コンソールでのMACカーネルとフルディスクアクセス – AMP for Endpoints

内容

概要

このドキュメントでは、エンドポイントが2つのMac障害を処理するための高度なマルウェア防御(AMP)におけるトラブルシューティング手順について説明します。フルディスクアクセス(FDA)およびカーネルモジュールが許可されていません。

著者：Cisco TACエンジニア、Uriel Torres、Javier Jesis Martinez

前提条件

要件

次の項目に関する知識があることが推奨されます。

・ Macツールの知識
・ 管理者権限を持つアカウント

使用するコンポーネント

このドキュメントの情報は、Cisco AMP for Endpoints for MACに基づくものです。

このドキュメントの情報は、特定の環境にあるデバイスから作成されたものです。

- MacOS High Sierra 10.13

- MacOS 10.14(Mojave)

制限

これは、OSV-10.4.XおよびコネクタバージョンOSXおよびAMPコネクタの表面的なバグです。AMPポータルにはFDAの障害メッセージが表示され、ホストにはFDAが許可されていることが示されています。
バグID:CSCvq98799

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

KEXTのロードが要求されたが、まだ承認されていない場合、ロード要求は拒否されます。MacOS High Sierra 10.13では新機能が導入されています。これは、新しくインストールされたサードパーティ製カーネル拡張(KEXT)をロードする前にユーザが承認を必要とし、承認されたカーネル拡張だけがシステムにロードされることを意味します。ユーザは、前に説明した手順に従って、カーネルエラーを解決する必要があります。
macOS 10.14(Mojave)では、エンドポイント用AMPに影響する新しいセキュリティ機能Macコネクタが導入されているため、AMPサービスデーモンにFull Disk Accessが許可されていることを確認する必要があります。

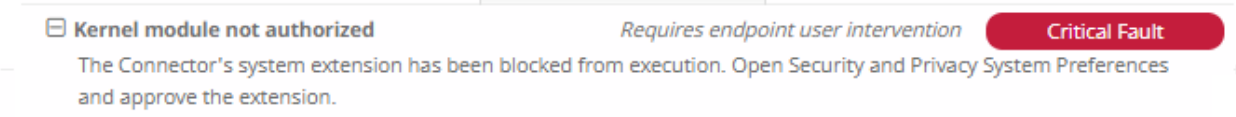
トラブルシュート

ここでは、設定のトラブルシューティングに使用できる情報を示します。

コンソールエラー

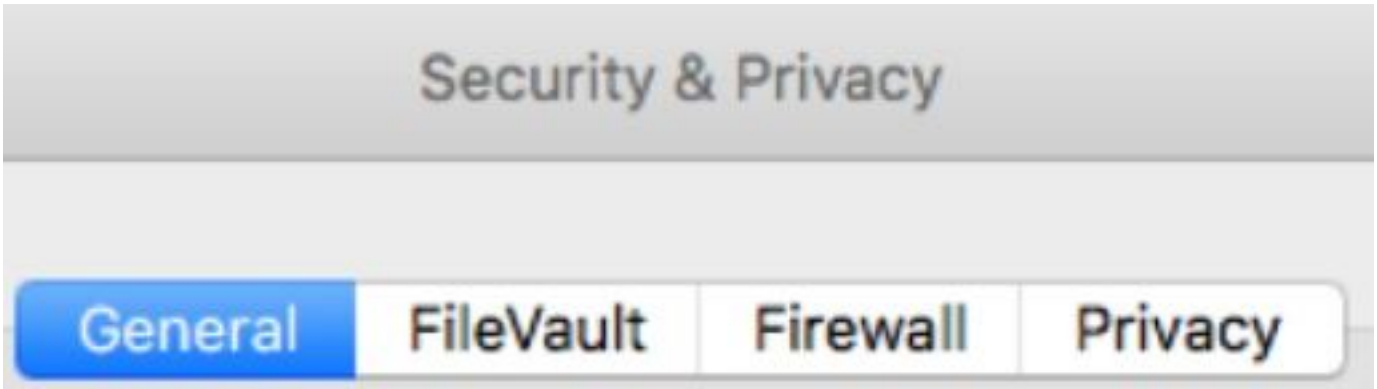
カーネル障害

図に示すように、AMPコンソールは、Kernel Extension(KEXT)をロードする要求が行われ、承認されていない場合、ロード要求が拒否され、macOSがアラートを表示すると、「Kernel module not authorized」エラーを表示します。

