콘솔에서 MAC 커널 및 전체 디스크 액세스 - AMP for Endpoints

목차

소개

이 문서에서는 AMP(Advanced Malware Protection) for Endpoints에서 두 가지 Mac Fault를 작동하는 문제를 해결하는 단계에 대해 설명합니다.FDA(Full Disk Access) 및 커널 모듈이 인증되지 않았습니다.

기고자: Uriel Torres, Javier Jesus Martinez, Cisco TAC 엔지니어

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

·Mac 툴 지식
·관리자 권한이 있는 계정

사용되는 구성 요소

이 문서의 정보는 Cisco AMP for Endpoints for MAC를 기반으로 합니다.

이 문서의 정보는 특정 환경의 디바이스에서 생성되었습니다.

- MacOS High Sierra 10.13

- MacOS 10.14(Mojave)

제한 사항

OSSV-10.4.X 및 커넥터 버전 1.11.0에 설치된 OX 및 AMP Connector의 코스메틱 버그입니다. AMP 포털에는 FDA에 대한 결함 메시지가 표시되고 호스트는 FDA가 허용됨을 보여줍니다.
버그 ID:CSCvq98799

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 이해해야 합니다.

배경 정보

KEXT를 로드하도록 요청했지만 아직 승인되지 않은 경우 로드 요청이 거부됩니다.MacOS High Sierra 10.13에는 새로운 기능이 도입되었습니다. 즉, 새로 설치된 KEXT(Third-Party Kernel Extensions)를 로드하기 전에 사용자가 승인을 받아야 하며 승인된 커널 확장만 시스템에 로드됩니다.사용자는 커널 오류를 해결하기 위해 앞서 언급한 단계를 따라야 합니다.
MacOS 10.14(Mojave)는 AMP for Endpoints Mac Connectors에 영향을 주는 새로운 보안 기능을 도입하기 때문에 승인 없이 AMP 서비스 데몬에 전체 디스크 액세스가 부여되도록 해야 합니다. AMP Connector는 macOS에서 보호하는 파일 시스템의 이러한 부분에 대한 보호 또는 가시성을 제공할 수 없습니다.

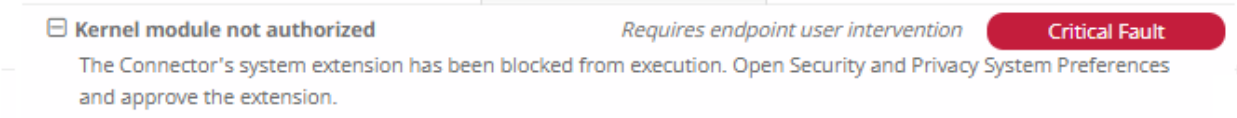
문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

