

Noyau MAC et accès au disque complet dans la console - AMP for Endpoints

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Limites](#)

[Informations générales](#)

[Dépannage](#)

[Erreurs de console](#)

[Défaillance du noyau](#)

[Défaillance de l'accès au disque complet](#)

Introduction

Ce document décrit les étapes à suivre pour dépanner dans Advanced Malware Protection (AMP) for Endpoints afin que les points de terminaison fonctionnent avec deux failles Mac : Accès au disque complet (FDA) et module noyau non autorisé.

Contribué par Uriel Torres, Javier Jesus Martinez, Ingénieurs TAC Cisco.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

Connaissances en matière d'outils · Mac
Compte · avec privilèges d'administrateur

Components Used

Les informations de ce document sont basées sur Cisco AMP for Endpoints for MAC.

Les informations de ce document ont été créées à partir des périphériques d'un environnement spécifique :

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Limites

Il s'agit d'un bogue cosmétique sur les connecteurs OSX et AMP installés sur OSV-10.4.X et le connecteur version 1.11.0. Le portail AMP affiche un message de défaillance pour la FDA et l'hôte indique que la FDA est autorisée.

ID de bogue : [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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Lorsqu'une demande de chargement d'un fichier KEXT, mais non encore approuvée, la demande de chargement est refusée. MacOS High Sierra 10.13 introduit une nouvelle fonctionnalité, ce qui signifie que l'utilisateur a besoin d'approbation avant de charger les extensions de noyau tierce (KEXT) récemment installées et que seules les extensions de noyau approuvées sont chargées sur un système. L'utilisateur doit suivre les étapes mentionnées précédemment pour résoudre l'erreur de noyau.

Puisque macOS 10.14 (Mojave) introduit de nouvelles fonctionnalités de sécurité qui affectent les connecteurs Mac AMP for Endpoints, vous devez vous assurer que l'accès au disque complet est accordé au démon de service AMP, sans approbation, le connecteur AMP ne peut pas fournir de protection ou de visibilité à ces parties du système de fichiers protégées par macOS.

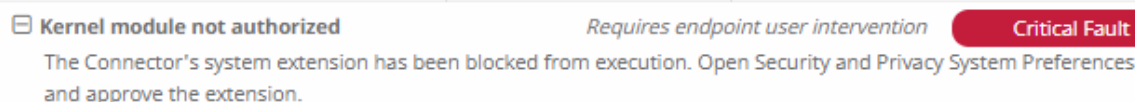
Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Erreurs de console

Défaillance du noyau

AMP Console affiche l'erreur " le module de noyau non autorisé " lorsqu'une demande est faite pour charger une extension de noyau (KEXT) et qu'elle n'est pas approuvée, que la demande de chargement est refusée et que macOS présente une alerte, comme l'illustre l'image.

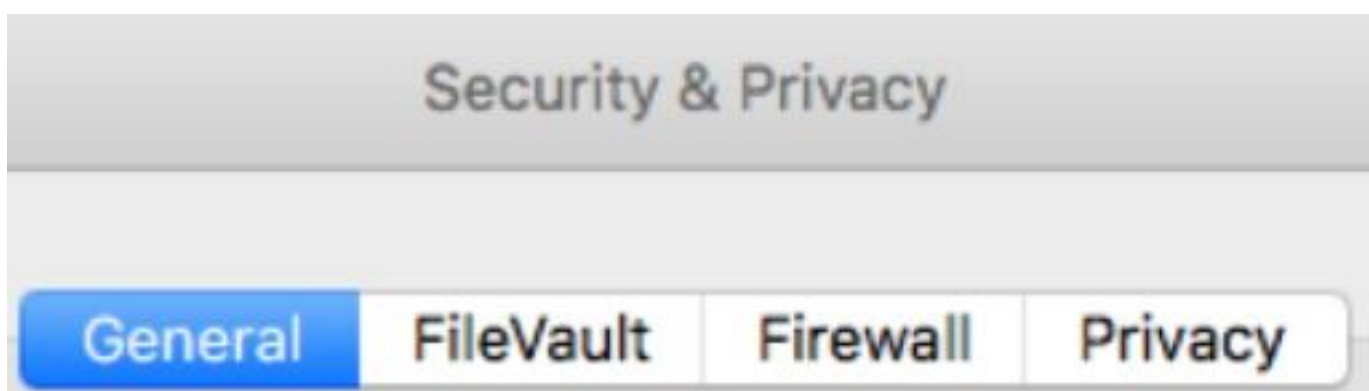
 **Kernel module not authorized** *Requires endpoint user intervention* **Critical Fault**
The Connector's system extension has been blocked from execution. Open Security and Privacy System Preferences and approve the extension.