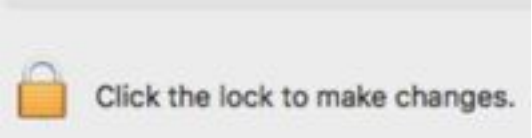


Apple macOSのアップグレード後、図に示すように、カーネルの承認に関する公式発表が開始されました。

コネクタの拡張を許可するには、図に示すように、**[System Preferences] > [Security & Privacy] > [General]**に移動します。



図に示すように、[Lock]をクリックしてKEXTを承認します（ユーザによって承認されたカーネル拡張だけがシステムにロードされます）。

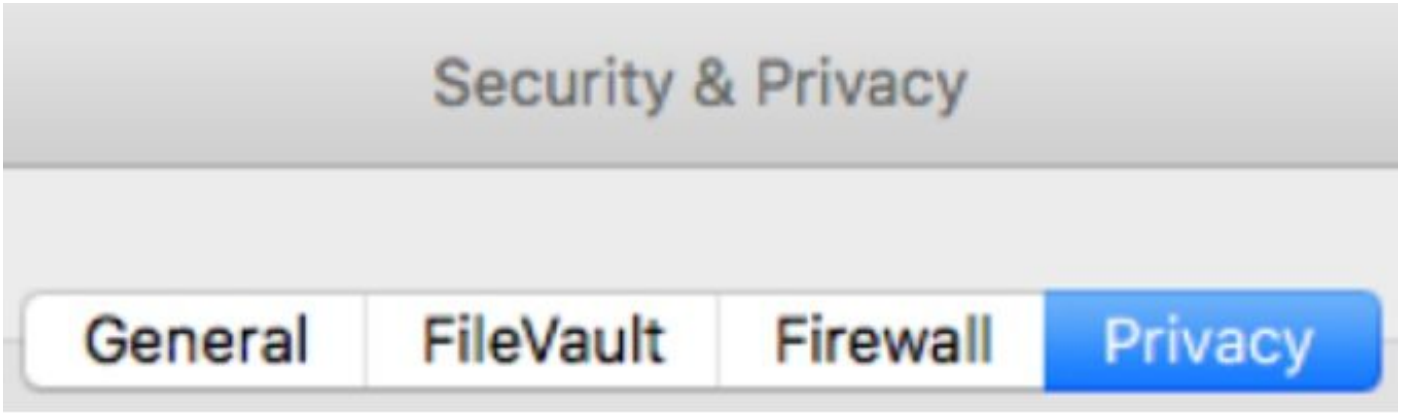


注：ユーザの承認は、アラートの30分後に[Security & Privacy preferences]ペインに表示されます。KEXTが承認された後のロード試行によって承認ユーザインターフェイスが再度表示されますが、別のユーザアラートはトリガーされません。

