Configure Permissions for Secure Endpoint Mac Connector and Orbital with MDM: Full Disk Access, System Extensions

Contents

Introduction

This document describes recent changes and steps for administrators to deploy Mac connector 1.14 and newer.

MDM Profiles

It is highly recommended to deploy the Mac connector with an MDM profile that grants the required approvals. MDM profiles must be installed before installation, upgrade, or removal of the Mac connector to ensure the needed permissions are recognized. Refer to the Known Issues section later in this document if MDM cannot be used.

Advisories

Mac connector version 1.14 introduced changes that require attention:

- Full disk access approval
- System Extension approval

Mac connector 1.14 or newer is required to ensure endpoint protection on macOS 11 and later. Older Mac connectors do not work on these versions of macOS.

Mac connector version 1.16 introduced support for Cisco Orbital on Intel hardware. Orbital can be enabled in policy with the Advantage or Premier Tier and is installed automatically when enabled and installed on a supported OS version and supported hardware. Mac connector version 1.20 introduces support readiness for Cisco Orbital on Apple silicon hardware, planned for release with Orbital Node 1.21. Refer to the Cisco Orbital sections of this document for details on how to grant the additional full disk access permissions needed for Orbital.

Minimum OS Requirements

Cisco Secure Endpoint Mac connector 1.14.0 supports macOS versions:

- macOS 11, with macOS system extensions.
- macOS 10.15.5 and later, with macOS system extensions.
- macOS 10.15.0 through macOS 10.15.4, with macOS kernel extensions.
- macOS 10.14, with macOS kernel extensions.

Cisco Secure Endpoint Mac connector 1.14.1 supports macOS versions:

- macOS 11, with macOS system extensions.
- macOS 10.15 with macOS kernel extensions.
- macOS 10.14, with macOS kernel extensions.

Support for Cisco Orbital on Intel hardware was introduced in Secure Endpoint Mac connector version 1.16.0. Support for Cisco Orbital on Apple silicon hardware was introduced in Secure Endpoint Mac connector version 1.20.0.

Consult the OS Compatibility Table for current Mac connector compatibility.

Important Changes

Mac connector 1.14 introduced important changes in three areas:

1. Approval of the macOS Extensions used by the connector
2. Full Disk Access
3. New Directory Structure

MacOS 12 introduced an MDM option to allow removal of the macOS Extensions of the connector without a prompt for user passwords.

Approval of the Mac Connector macOS Extensions

The Mac connector uses either System Extensions or legacy Kernel Extensions to monitor system activities, as needed for the macOS version. On macOS 11, System Extensions replace the legacy Kernel Extensions that are unsupported in macOS 11 and later. User approval is required on all versions of macOS before either type of extension is allowed to run. Without approval, certain connector functions such as on-access file scan and network access monitor are unavailable.

Mac connector 1.14 introduces two new macOS system extensions:

1. An Endpoint Security extension, named Secure Endpoint File Monitor (formerly AMP Security Extension), to monitor system events
2. A Network Content Filter extension, named Cisco Secure Endpoint Filter (formerly AMP Network Extension), to monitor network access

The two legacy Kernel Extensions, `ampfileop.kext` and `ampnetworkflow.kext`, are included for backwards compatibility on older macOS versions that do not support the new macOS System Extensions.

The approvals required for macOS 11** and later:

- Approve Secure Endpoint File Monitor to load
- Approve Cisco Secure Endpoint Filter to load
- Allow Cisco Secure Endpoint Filter to filter network content

** Mac connector version 1.14.0 also required these approvals on macOS 10.15. These approvals are no longer required on macOS 10.15 for Mac connector 1.14.1 or newer.

