نواة MAC والوصول الكامل إلى القرص في نقاط النهاية AMP - وحدة التحكم

المحتويات

المقدمة

يصف هذه المستند خطوات استكشاف الأخطاء وإصلاحها في "الحماية المتقدمة من البرامج الضارة" (AMP) لنقاط النهاية للعمل على أخطاء MAC اثنين: الوصول الكامل إلى القرص (FDA) ووحدة kernel غير المعتمدة.

ساهم في هذا العمل أوريل توريس، خافيير جيسوس مارتينيز، مهندس Cisco TAC.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أدوات Mac
- حساب بامتيازات المسؤول

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى Cisco AMP لنقاط النهاية لـ MAC.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معينة:

- MacOS High Sierra 10.13

- MacOS 10.14 (Mojave)

القيود

هذا خطأ تجميلي في موصلات OSX و AMP المثبتة على OSV-10.4.X وإصدار الموصل 1.11.0.
تظهر بوابة AMP رسالة خطأ لـ FDA، ويبدي المضيف FDA مسموح به.
بق id: CSCvq98799

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المُستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

معلومات أساسية

عند تقديم طلب لتحميل KEXT، ولكن لم تتم الموافقة عليه بعد، يتم رفض طلب الحمل. يقدم MacOS High Sierra 10.13 ميزة جديدة، مما يعني أن المستخدم يتطلب الموافقة قبل تحميل امتدادات نواة الطرف الثالث المثبتة حديثا (KEXTs) ويتم تحميل امتدادات kernel المعتمدة فقط على النظام. يجب على المستخدم اتباع الخطوات المذكورة سابقا لحل خطأ kernel.
بما أن نظام التشغيل MacOS 10.14 (Mojave) يقدم ميزات أمان جديدة تؤثر على AMP لنقاط النهاية لموصلات Mac، فأنت بحاجة إلى التأكد من أن الوصول الكامل إلى القرص ممنوح للخوارزمية خدمة AMP، دون موافقة، لأن موصل AMP غير قادر على توفير الحماية أو الرؤية لهذه الأجزاء من نظام الملفات التي يتم حمايتها بواسطة MacOS.

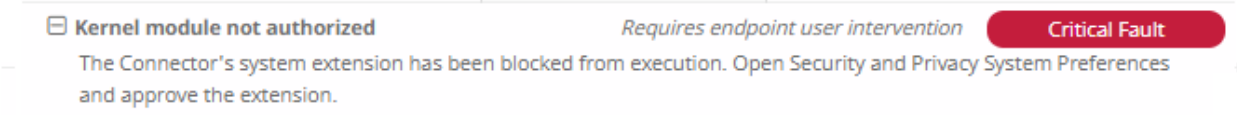
استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أخطاء وحدة التحكم

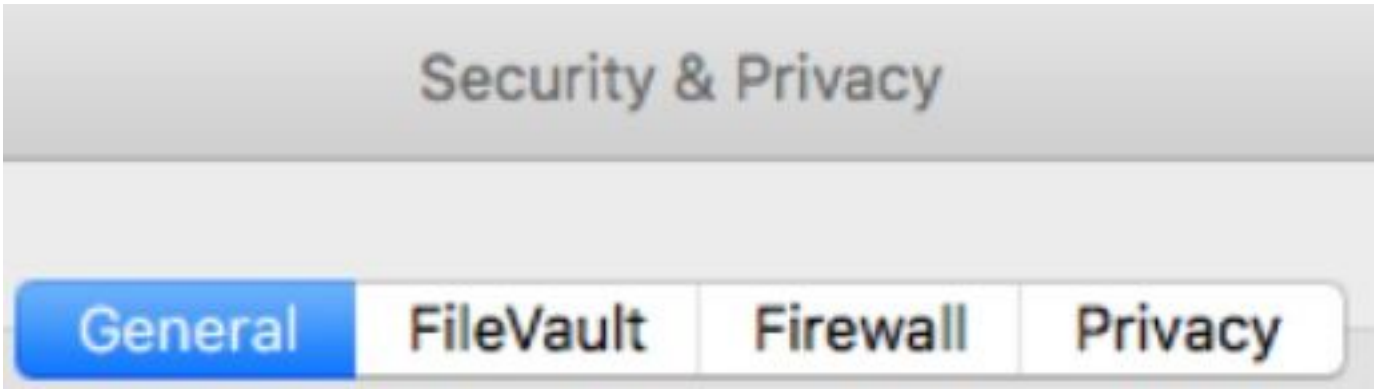
خطأ النواة

تظهر "وحدة تحكم AMP" الخطأ "وحدة Kernel النمطية غير المصرح بها" عند إجراء طلب لتحميل ملحق Kernel (KEXT) ولم تتم الموافقة عليه، ويتم رفض طلب التحميل ويقدم نظام التشغيل MacOS تنبيها، كما هو موضح في الصورة.

