Kernel MAC e accesso completo al disco nella console - AMP for Endpoints

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi in Advanced Malware Protection (AMP) affinché gli endpoint funzionino con due errori Mac: Accesso completo al disco (FDA) e modulo del kernel non autorizzati.

Contributo di Uriel Torres, Javier Jesus Martinez, Cisco TAC Engineers.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

·Conoscenza degli strumenti Mac
·Account con privilegi di amministratore

Componenti usati

Le informazioni di questo documento si basano su Cisco AMP for Endpoints per MAC.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente:

- MacOS High Sierra 10.13
- MacOS 10.14 (Mojave)

Limitazioni

Si tratta di un bug cosmetico sui connettori OSX e AMP installati su OSV-10.4.X e sul connettore versione 1.11.0. Sul portale AMP viene visualizzato un messaggio di errore per FDA e l'host indica che FDA è consentito.
ID bug: CSCvq98799

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando viene effettuata una richiesta di caricamento di un KEXT, ma non ancora approvata, la richiesta di caricamento viene negata. MacOS High Sierra 10.13 introduce una nuova funzione, il che significa che l'utente richiede l'approvazione prima di caricare le nuove estensioni del kernel di terze parti (KEXT) e solo le estensioni del kernel approvate sono caricate su un sistema. Per risolvere l'errore del kernel, l'utente deve eseguire la procedura descritta in precedenza.
Poiché macOS 10.14 (Mojave) introduce nuove funzioni di sicurezza che interessano AMP for Endpoints Mac Connector, è necessario garantire l'accesso completo al disco al daemon del servizio AMP, senza approvazione, AMP Connector non è in grado di fornire protezione o visibilità a queste parti del file system protette da macOS.

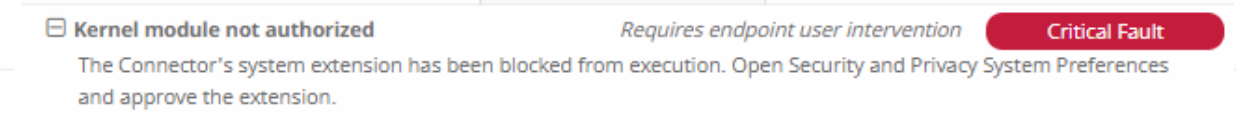
Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Errori console

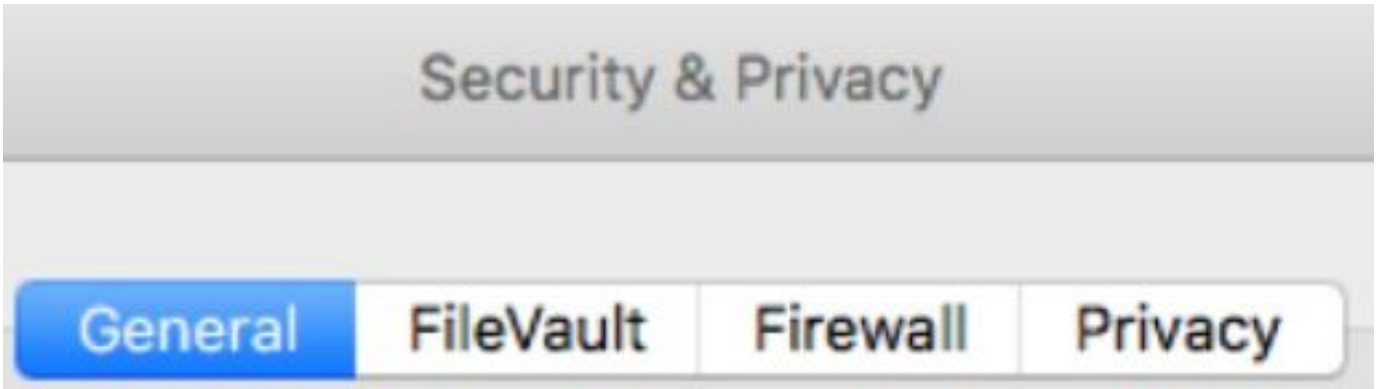
Errore kernel

AMP Console visualizza l'errore "Modulo kernel non autorizzato" quando viene effettuata una richiesta di caricamento di un'estensione del kernel (KEXT) e questa non viene approvata, la richiesta di caricamento viene negata e macOS presenta un avviso, come mostrato nell'immagine.