콘솔 오류

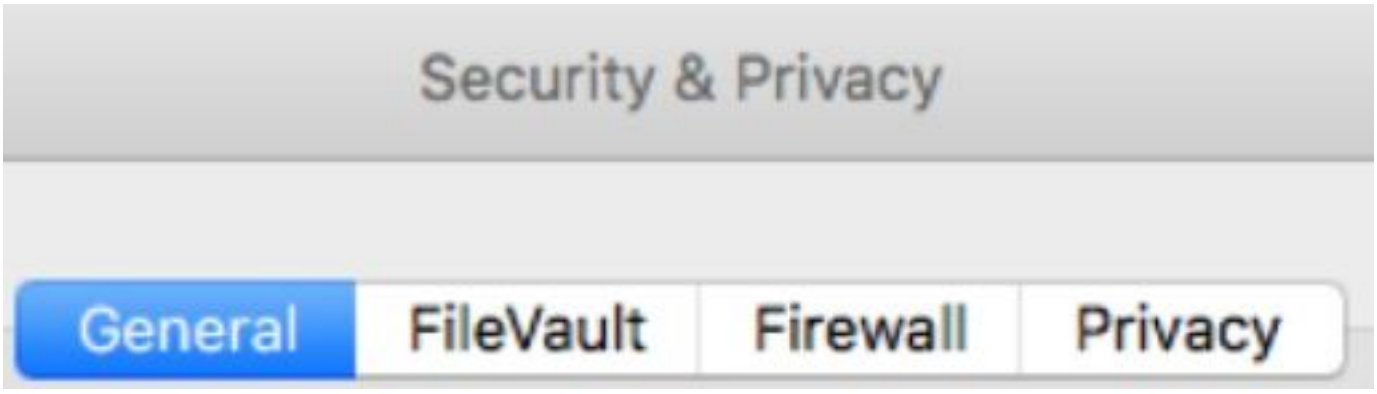
커널 결함

AMP Console은 KEXT(Kernel Extension)를 로드하도록 요청했지만 승인되지 않은 경우 "Kernel module not authorized(커널 모듈이 승인되지 않음)" 오류를 표시하며, 이미지에 표시된 것처럼 로드 요청이 거부되고 macOS가 알림을 표시합니다.

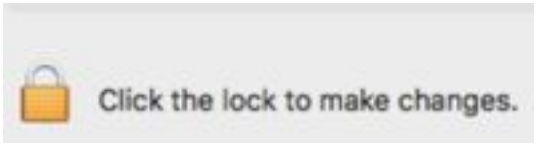


Apple macOS를 업그레이드한 후 이미지에 표시된 대로 커널 승인에 대한 공식 공지가 시작되었습니다.

커넥터 확장을 허용하려면 이미지에 표시된 대로 **System Preferences(시스템 환경 설정) > Security & Privacy(보안 및 개인 정보 보호) > General(일반)**으로 이동합니다.



Lock(잠금)을 클릭하여 이미지에 표시된 대로 KEXT(사용자가 승인한 커널 확장만 시스템에 로드됨)를 승인합니다.

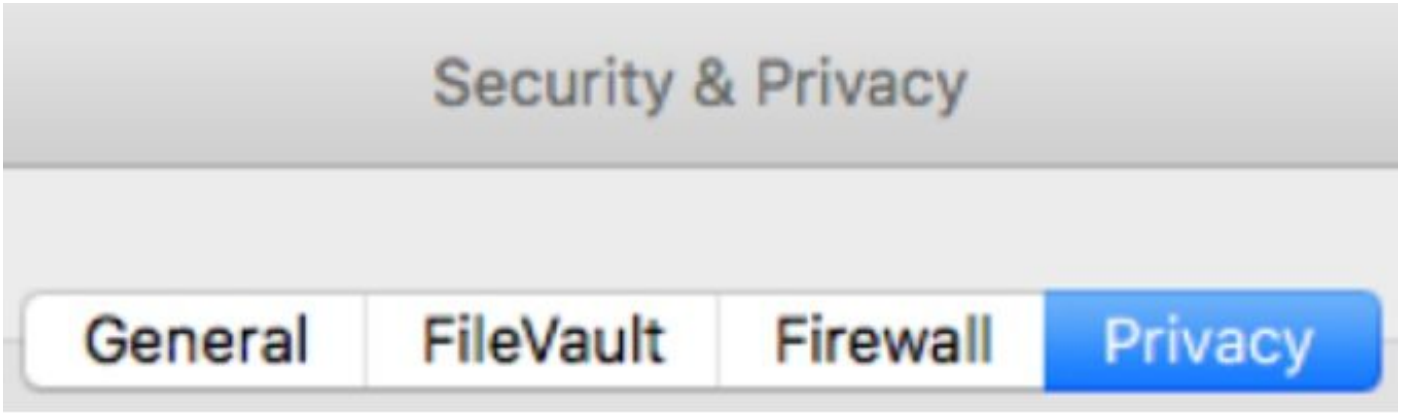


> **참고**: 사용자 승인은 알림 후 30분 동안 Security & Privacy Preferences 창에 표시됩니다.KEXT가 승인된 이후 로드 시도는 승인 사용자 인터페이스가 다시 나타나지만 다른 사용자 알림을 트리거하지 않습니다.