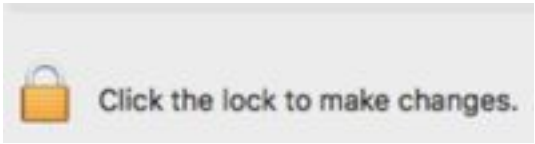


بعد ترقية Apple macOS، تم إطلاق إعلان رسمي حول موافقة kernel، كما هو موضح في الصورة.

للسماح بامتداد الموصل، انتقل إلى **تفضيلات النظام > الأمان والخصوصية > عامة** كما هو موضح في الصورة.



انقر فوق القفل للموافقة على KEXT (يتم تحميل ملحقات kernel التي يوافق عليها المستخدم على النظام فقط) كما هو موضح في الصورة.

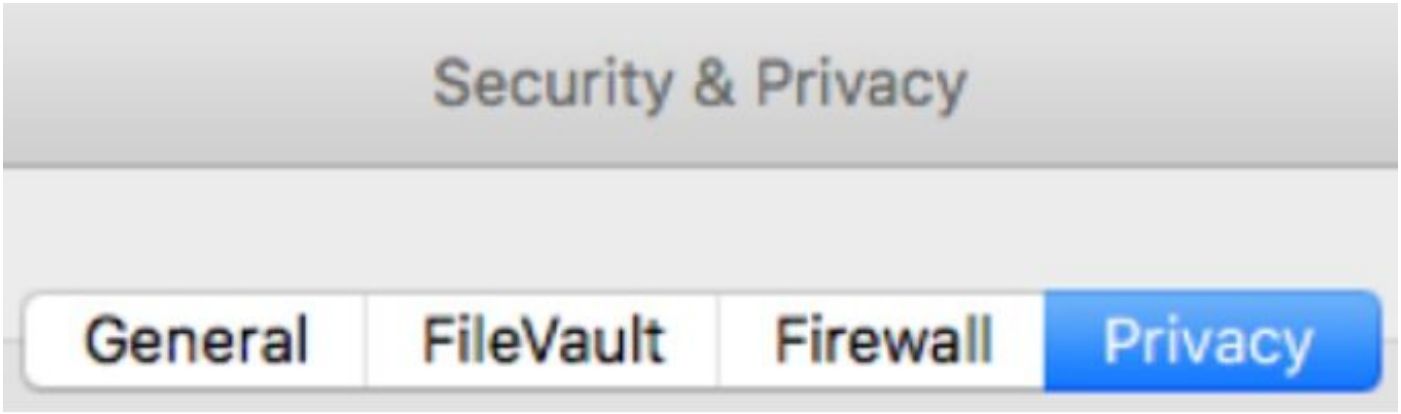


ملاحظة: يتم تقديم موافقة المستخدم في جزء تفضيلات الأمان والخصوصية لمدة 30 دقيقة بعد التنبيه. عندما يتم اعتماد KEXT، تتسبب محاولات التحميل المستقبلية في ظهور واجهة مستخدم الاعتماد مرة أخرى، ولكنها لا تقوم بتشغيل تنبيه مستخدم آخر.