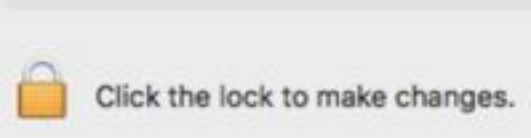


Dopo l'aggiornamento di Apple macOS, è stato lanciato un annuncio ufficiale sull'approvazione del kernel, come mostrato nell'immagine.

Per consentire l'estensione Connettore, selezionare **System Preferences > Security & Privacy > General** (Preferenze di sistema > Protezione e privacy > Generale), come mostrato nell'immagine.



Fare clic sul blocco per approvare il KEXT (solo le estensioni del kernel approvate dall'utente sono caricate su un sistema), come mostrato nell'immagine.

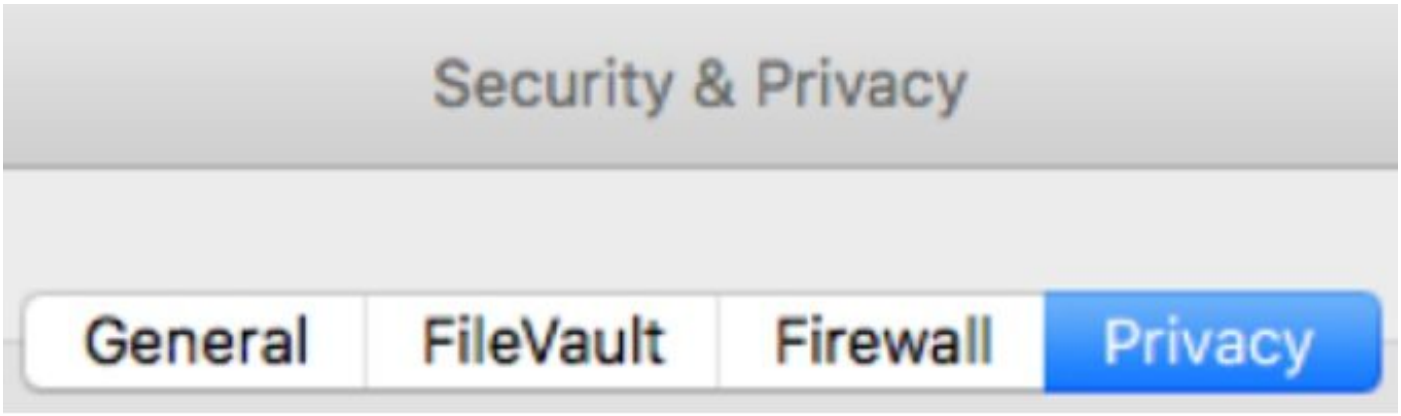


Nota: l'approvazione dell'utente viene presentata nel riquadro delle preferenze Protezione e privacy per 30 minuti dopo l'avviso. Quando il KEXT viene approvato, i futuri tentativi di caricamento determinano la visualizzazione dell'interfaccia utente di approvazione, ma non attivano un altro avviso utente.