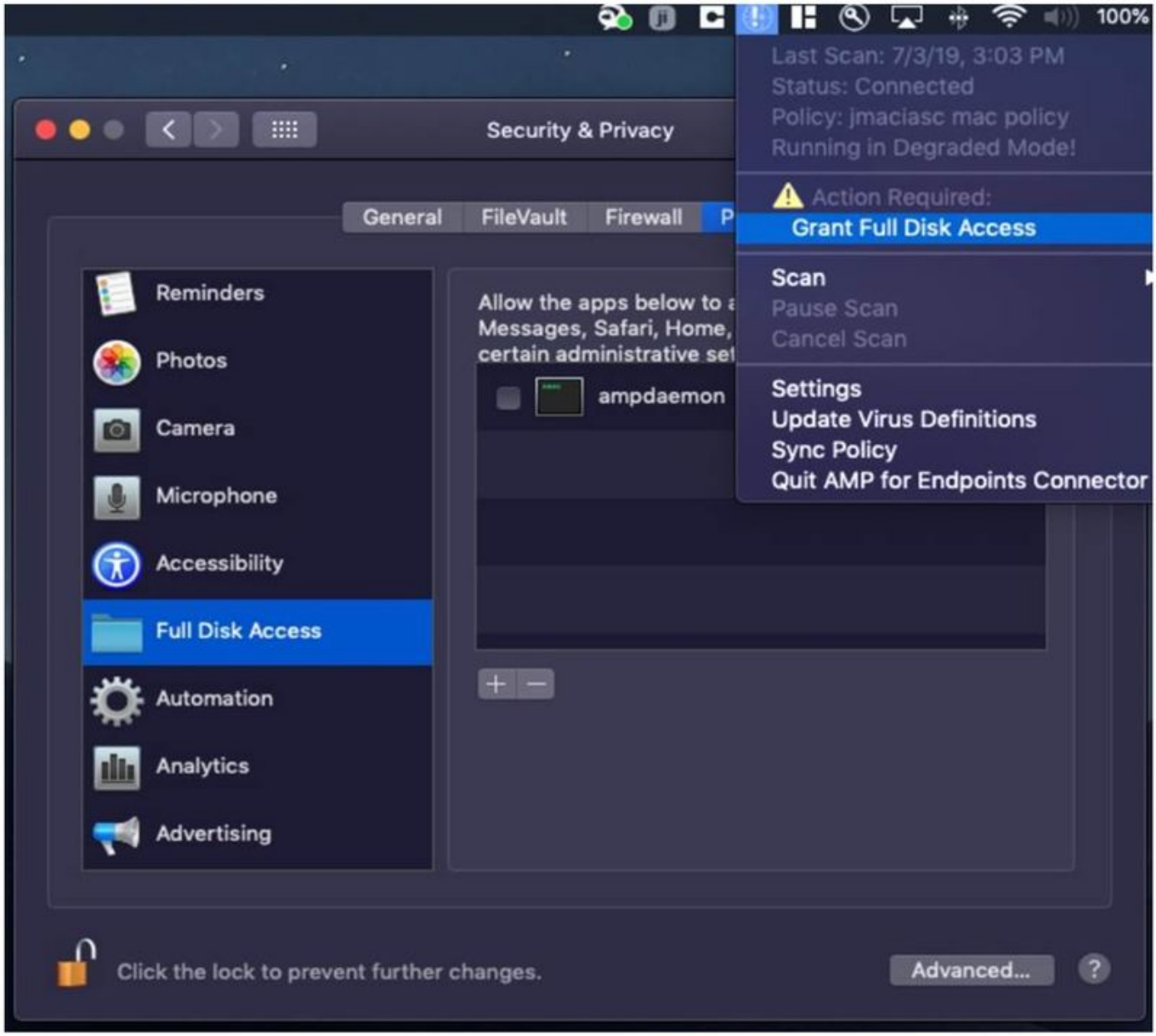
전체 디스크 액세스 장애

AMP 콘솔에는 이미지에 표시된 대로 "Disk Access not granted(디스크 액세스가 허용되지 않음)"가 표시됩니다.