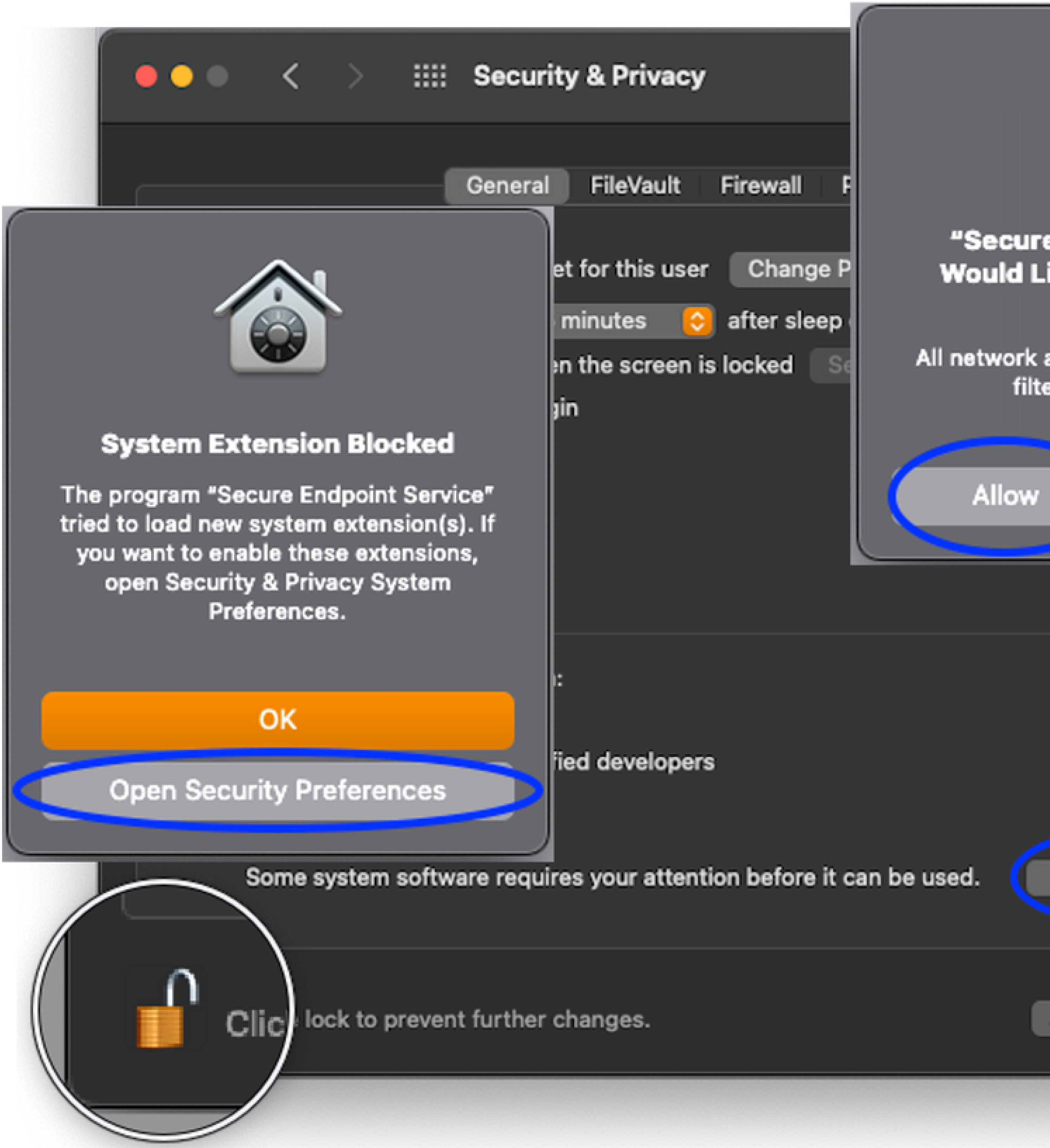
The approvals required for macOS 10.14 and macOS 10.15:

- Approve connector Kernel Extensions to load

These approvals can be granted in the macOS Security & Privacy Preferences on the endpoint, or through Mobile Device Management (MDM) profiles.

Approval of the Mac Connector macOS Extensions at the Endpoint

System and Kernel extensions can be approved manually from the macOS Security & Privacy Preferences pane.



System Extension Blocked

The program "Secure Endpoint Service" tried to load new system extension(s). If you want to enable these extensions, open Security & Privacy System Preferences.

Some system software requires your attention before it can be used.