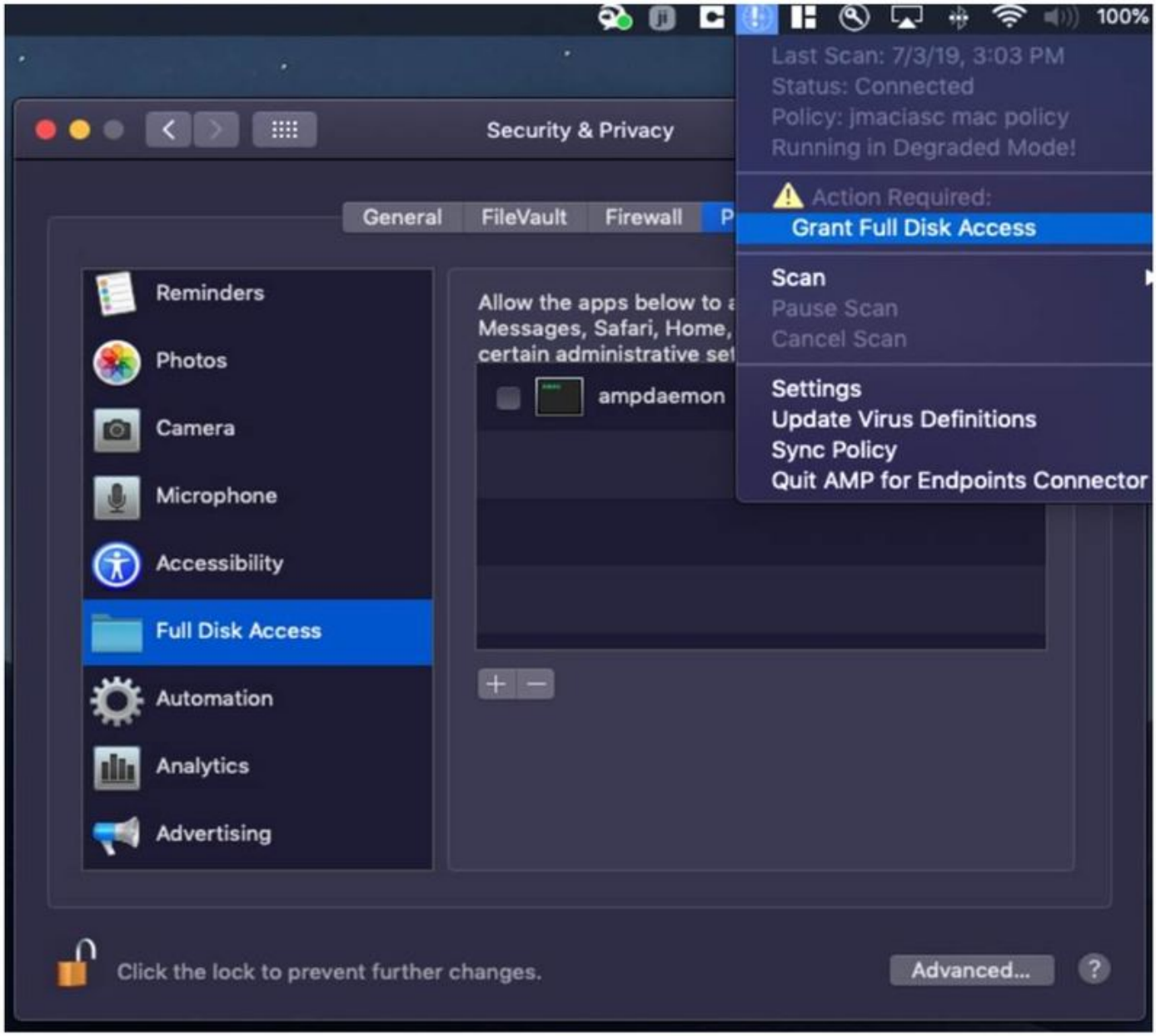
Errore di accesso completo al disco

Nella console AMP viene visualizzato il messaggio "Accesso al disco non concesso", come illustrato nell'immagine.

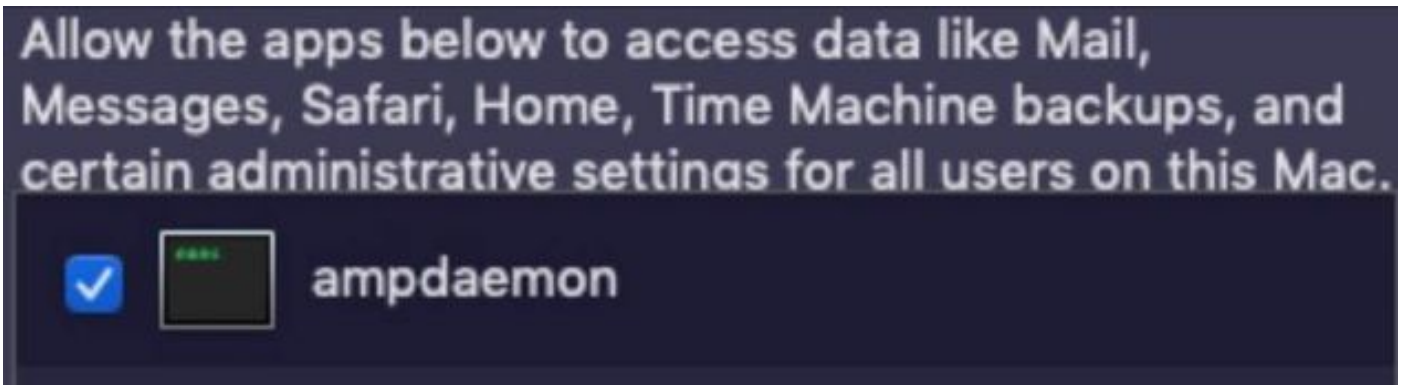
Verificare che l'accesso completo al disco non sia consentito, selezionare **System Preferences > Security & Privacy > Privacy,** come mostrato nell'immagine.