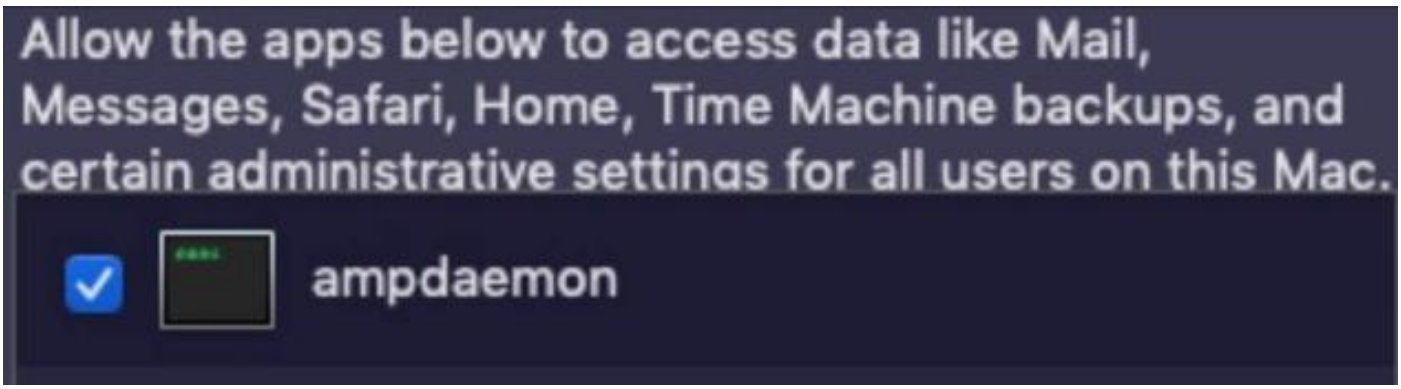
전체 디스크 액세스가 허용되지 않는지 확인하려면 이미지에 표시된 대로 **System Preferences > Security & Privacy > Privacy**로 이동합니다.



AMP 커넥터의 전체 디스크 액세스를 승인하려면 Full Disk Access(전체 디스크 액세스)로 이동하여 이미지에 표시된 대로 ampdaemon 프로세스를 선택합니다.

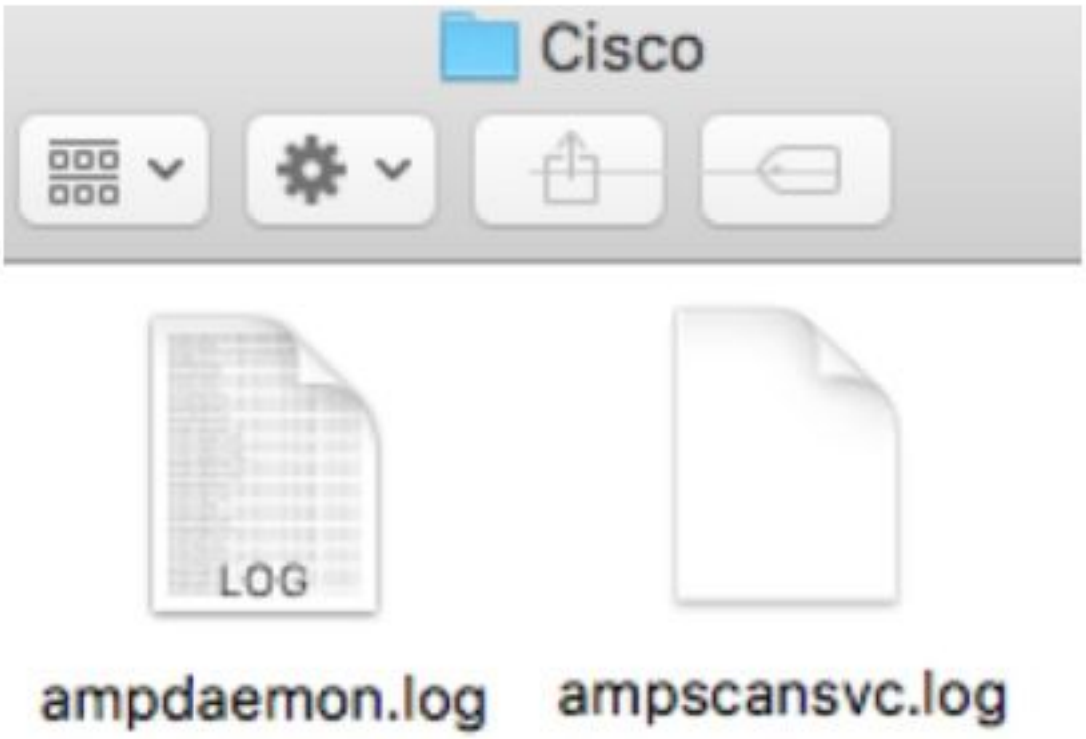


터미널을 열고 AMP 서비스를 중지하고 다음 명령을 실행합니다. **sudo /bin/launchctl unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** 이미지에 표시된 대로 확인란을 선택합니다.