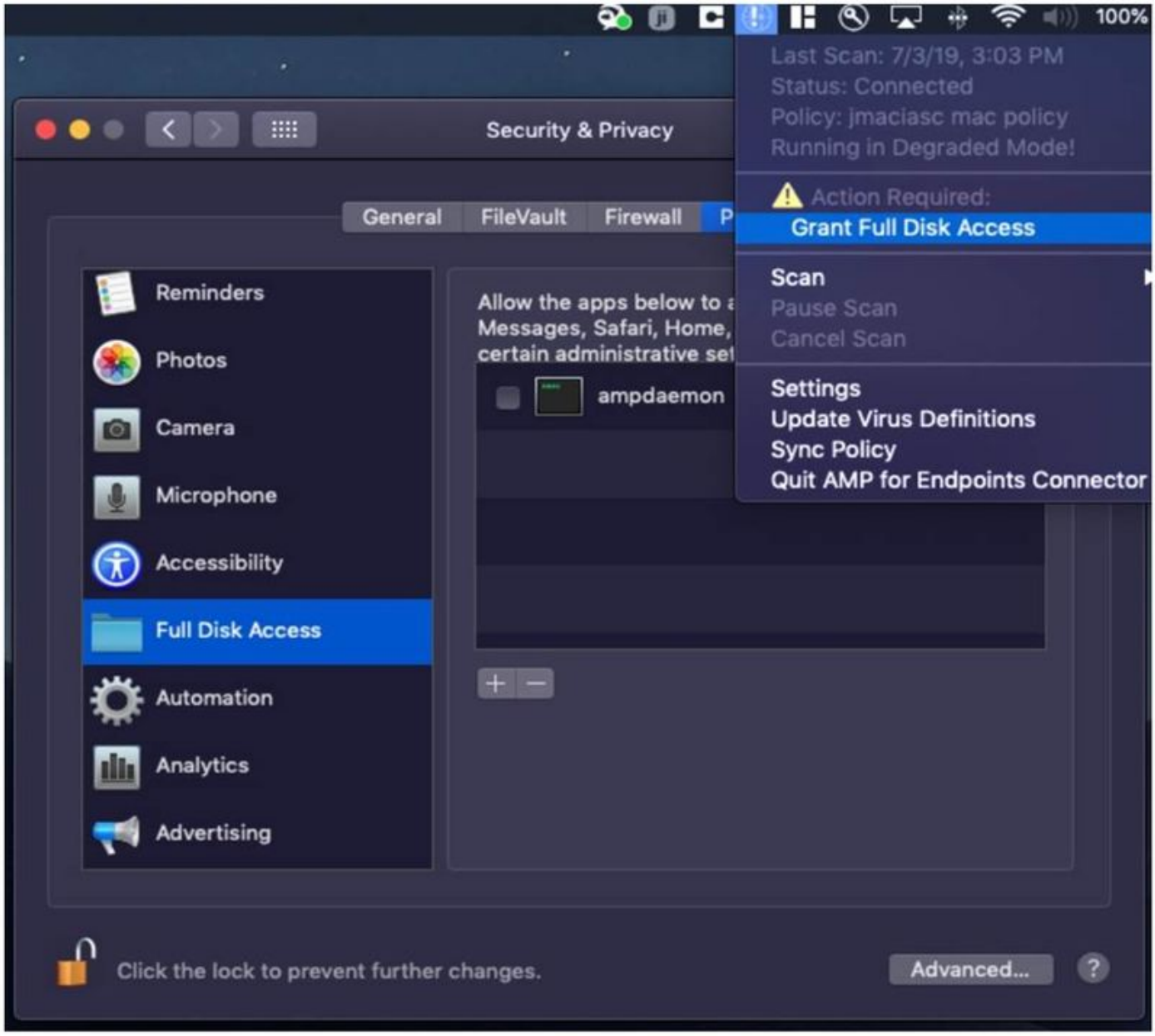
フルディスクアクセス障害

図に示すように、AMPコンソールに「Disk Access not granted」と表示されます。

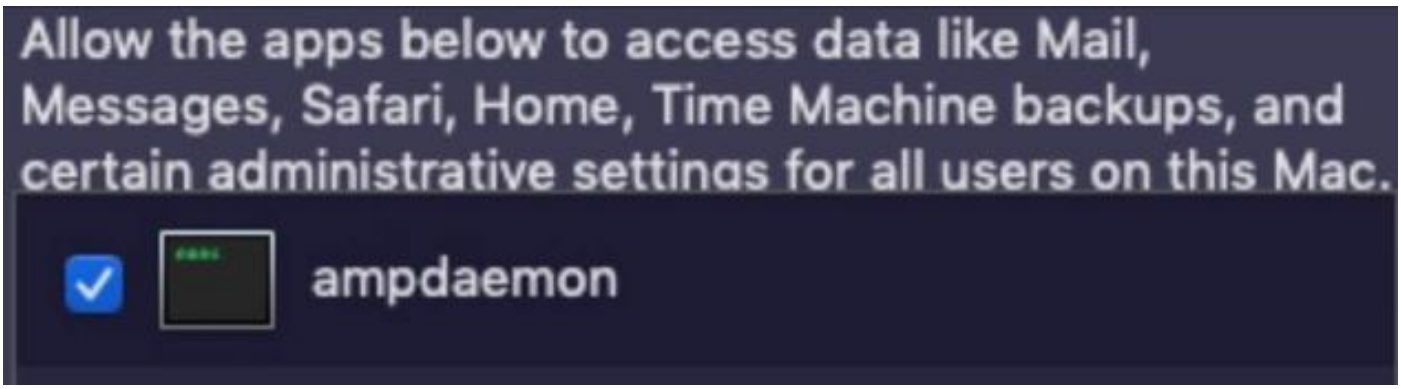
フルディスクアクセスが許可されていないことを確認します。図に示すように、[シス**テム設定] > [セキュリティとプライバシー] > [プライバシー**]に移動します。