Après la mise à niveau d'Apple macOS, une annonce officielle a été lancée sur l'approbation du noyau, comme le montre l'image.

Mac OS 10.13 - High Sierra Advisory

Apple macOS 10.13 includes additional kernel extension security that requires user interaction for the AMP for Endpoints Mac Connector to run properly. End users must approve the execution of new kernel extensions for Mac devices that are not managed by an MDM. We recommend that you upgrade all your AMP for Endpoints Mac Connectors to v1.4.5 prior to upgrading to macOS 10.13 to have the least amount of user intervention. See this [Apple Tech Note](#) for details about this feature.

Afin d'autoriser l'extension Connector, accédez à **Préférences système > Sécurité et confidentialité > Général** comme indiqué dans l'image.



Cliquez sur le bouton Verrouiller pour approuver le KEXT (seules les extensions de noyau approuvées par l'utilisateur sont chargées sur un système), comme le montre l'image.



Click the lock to make changes.

Remarque : l'approbation de l'utilisateur est présentée dans le volet des préférences de sécurité et de confidentialité pendant 30 minutes après l'alerte. Lorsque le KEXT est approuvé, de futures tentatives de chargement provoquent la réapparition de l'interface utilisateur d'approbation, mais elle ne déclenche aucune autre alerte utilisateur.

Défaillance de l'accès au disque complet

La console AMP affiche “accès au disque non accordé ” comme l'illustre l'image.