Per approvare l'accesso completo al disco del connettore AMP, passare ad Accesso completo al disco e selezionare il processo ampdaemon, come mostrato nell'immagine.

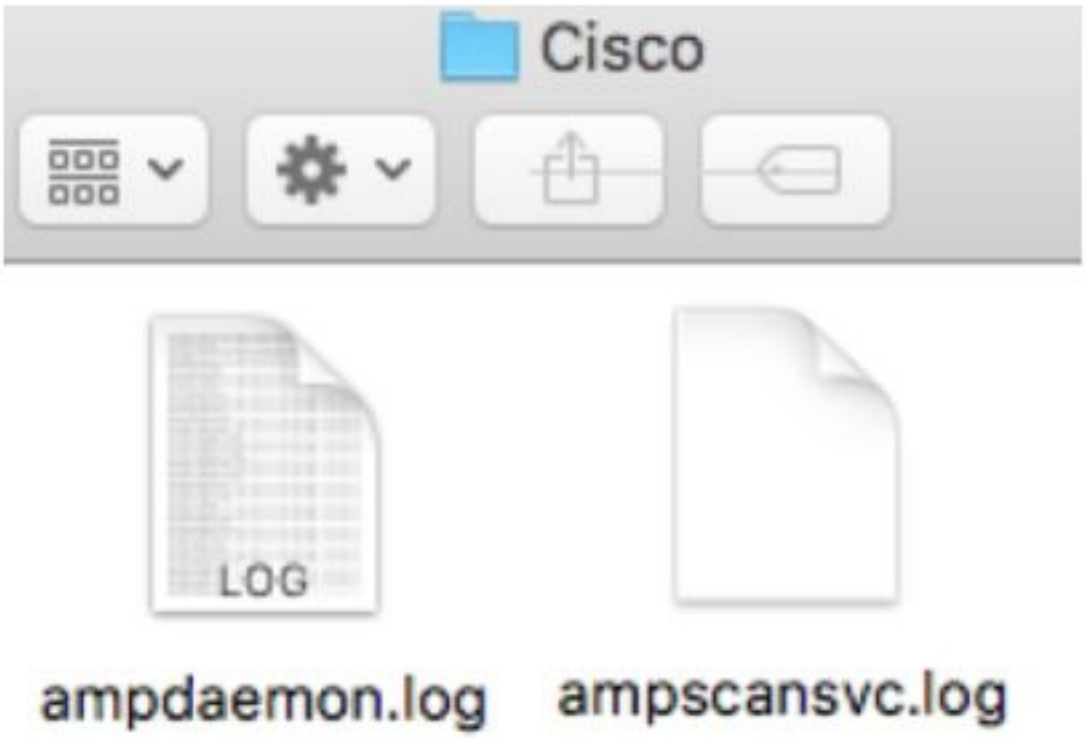


Aprire un terminale, arrestare il servizio AMP ed eseguire il comando successivo: **sudo /bin/LAUNCHCTL unload /Library/LaunchDaemons/com.cisco.amp.daemon.plist,** selezionare la casella di controllo, come mostrato nell'immagine.