Approval of the Mac Connector macOS Extensions with MDM

NOTE: macOS Extensions cannot be retroactively approved via MDM. If the MDM profile is not deployed prior to install of the connector then the approvals are not granted and additional intervention is required in one of two forms:

1. Manual approval of the macOS Extensions on endpoints that had the management profile deployed retroactively.

2. Upgrade the Mac connector to a newer version than the one currently deployed. Endpoints that had themanagement profile deployed retroactively recognize the management profile after an upgrade and gain approval once the upgrade completes.

Secure Endpoint extensions can be approved with a management profile with these payloads and properties:

Payload	Property	Value
SystemExtensions	AllowedSystemExtensions	com.cisco.endpoint.svc.securityextensi com.cisco.endpoint.svc.networkextensi
	AllowedSystemExtensionTypes	EndpointSecurityExtension, NetworkExtension
	AllowedTeamIdentifiers	DE8Y96K9QP
SystemPolicyKernelExtensions	AllowedKernelExtensions	com.cisco.amp.fileop, com.cisco.amp.n
	AllowedTeamIdentifiers	TDNYQP7VRK
WebContentFilter	AutoFilterEnabled	false
	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.networkextensi
	FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc.networkextens and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* ex */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU DE8Y96K9QP)
	FilterGrade	firewall
	FilterBrowsers	false
	FilterPackets	false
	FilterSockets	true
	PluginBundleID	com.cisco.endpoint.svc
	UserDefinedName	Cisco Secure Endpoint Filter (AMP Network Extension if connector versio older than 1.18.0)

Removal of the Mac Connector macOS Extensions with MDM

MacOS 12 and later allows macOS Extensions to be marked as removable with the RemovableSystemExtensions property as described below.
NOTE: When macOS Extension removable permission is allowed, any user or process with root privileges has the ability to remove the extension without a prompt for the user password. Thus, the RemovableSystemExtensions property must only be used when the administrator wants to automate the uninstallation of the connector.
NOTE: macOS Extensions cannot be retroactively removed via MDM. If the MDM profile is not deployed prior to uninstall of the connector then the macOS Extensions removal approval is not granted and the user is required to manually enter a password on the endpoint during the connector uninstallation process to remove the macOS Extensions.

Secure Endpoint extensions can be removed as part of the connector uninstallation by when a management profile with the RemovableSystemExtensions property added to the SystemExtensions payload is installed. The RemovableSystemExtensions property must contain the bundle identifiers of both Secure Endpoint extensions:

Payload	Property	Value
SystemExtensions	RemovableSystemExtensions	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Full Disk Access

MacOS 10.14 and later require approval before an application can access parts of the filesystem that contain personal user data (for example, Contacts, Photos, Calendar, and other applications). Certain connector functions such as on-access file scan are unable to scan these files for threats without approval.

Previous Mac connector versions required the user to grant Full Disk Access to the `ampdaemon` program. Mac connector 1.14 requires Full Disk Access for:

- "AMP for Endpoints Service"
- "AMP Security Extension"

Mac connector 1.16.0 and newer requires additional Full Disk Access for:

- "Cisco Orbital" when enabled in policy, available with Advantage and Premier access

Mac connector 1.18 and newer requires Full Disk Access for:

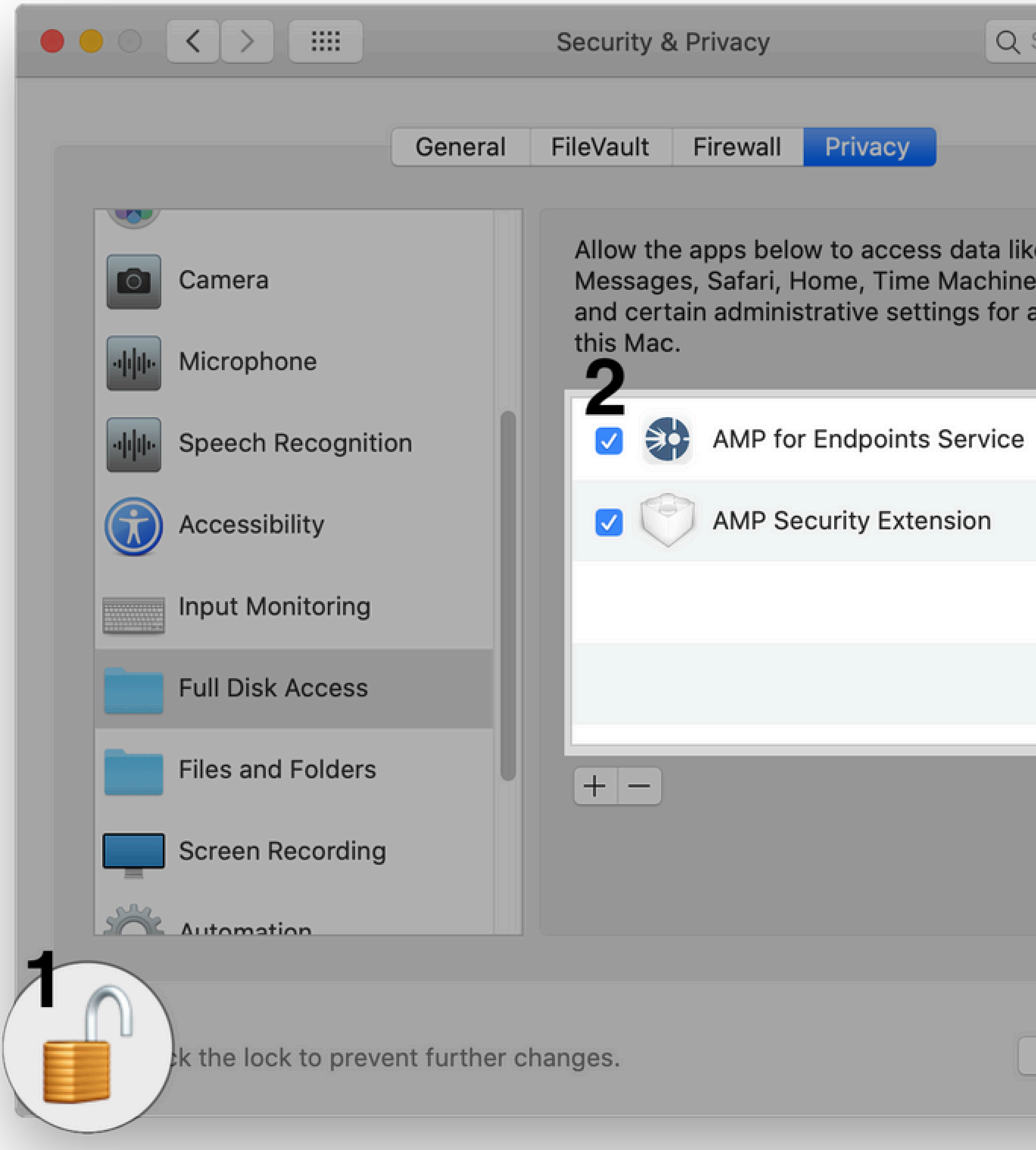
- "Secure Endpoint Service"
- "Secure Endpoint System Monitor"
- "Cisco Orbital" when Orbital is enabled in policy (available with Advantage and Premier tiers)

The `ampdaemon` program no longer requires Full Disk Access with Mac connector version 1.14 and newer.

Full Disk Access approvals can be granted in the macOS Security & Privacy Preferences on the endpoint, or through Mobile Device Management (MDM) profiles.

Approval of Full Disk Access for connector versions older than 1.18.0 at the Endpoint

Full Disk Access can be approved manually from the macOS Security & Privacy Preferences pane.



Allow the apps below to access data lik
Messages, Safari, Home, Time Machine
and certain administrative settings for a
this Mac.