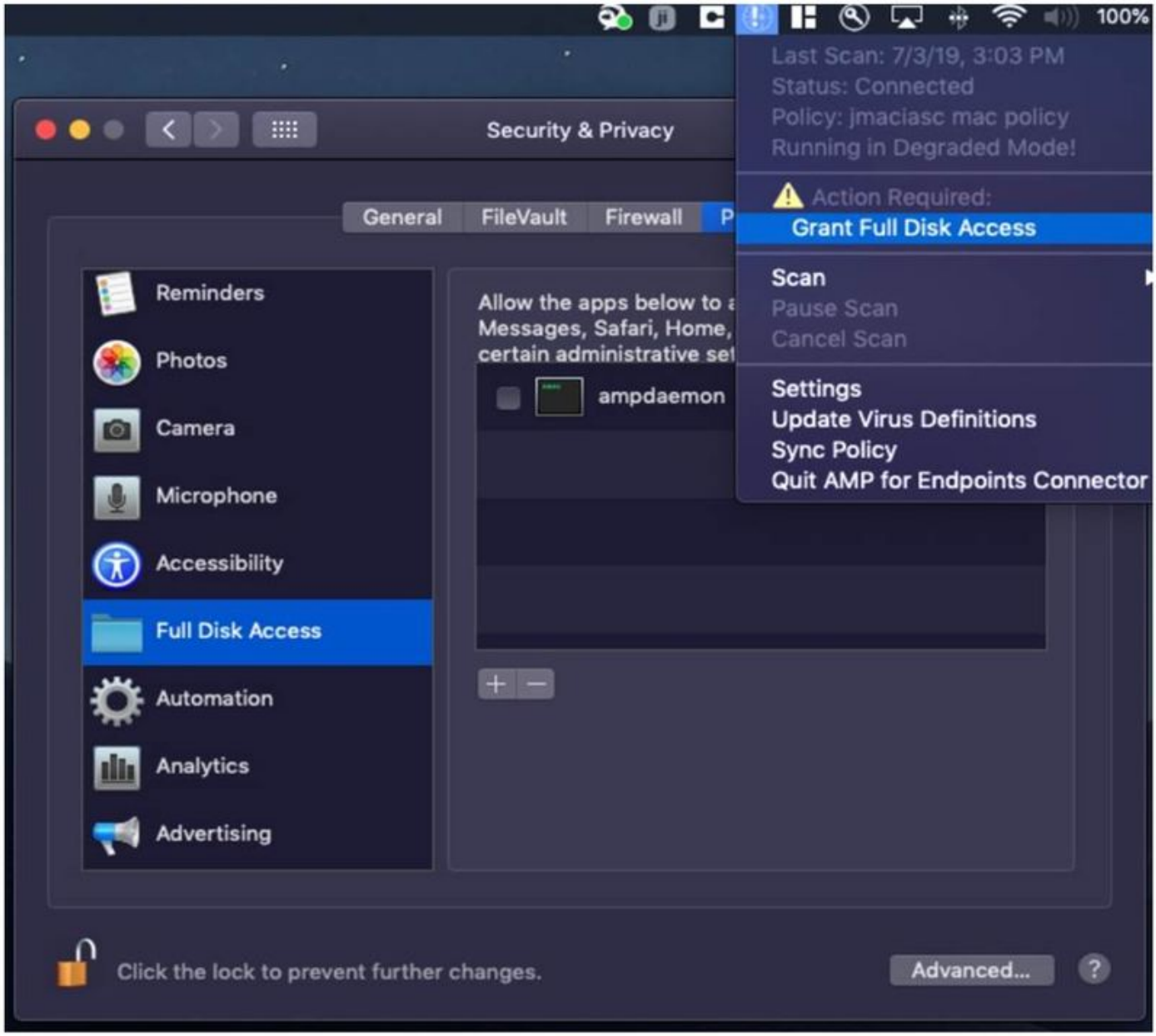
خطأ في الوصول الكامل للقرص

تظهر وحدة التحكم AMP "عدم منح الوصول إلى القرص" كما هو موضح في الصورة.

