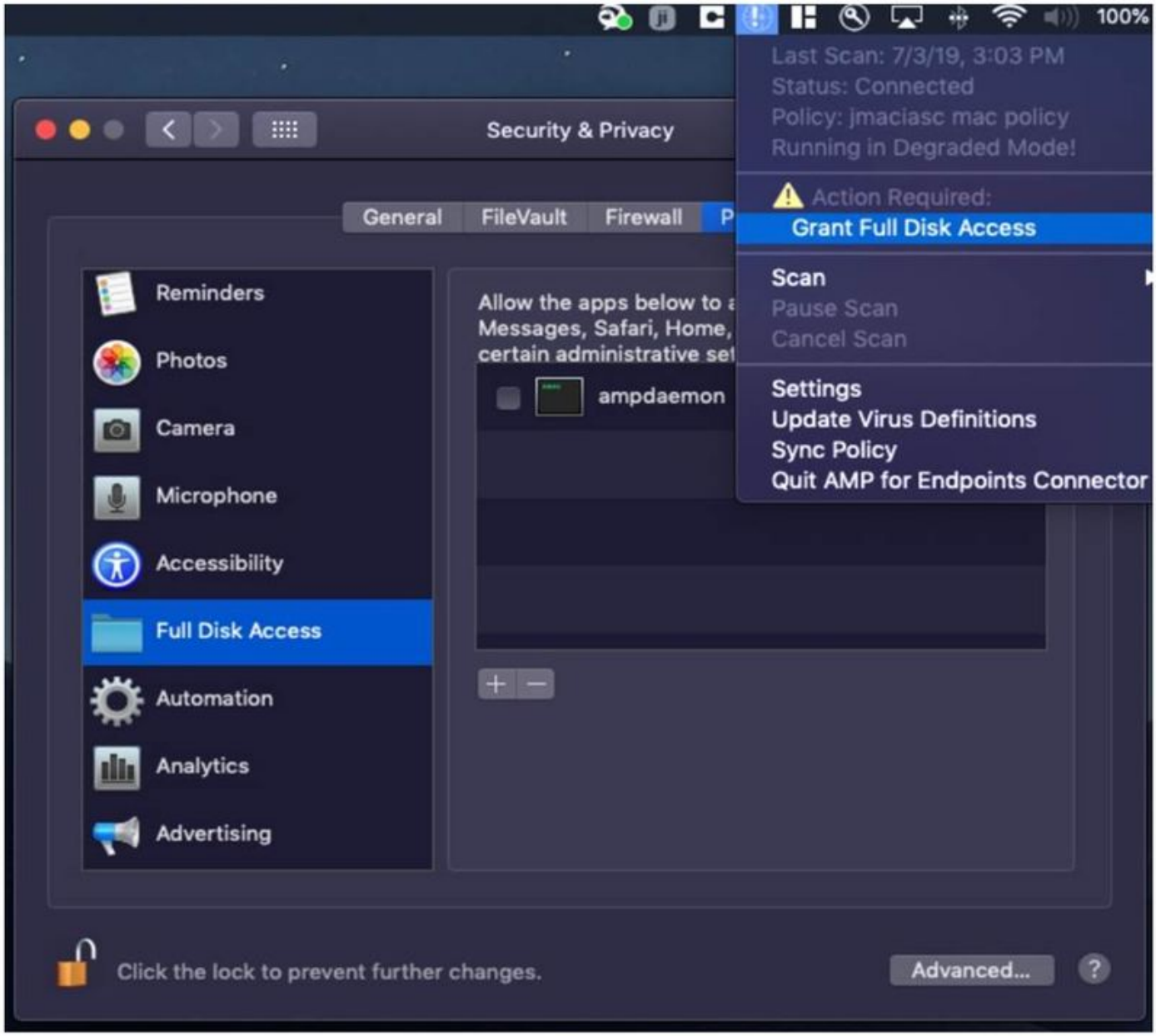
Falha completa do acesso a disco

O console AMP mostra o “acesso a disco não concedido” segundo as indicações da imagem.