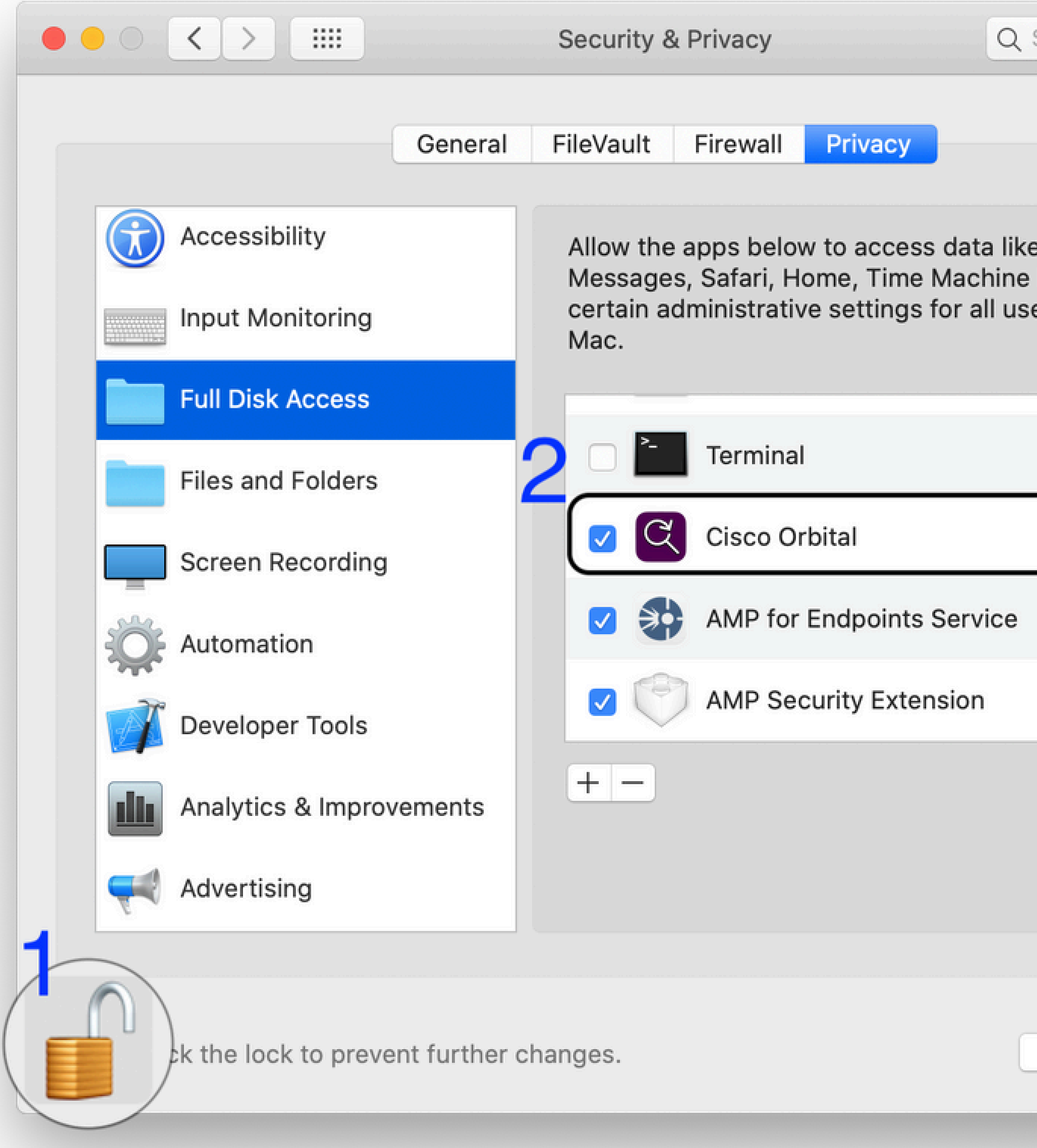
☑ AMP for Endpoints Service

☑ AMP Security Extension

k the lock to prevent further changes.

Approval of Full Disk Access for Cisco Orbital at the Endpoint

Full Disk Access can be approved manually from the macOS Security & Privacy Preferences pane.



Allow the apps below to access data like
Messages, Safari, Home, Time Machine
certain administrative settings for all use
Mac.