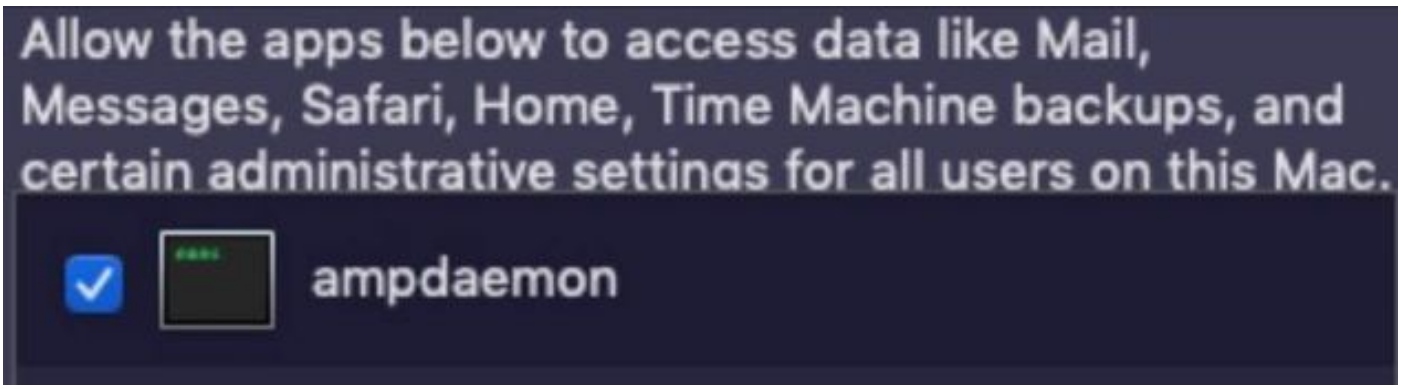
تحقق من عدم السماح بالوصول الكامل إلى القرص، انتقل إلى **تفضيلات النظام > الأمان والخصوصية > الخصوصية**، كما هو موضح في الصورة.



للموافقة على الوصول الكامل إلى القرص الخاص بموصل AMP، انتقل إلى "الوصول الكامل إلى القرص" ووضع علامة إختيار للعملية المتقدمة، كما هو موضح في الصورة.

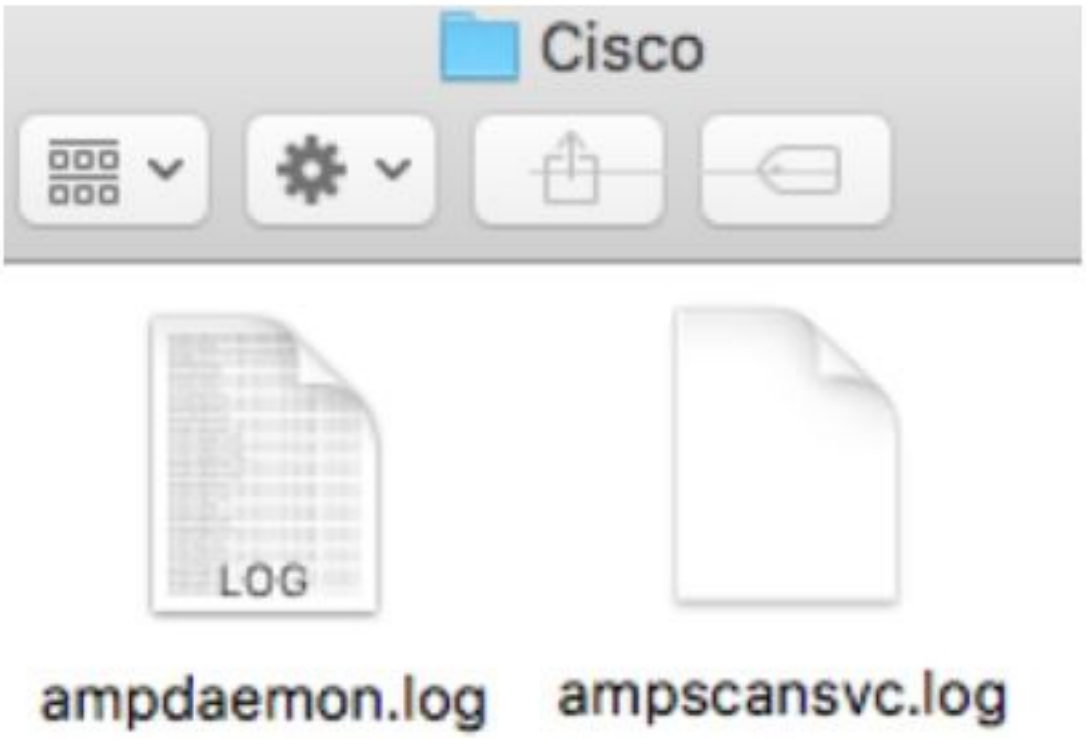


افتح وحدة طرفية وأوقف خدمة AMP وقم بتشغيل الأمر التالي: **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist**، كما هو موضح في الصورة.