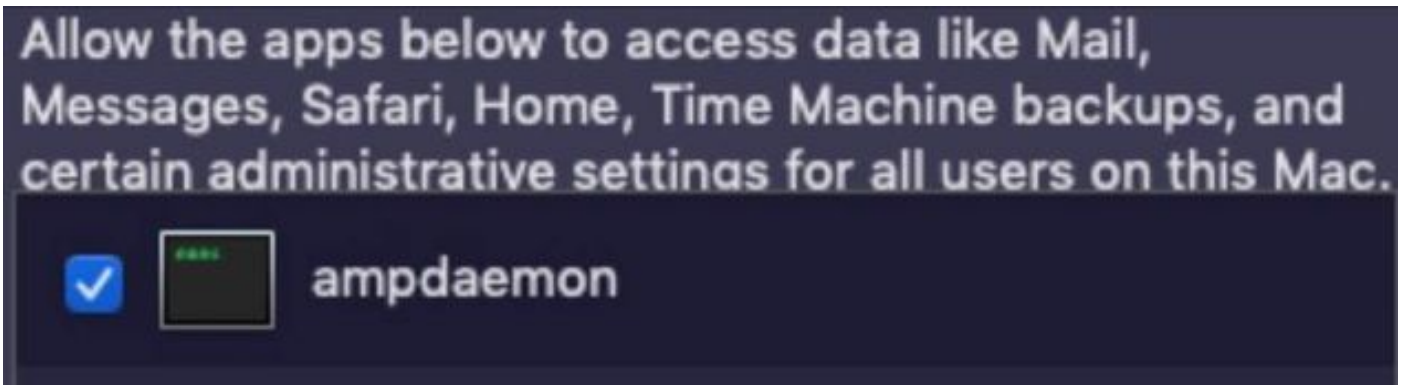
Verifique que o acesso a disco completo não está permitido, navega ao **> segurança das preferências do sistema & ao > Privacidade da privacidade,** segundo as indicações da imagem.



A fim aprovar o acesso a disco de Ful do conector AMP, navegue ao acesso a disco completo e ao sinal o processo do ampdaemon, segundo as indicações da imagem.

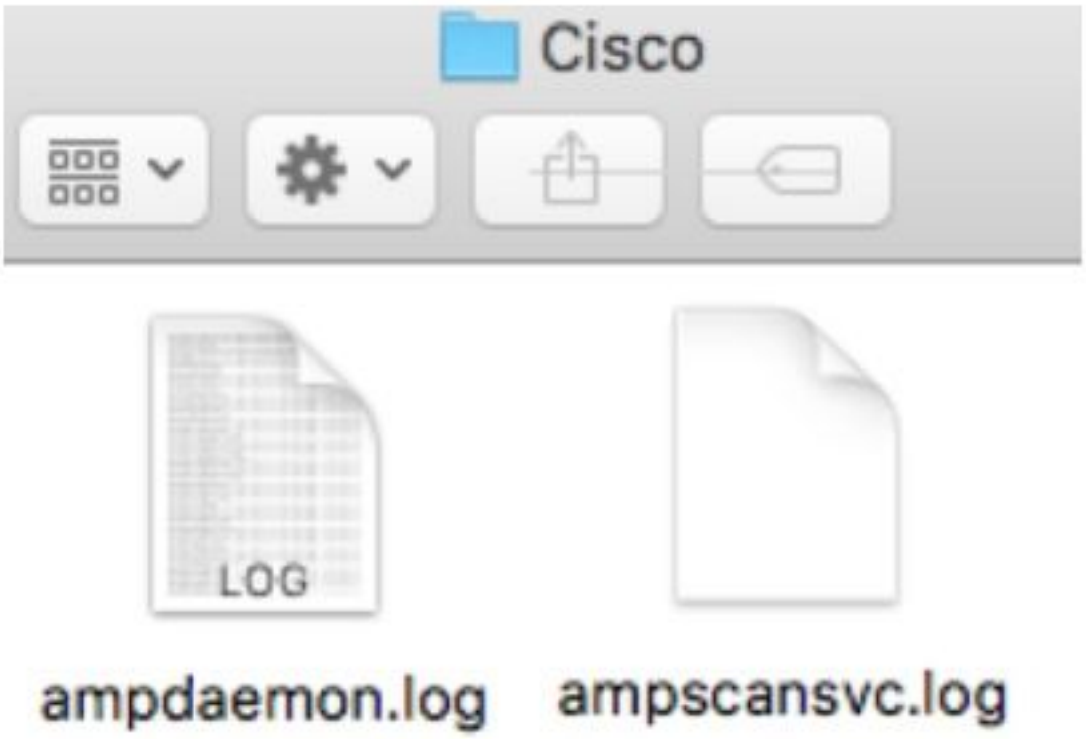


Abra um terminal e pare o serviço AMP e execute o comando seguinte: **o sudo /bin/launchctl descarrega /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** marca a caixa de seleção, segundo as indicações da imagem.