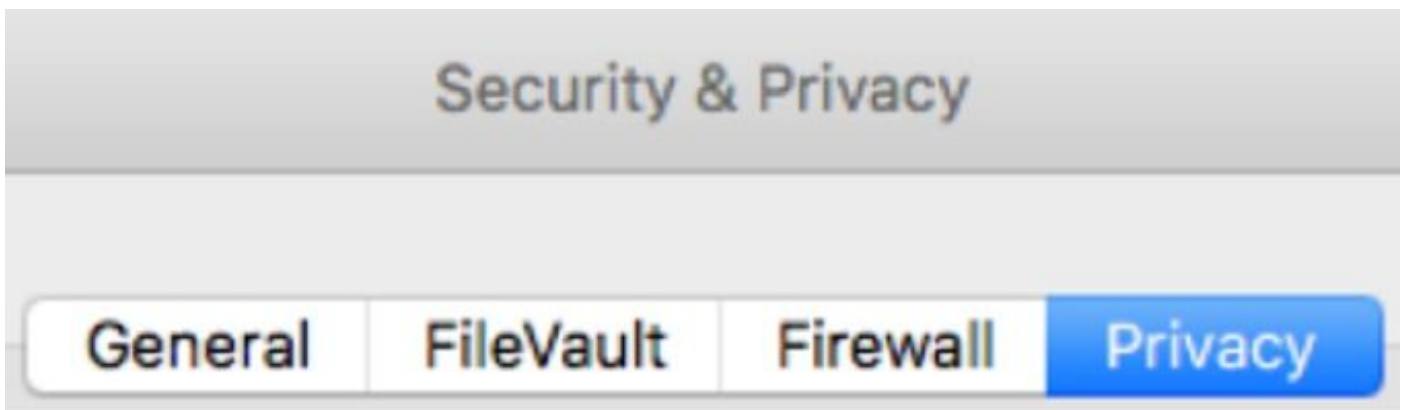
Disk access not granted

Requires endpoint user intervention

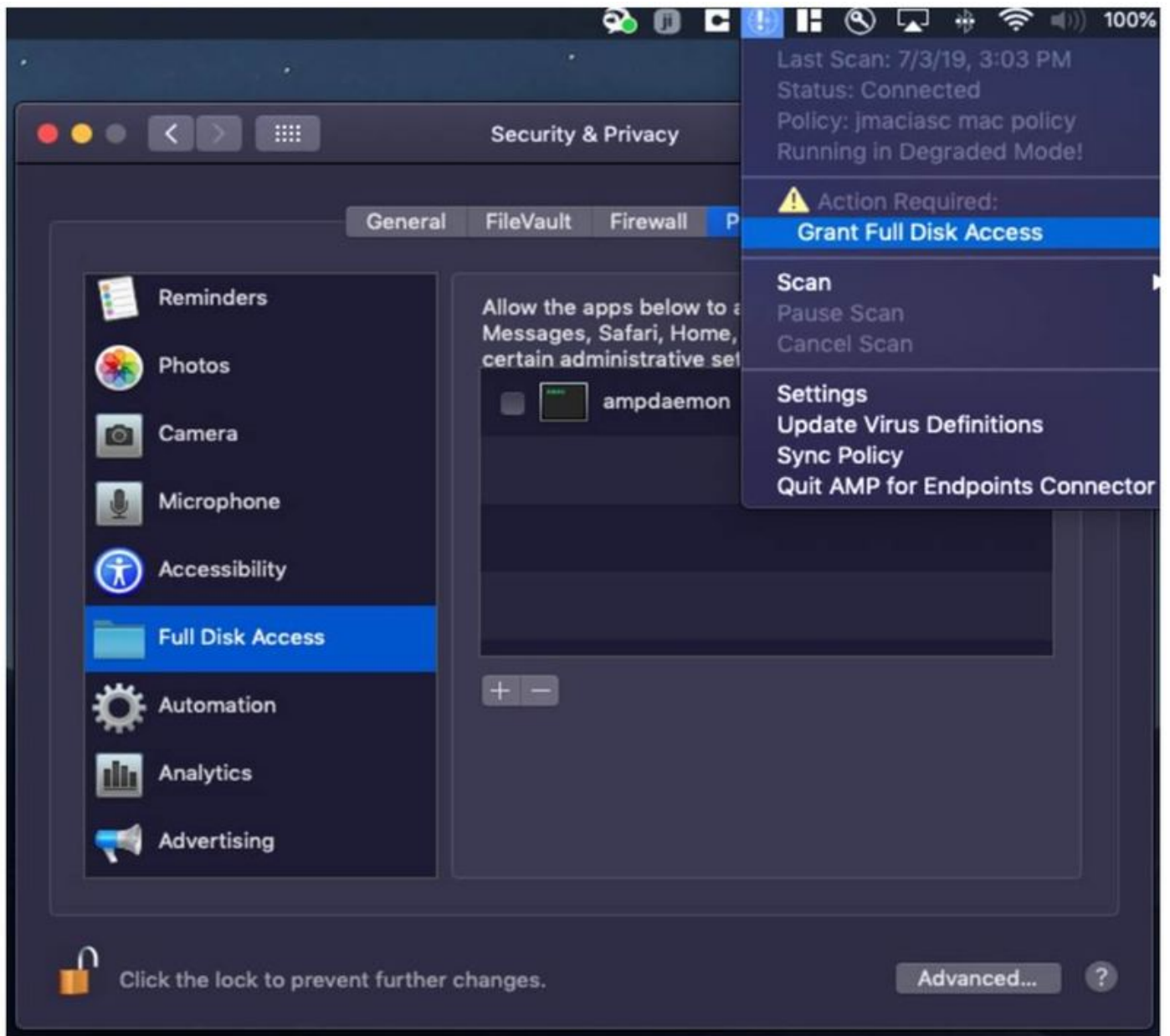
Major Fault

The Connector cannot access user files for scan. Open Security and Privacy System Preferences and grant Full Disk Access to the AMP background service: '/opt/cisco/amp/ampdaemon'.