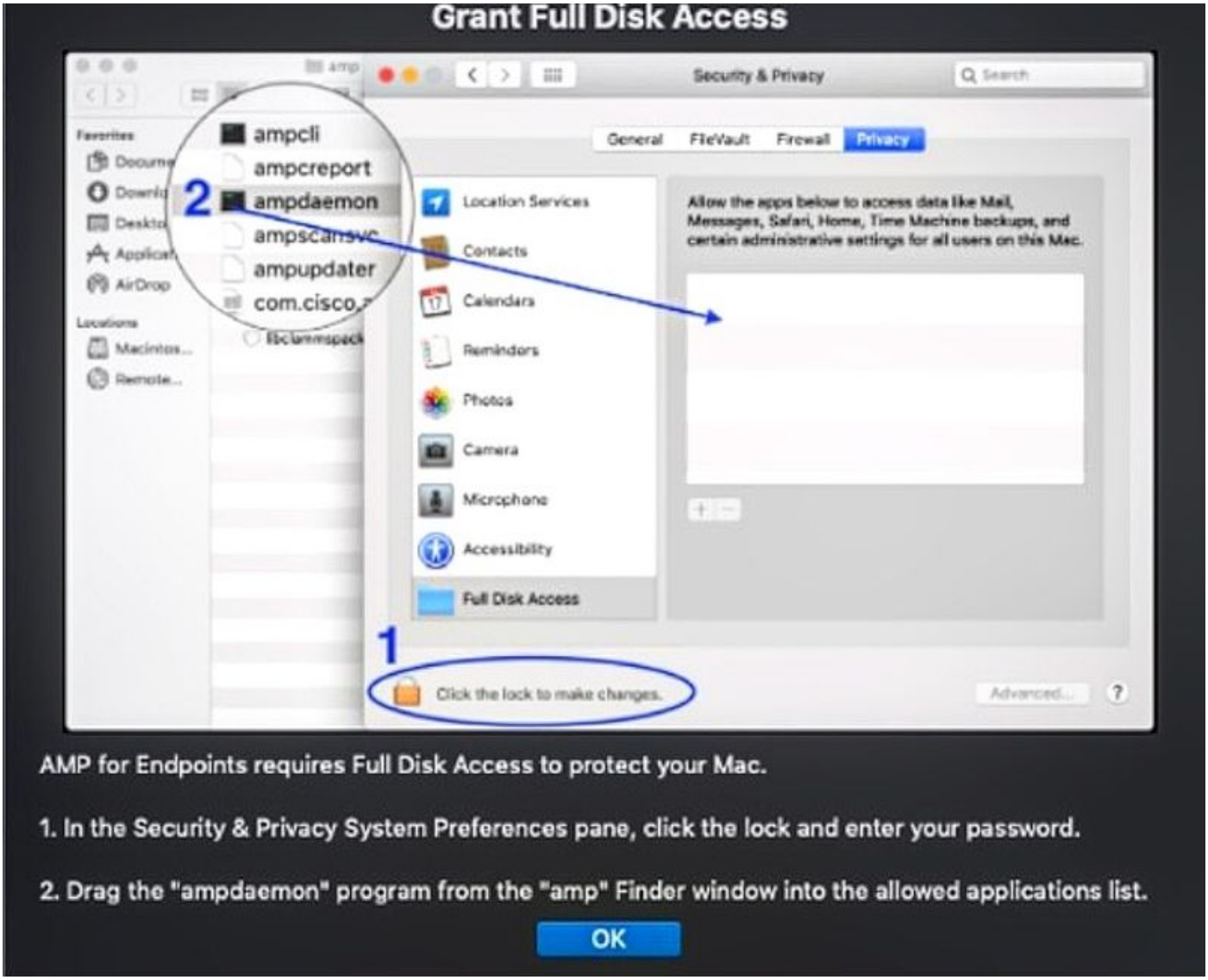
لتجنب حدوث مشاكل في التخزين المؤقت، انتقل إلى **/المكتبة/log/cisco** وامسح الملفات التالية، كما هو موضح في الصورة.