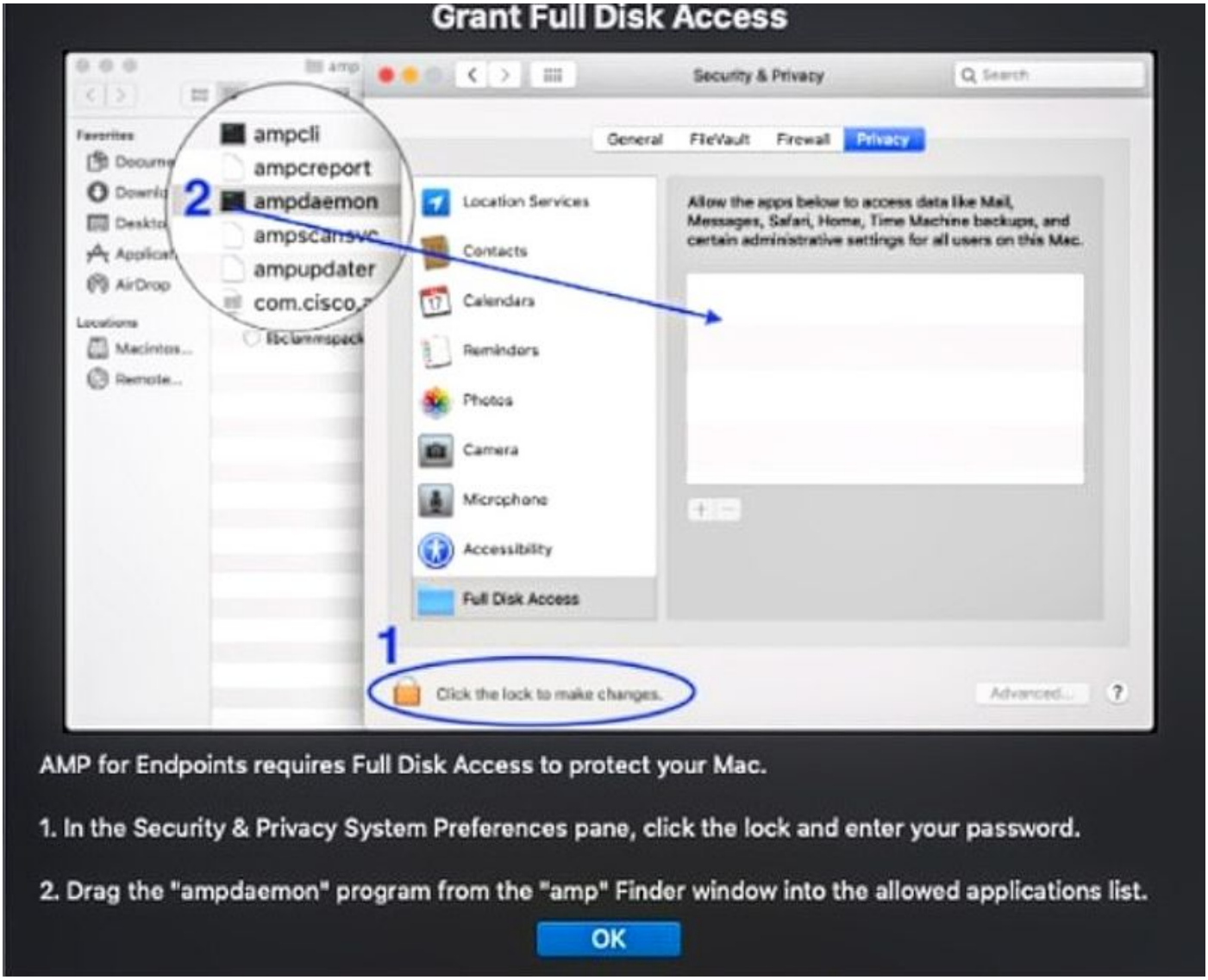
캐시 문제를 방지하려면 이미지에 표시된 대로 **/library/logs/cisco**로 이동하여 다음 파일을 지웁니다.