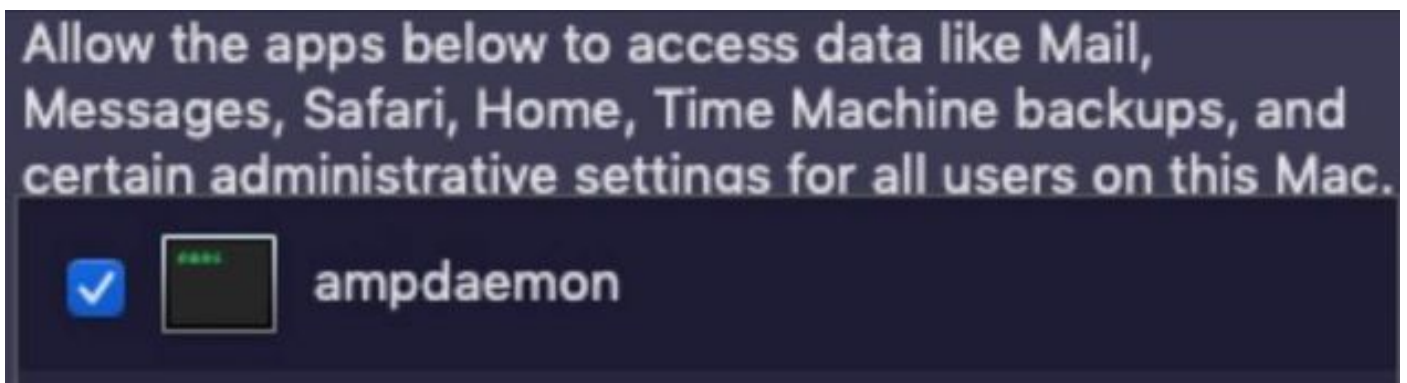
Vérifiez que l'accès au disque complet n'est pas autorisé, accédez à **Préférences système > Sécurité et confidentialité > Confidentialité**, comme indiqué dans l'image.



Afin d'approuver l'accès complet au disque du connecteur AMP, accédez à Accès complet au disque et cochez la case du processus d'ampdaemon, comme illustré dans l'image.

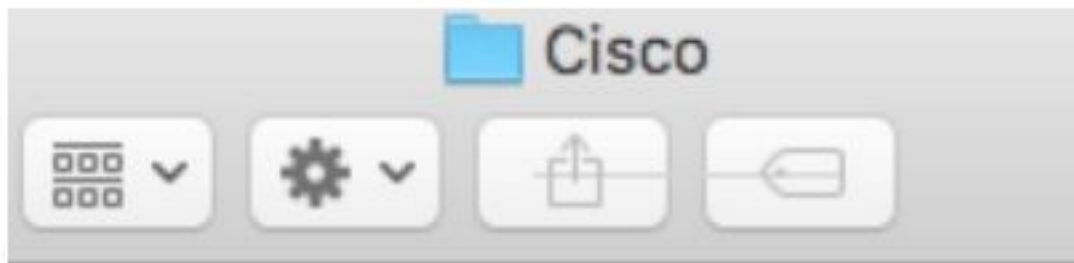


Ouvrez un terminal et arrêtez le service AMP et exécutez la commande suivante : `sudo /bin/Launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist`, cochez la case, comme indiqué dans l'image.



Afin d'éviter les problèmes de cache, accédez à `/library/logs/cisco` et effacez les fichiers suivants, comme illustré dans l'image.