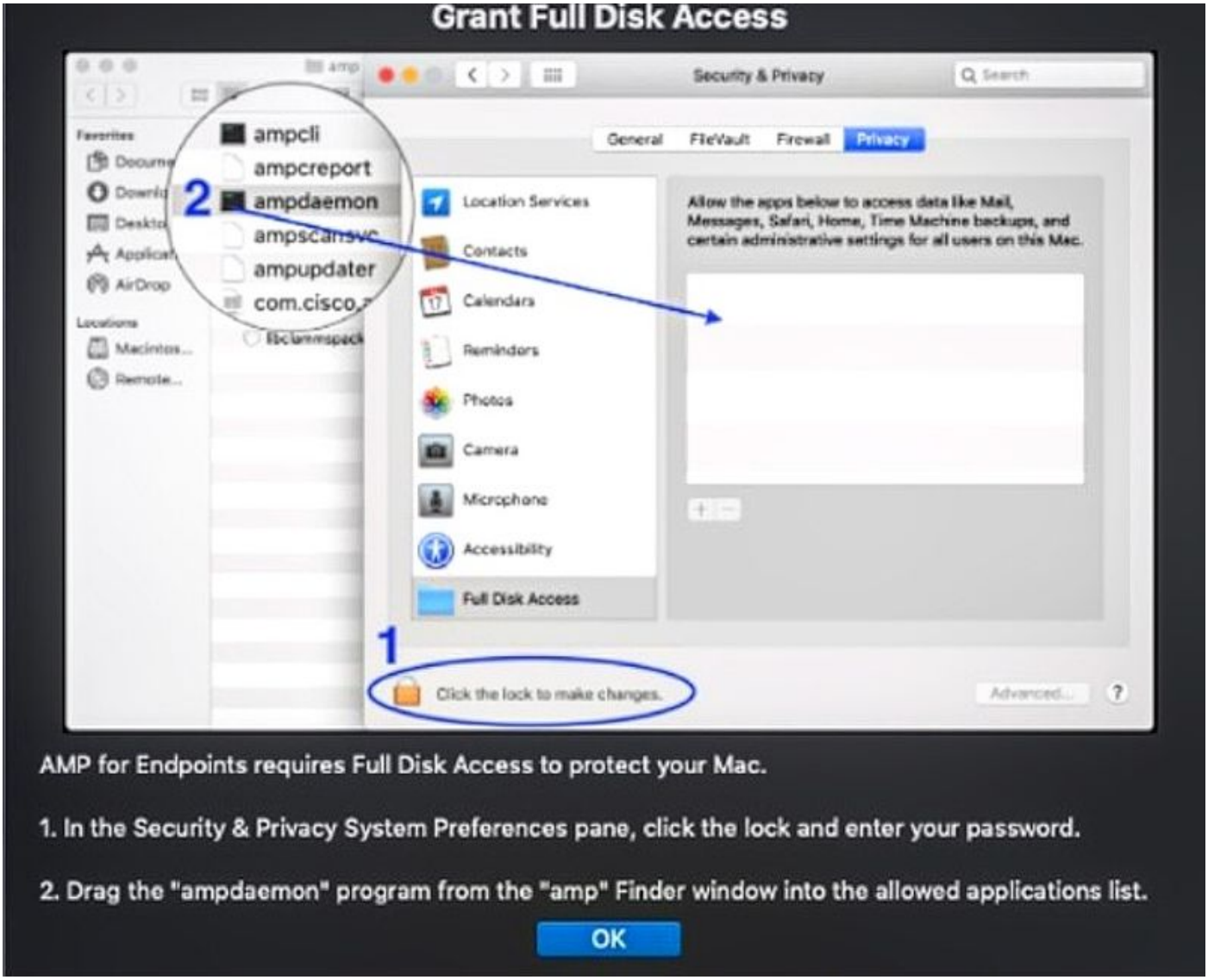
Per evitare problemi di cache, passare a **/library/logs/cisco** e cancellare i file successivi, come mostrato nell'immagine.