AMPコネクタのフルディスクアクセスを承認するには、[Full Disk Access]に移動し、図に示すようにampdaemonプロセスをチェックします。

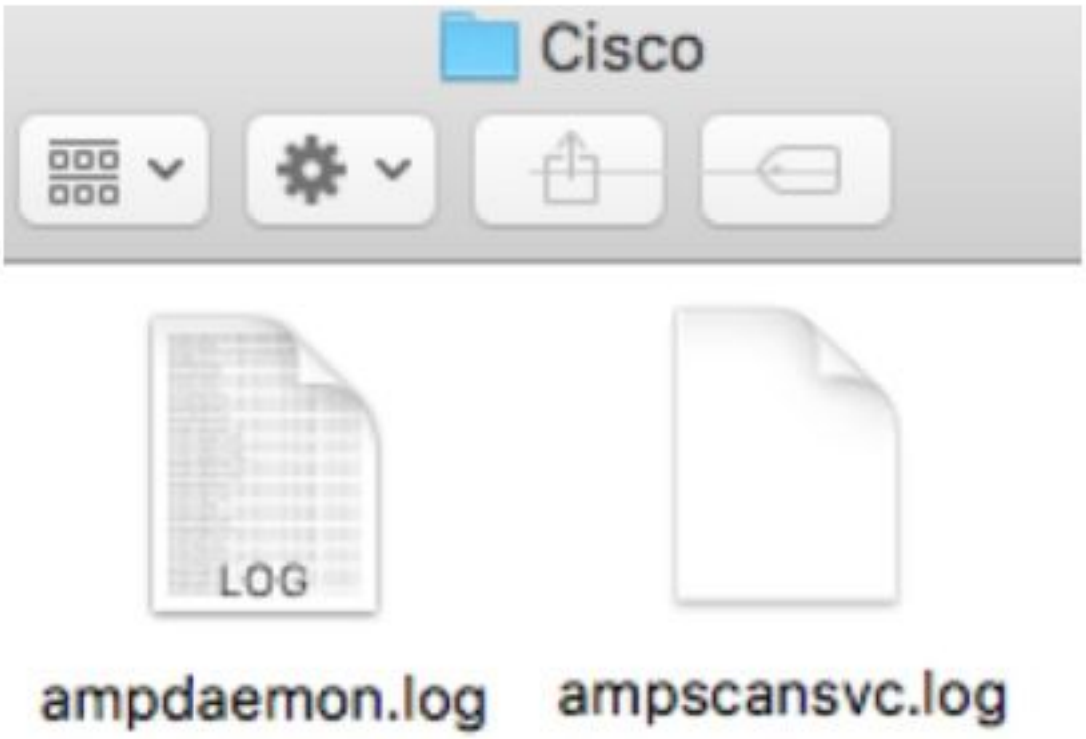


端末を開き、AMPサービスを停止し、次のコマンド**sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plistを実行し、図に示すようにチェックボックスをマークします。**