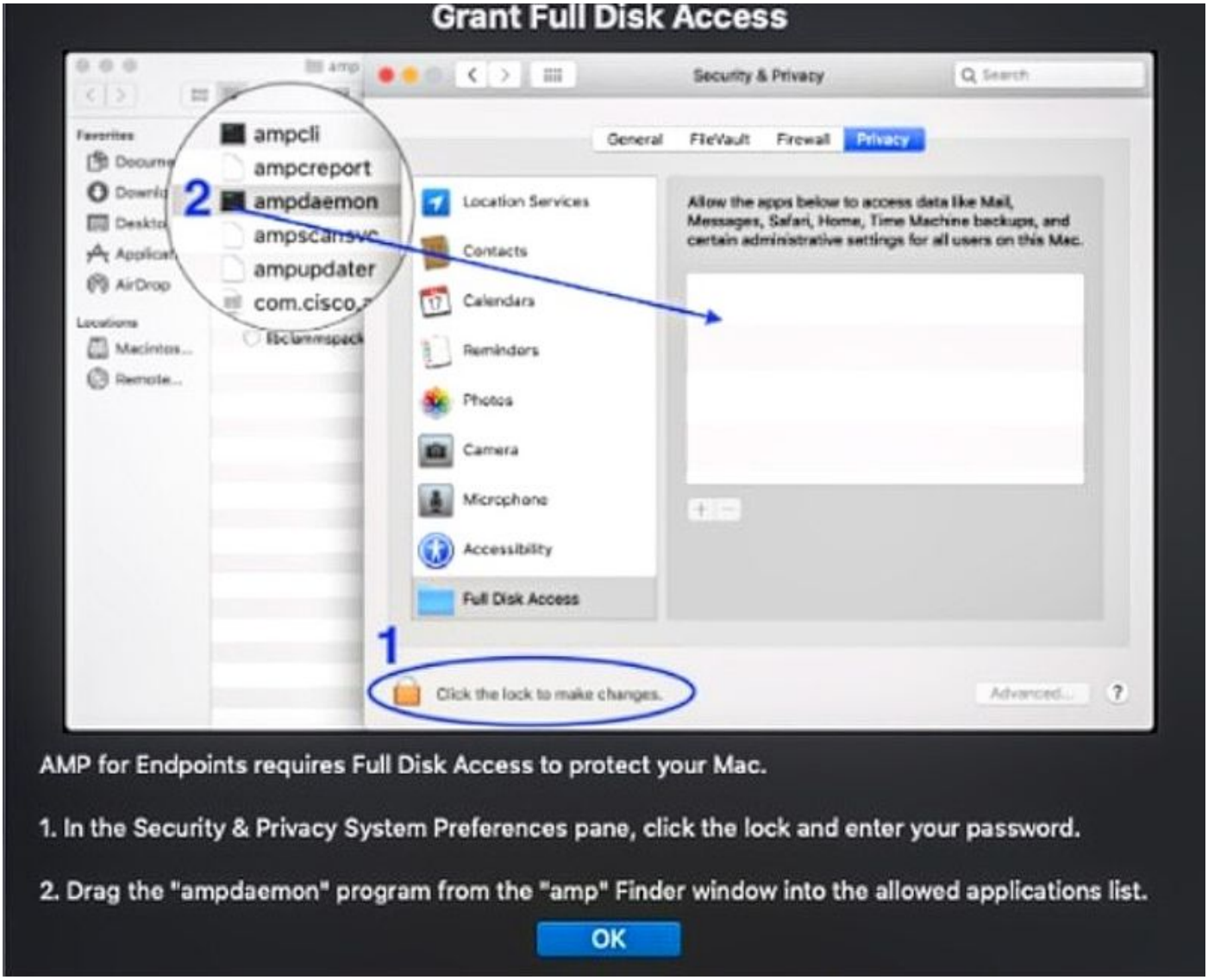
A fim evitar edições do esconderijo, navegue a **/library/logs/cisco** e apague os arquivos seguintes, segundo as indicações da imagem.