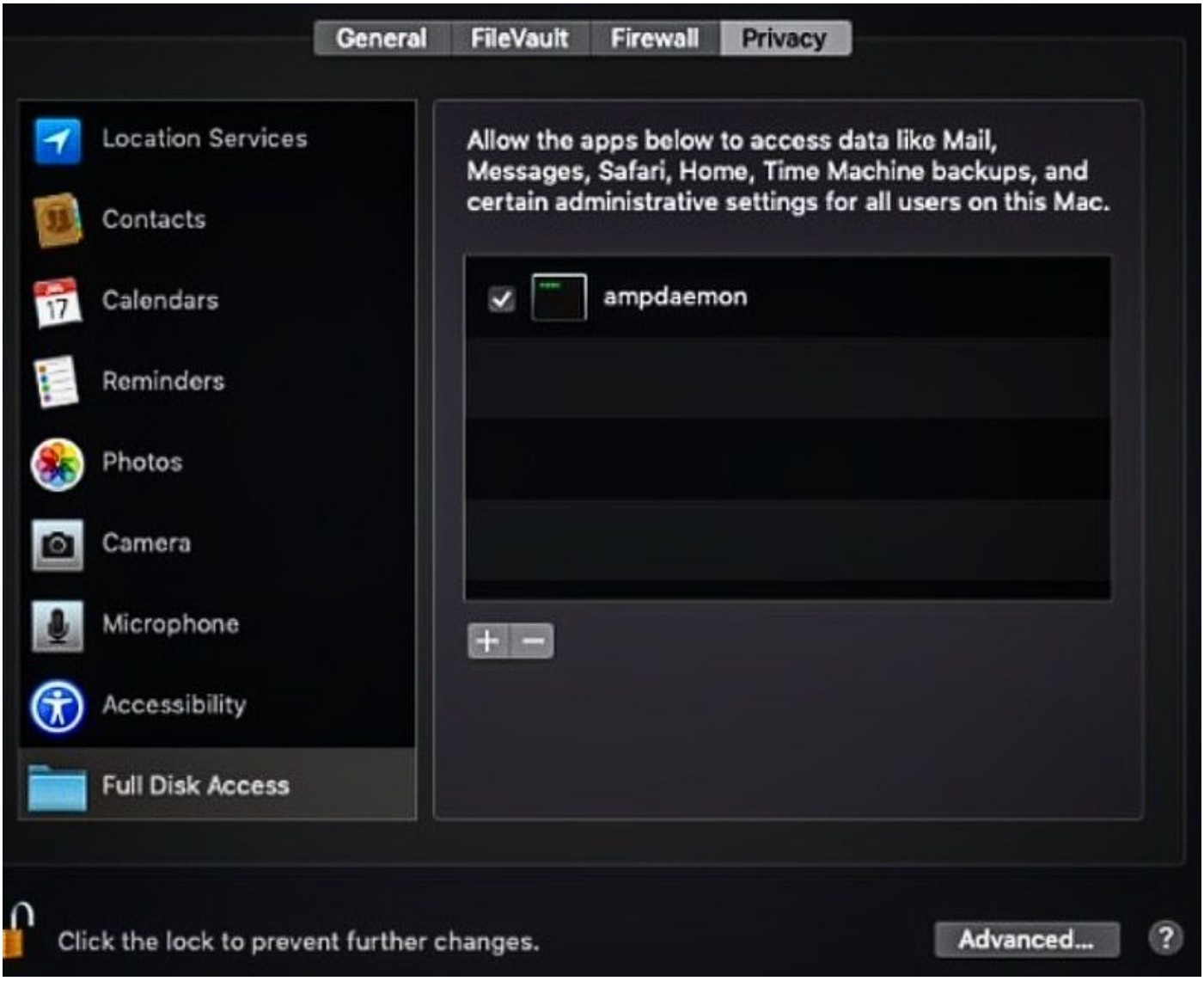
- ampdaemon.log
- ampscansvc.log



sudo /bin/launchctl load /Library/LaunchDaemons/com.cisco.amp.daemon.plist 명령을 사용하여 서비스를 시작합니다.

참고: 앰폴 파일을 찾을 수 없는 경우 전체 디스크 액세스 허용 목록에 끌어서 놓고 이미지에 표시된 대로 확인란이 선택되어 있는지 확인합니다.


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



전체 디스크 액세스 권한을 부여하려면 커널에 사용 권한을 부여하고 MAC 디바이스를 권장 재부팅합니다. 다음 하트비트 간격 동안 보고된 메시지가 콘솔에서 사라집니다.