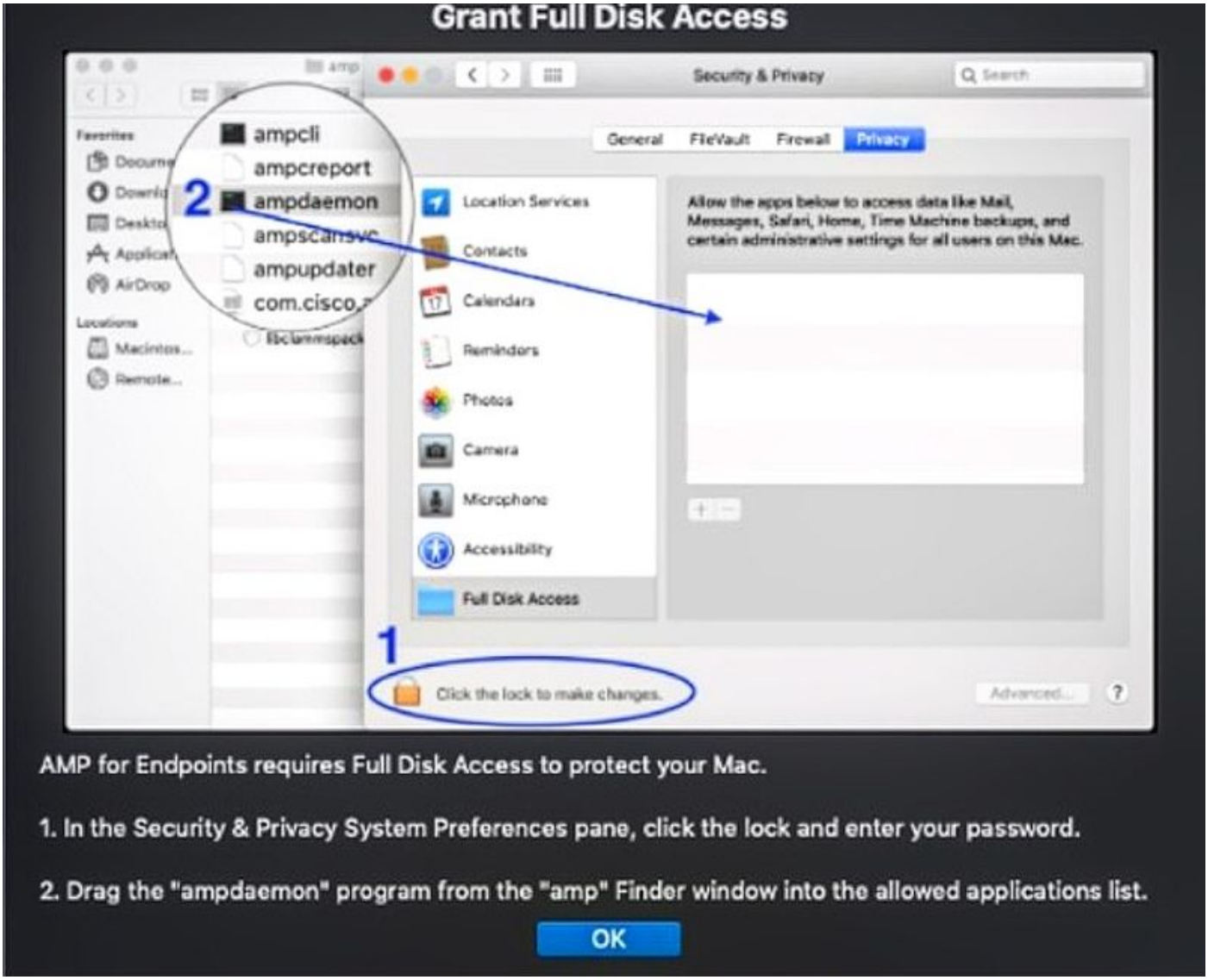
キャッシュの問題を回避するには、図に示すように**/library/logs/ciscoに移動**し、次のファイルを消去します。