□ Terminal

☑ Cisco Orbital

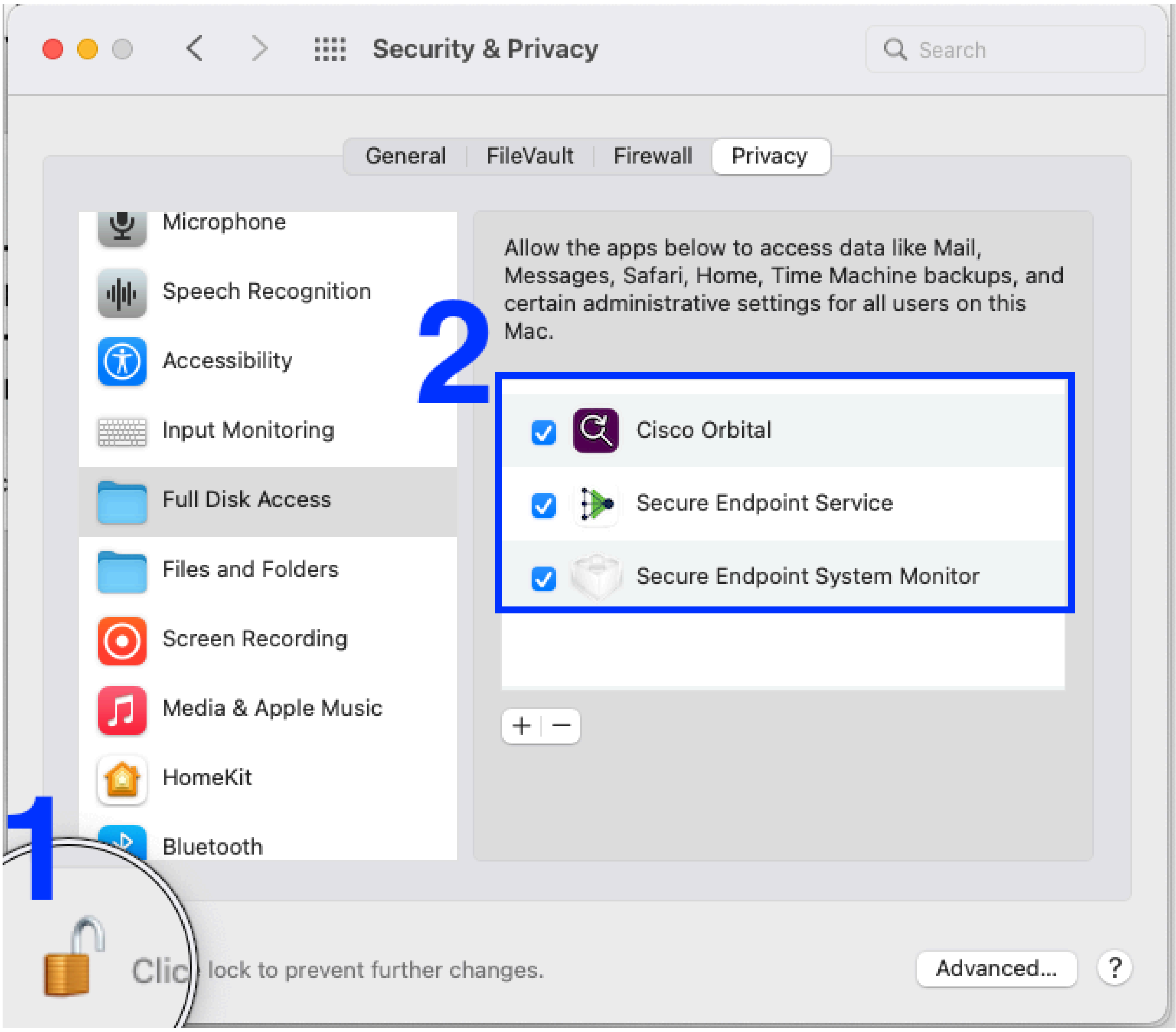
☑ AMP for Endpoints Service

☑ AMP Security Extension

ck the lock to prevent further changes.

Approval of Full Disk Access for Cisco Secure Endpoint connector 1.18.0 and Newer at the Endpoint

Full Disk Access can be approved manually from the macOS Security & Privacy Preferences pane.