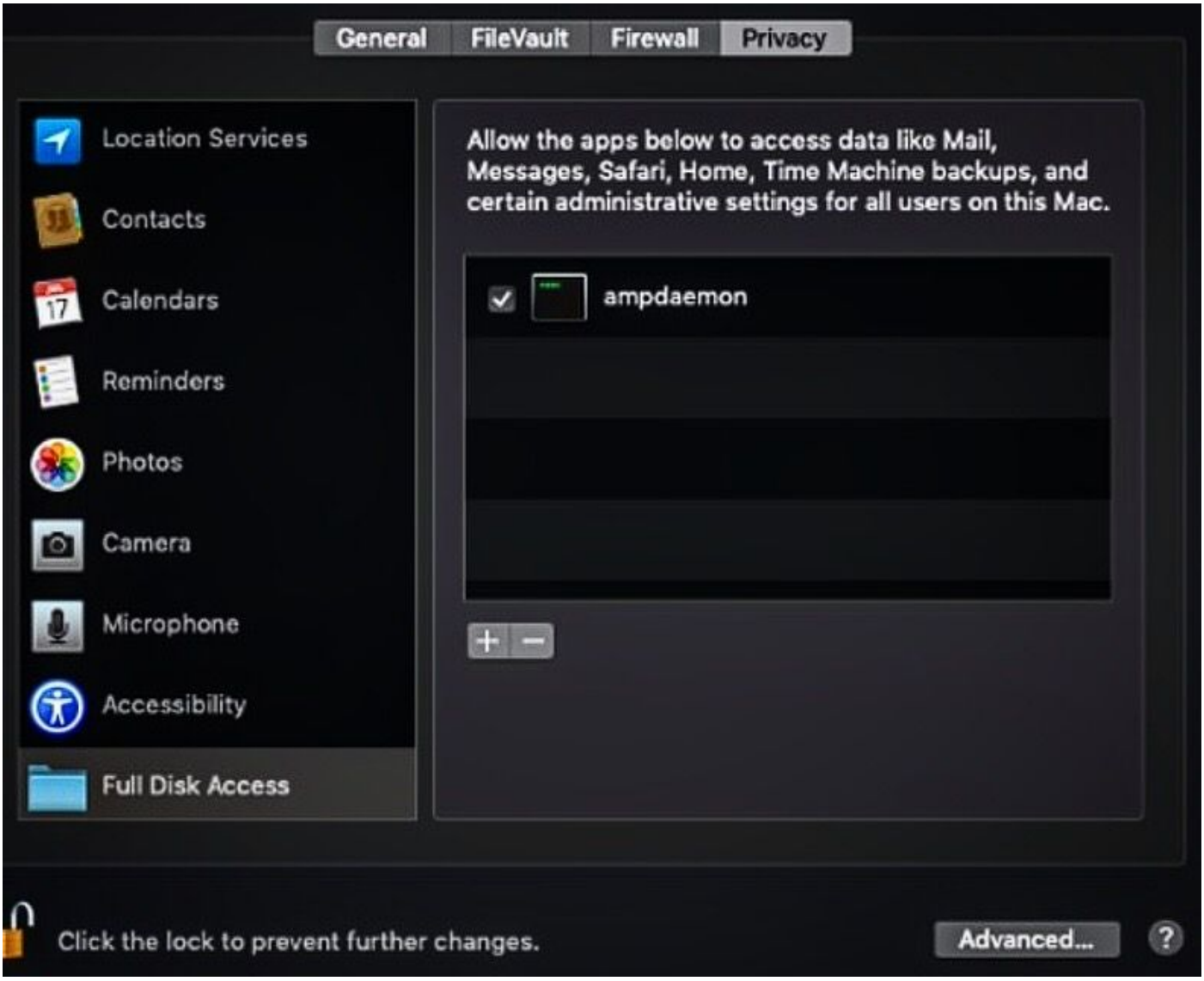
- ampdaemon.log
- ampscansvc.log



Avviare il servizio con il comando **sudo /bin/LAUNCHCTL load /Library/LaunchDaemons/com.cisco.amp.daemon.plist**.

> **Nota:** Se non è possibile trovare il file ampdeamon, trascinarlo nell'elenco Consenti accesso completo al disco e assicurarsi che la casella di controllo sia contrassegnata, come mostrato nell'immagine.


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



Per concedere l'accesso completo al disco, assegnare ai kernel le autorizzazioni e un riavvio consigliato dei dispositivi MAC, nel successivo intervallo di heartbeat il messaggio segnalato scompare dalla console.