- `ampdaemon.log`
- `ampscansvc.log`



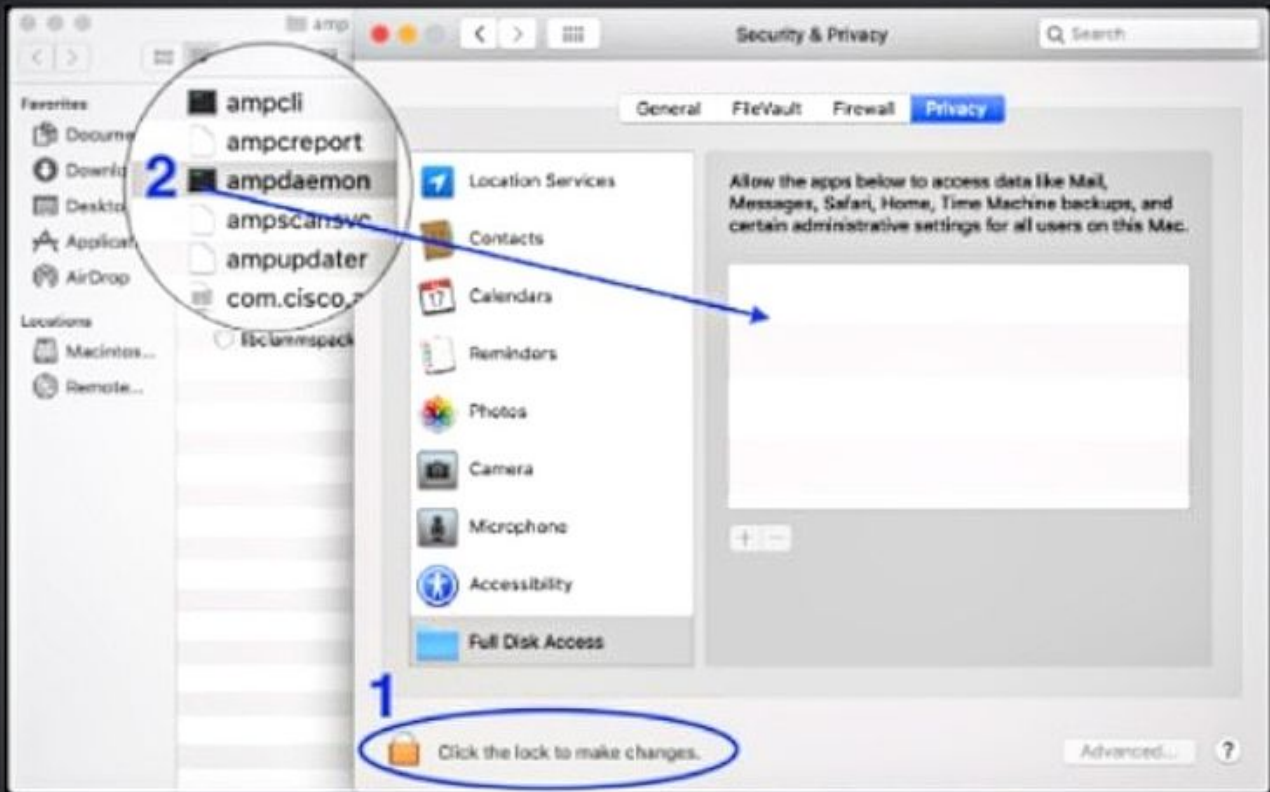
ampdaemon.log

ampscansvc.log

Démarrez le service avec la commande `sudo /bin/Launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist`.

Remarque : si vous ne trouvez pas le fichier ampdaemon, faites-le glisser et déposez-le dans la liste Autoriser l'accès au disque complet, assurez-vous que la case est cochée, comme l'indique l'image.