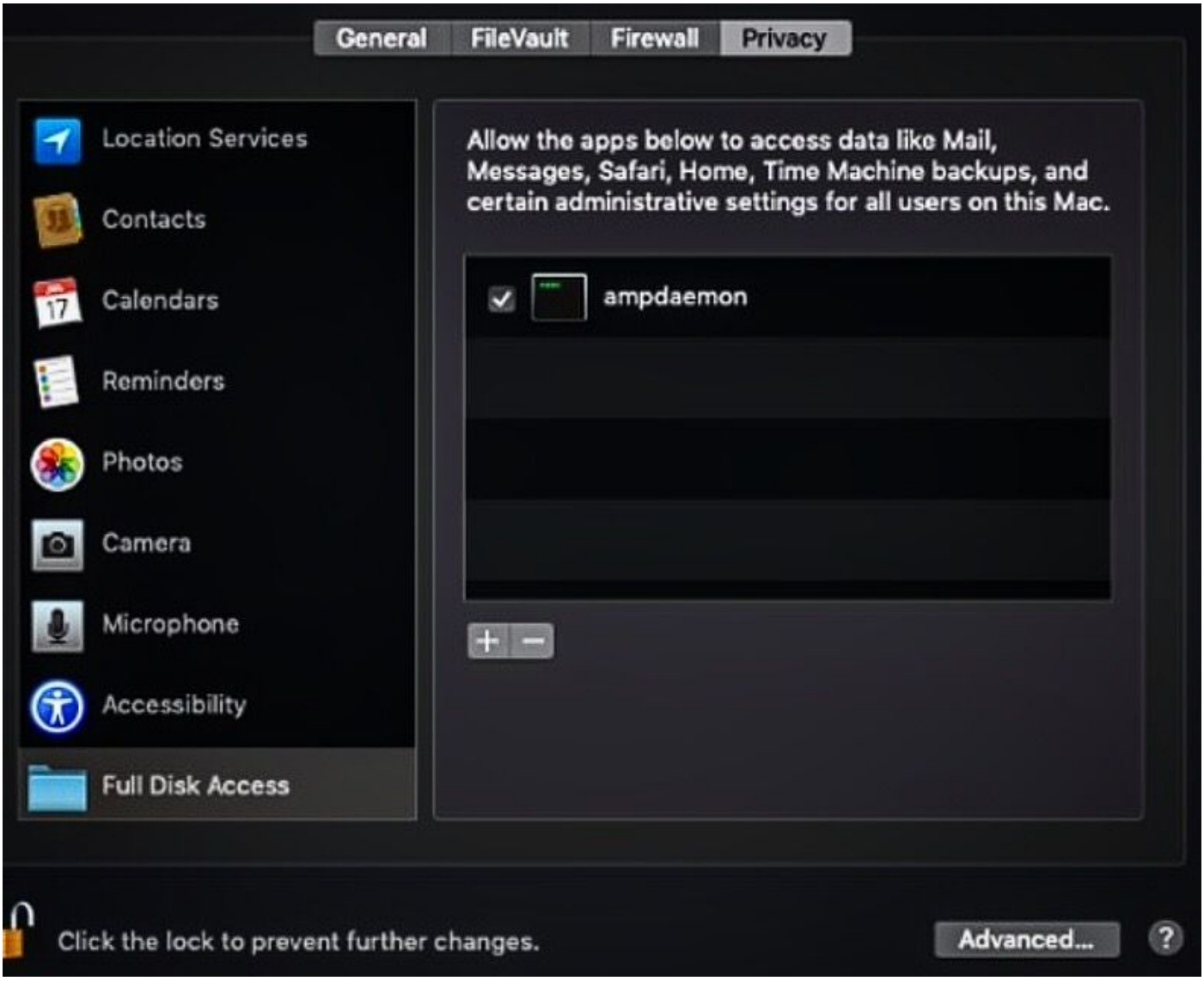
- ampdaemon.log
- ampscansvc.log



Comece o serviço com o comando: **carga /Library/LaunchDaemons/com.cisco.amp.daemon.plist de /bin/launchctl do sudo**.

> Nota: Caso que você não pode encontrar o arquivo do ampdeamon, arrasto & o deixar cair na lista de acesso a disco completa reservar, assegure-se de que a caixa de seleção esteja marcada, segundo as indicações da 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



A fim conceder o acesso a disco completo, dê aos núcleos permissões e uma repartição recomendada dos dispositivos MAC, no intervalo de batimento cardíaco seguinte a mensagem relatada desaparece do console.