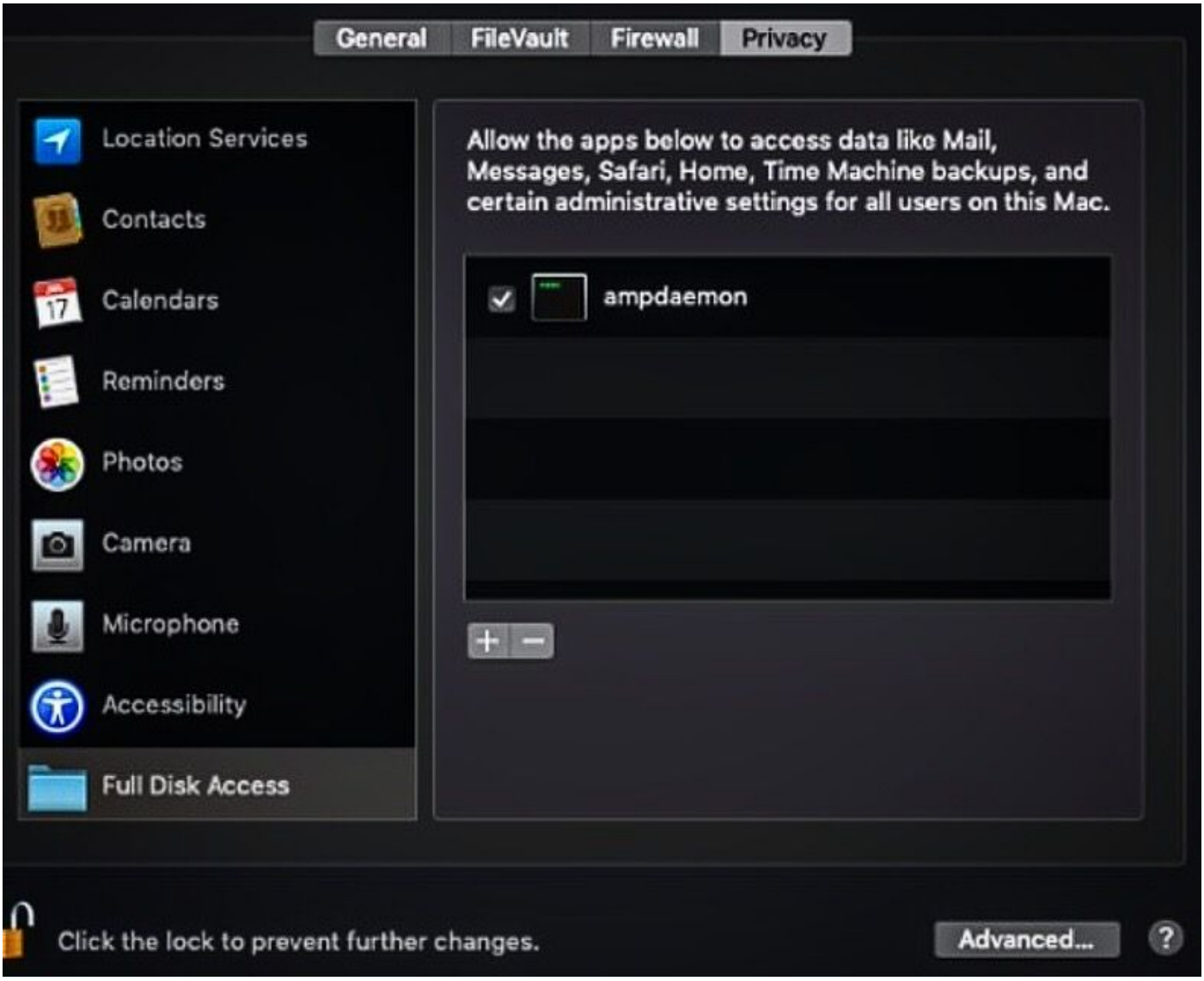
- ampdaemon.log
- ampscansvc.log



sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plistコマンドを使用してサービスを開始します。

> **注：** ampdeamonファイルが見つからない場合は、[Allow Full Disk Access]リストにドラッグアンドドロップし、図に示すようにチェックボックスがオンになっていることを確認します。


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



フルディスクアクセスを許可するには、カーネルにアクセス許可とMACデバイスの推奨リブートを与え、次回のハートビート間隔で報告されたメッセージがコンソールから消えます。