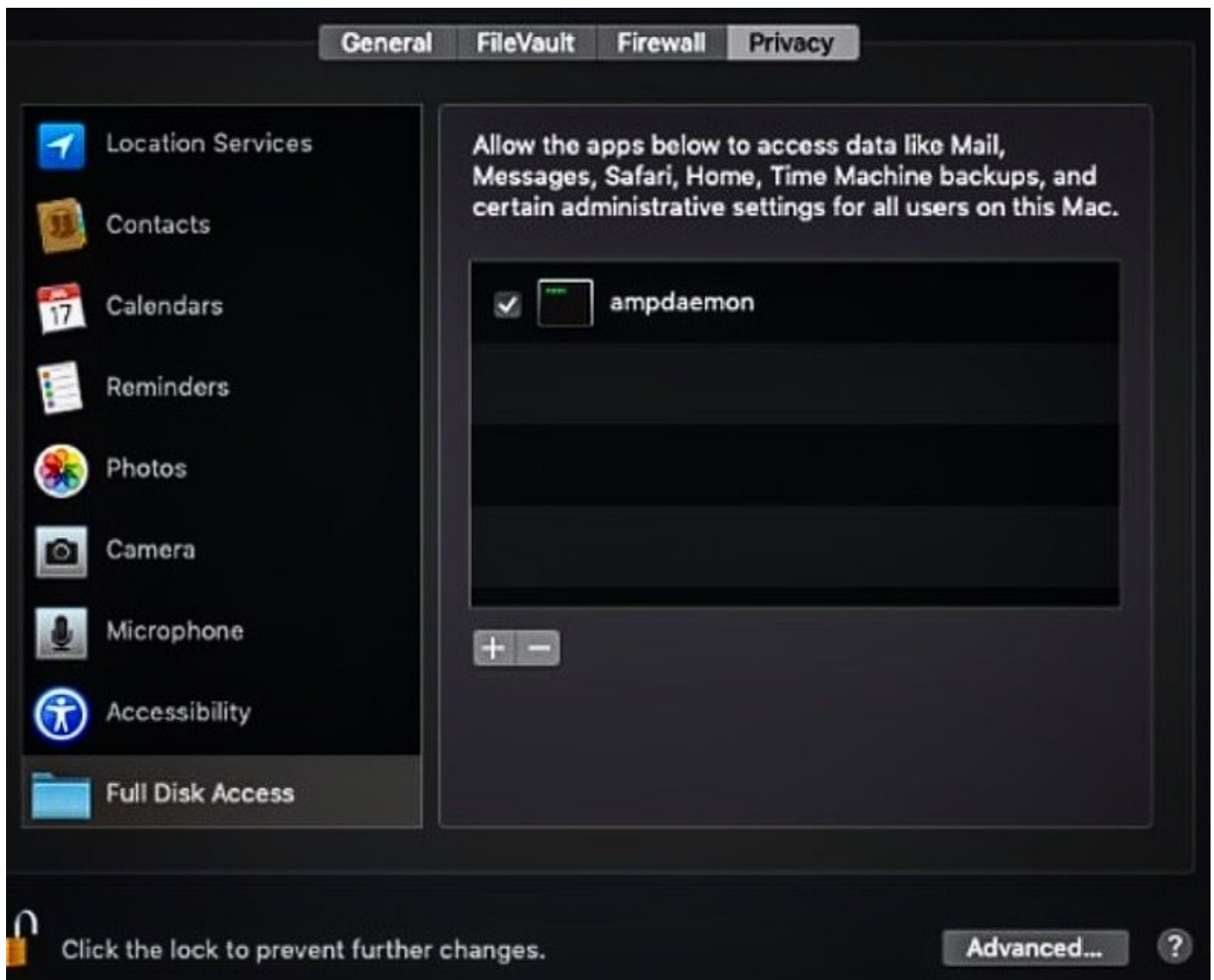
Grant Full Disk Access



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



Afin d'accorder l'accès au disque complet, donnez les autorisations Kernels et un redémarrage recommandé des périphériques MAC, au cours de l'intervalle de pulsation suivant, le message signalé disparaît de la console.