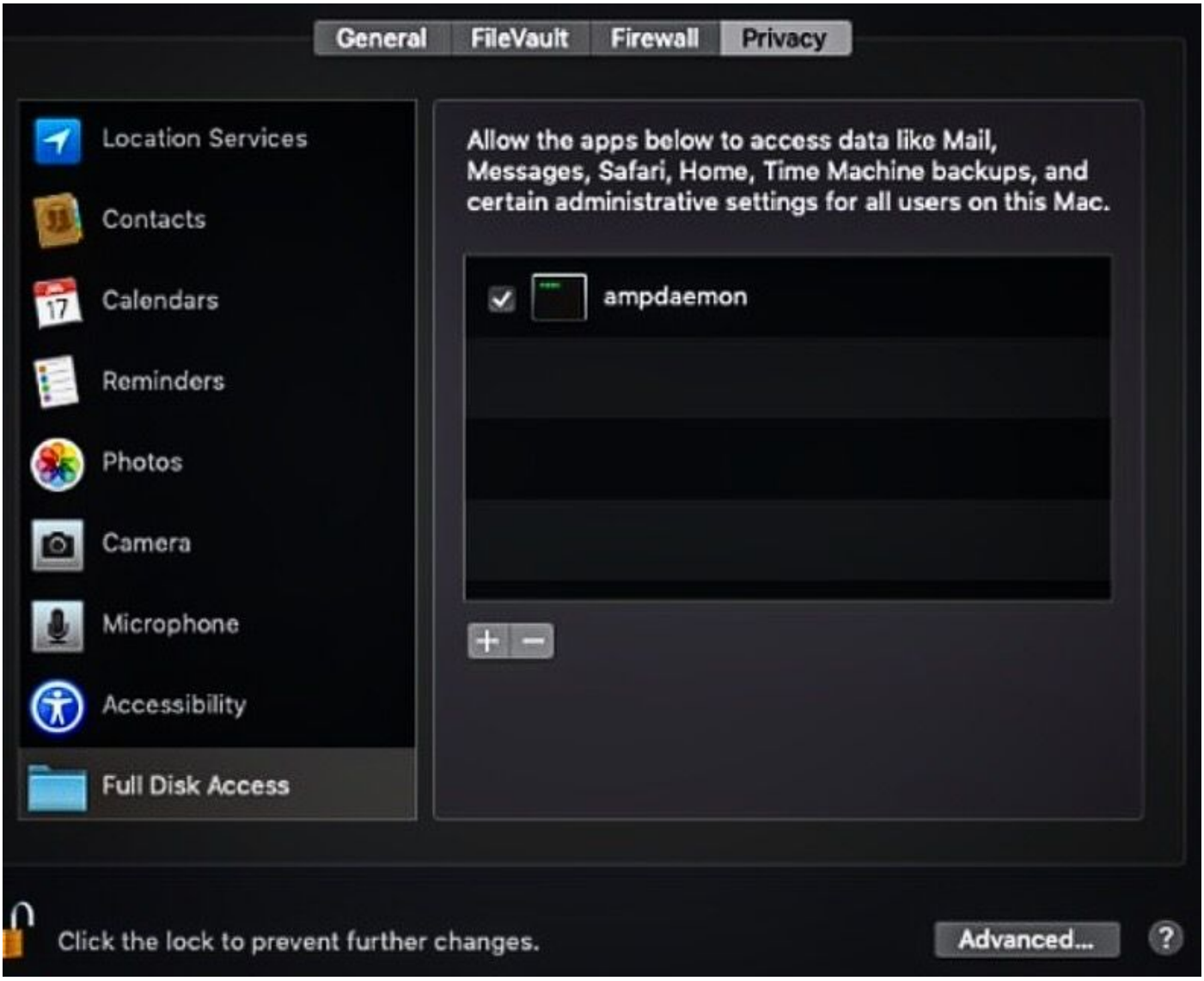
- أمبدامون لوغ
- amscanSVC.log



ابدأ الخدمة باستخدام الأمر: **sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

ملاحظة: في حالة عدم العثور على ملف الذاكرة المؤقتة، قم بسحبه وإسقاطه في سائمة السماح بالوصول الكامل إلى القرص، تأكد من وضع علامة على خانة الاختيار، كما هو موضح في الصورة.


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



لمنح حق الوصول الكامل إلى القرص، قم بمنح أذونات Kernel وإعادة تشغيل مستحسنة لأجهزة MAC، في الفاصل الزمني التالي لنبضات الفواصل، تختفي الرسالة التي تم الإبلاغ عنها من وحدة التحكم.

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).