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.

☑ Cisco Orbital

☑ Secure Endpoint Service

☑ Secure Endpoint System Monitor

Click lock to prevent further changes.

Approval of Full Disk Access for the Connector with MDM

NOTE: macOS Extensions cannot be retroactively approved via MDM. If the MDM profile is not deployed prior to install of the connector then the approvals are not granted and additional intervention is required in one of two forms:

1. Manual approval of the macOS Extensions on endpoints that had the management profile deployed retroactively.
2. Upgrade the Mac connector to a newer version than the one currently deployed. Endpoints that had the management profile deployed retroactively recognize the management profile after upgrade and gain approval once the upgrade completes.

Full Disk Access can be approved by a management profile Privacy Preferences Policy Control payload with a SystemPolicyAllFiles property with two entries, one for the `Secure Endpoint Service (AMP for Endpoints Service for connector versions older than 1.18.0)` and one for the `Secure Endpoint System Monitor (AMP Security Extension for connector versions older than 1.18.0)`:

Description	Property	Value
Secure Endpoint	Allowed	true
	CodeRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc" and

Description	Property	Value
Service (AMP for Endpoints Service)		(certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.svc
	IdentifierType	bundleID
Secure Endpoint System Monitor (AMP Security Extension)	Allowed	true
	CodeRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc.securityextension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.svc.securityextension
	IdentifierType	bundleID

If your deployment includes computers with connector version 1.12.7 or older installed, this additional entry is still required to grant full disk access to `ampdaemon` for those computers:

Description	Property	Value
ampdaemon	Allowed	true
	CodeRequirement	identifier ampdaemon and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TDNYQP7VRK
	Identifier	/opt/cisco/amp/ampdaemon
	IdentifierType	path

Approval of Full Disk Access for Cisco Orbital with MDM

If your deployment includes computers with Cisco Secure Endpoint Mac connector versions 1.16.0 or newer, on computers with macOS 10.15 or newer, and Orbital is enabled in policy, this additional entry is still required to grant full disk access to Orbital for those computers:

Description	Property	Value
Cisco Orbital	Allowed	true
	CodeRequirement	anchor apple generic and identifier "com.cisco.endpoint.orbital.app" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.orbital.app
	IdentifierType	bundleID

Sample MDM Configuration Profile

This sample MDM configuration profile can be used as a reference.

- Approval of system extensions for Secure Endpoint Mac connector.
- Grants full disk access for the Secure Endpoint Mac connector and Orbital.
- Allows silent uninstall of System Extensions when connector is uninstalled.
  NOTE: When RemovableSystemExtensions permission is allowed, any user or process with root privileges has the ability to remove the System Extension without a prompt for the user password. Thus, the RemovableSystemExtensions property must only be used when the administrator wants to automate the uninstallation of the connector.

```
<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN"
"http://www.apple.com/DTDs/PropertyList-1.0.dtd"> <plist version="1.0"> <dict> <key>PayloadContent</key> <array> <dict>
<key>AllowUserOverrides</key> <true/> <key>AllowedSystemExtensions</key> <dict> <key>DE8Y96K9QP</key> <array>
<string>com.cisco.endpoint.svc.securityextension</string> <string>com.cisco.endpoint.svc.networkextension</string> </array> </dict>
<key>PayloadDescription</key> <string></string> <key>PayloadDisplayName</key> <string>System Extensions</string>
<key>PayloadEnabled</key> <true/> <key>PayloadIdentifier</key> <string>92624553-06C3-4BE0-9000-91D8A260CC65</string>
<key>PayloadOrganization</key> <string>Cisco Systems, Inc.</string> <key>PayloadType</key> <string>com.apple.system-extension-
policy</string> <key>PayloadUUID</key> <string>92624553-06C3-4BE0-9000-91D8A260CC65</string> <key>PayloadVersion</key>
<integer>1</integer> <key>RemovableSystemExtensions</key> <dict> <key>DE8Y96K9QP</key> <array>
<string>com.cisco.endpoint.svc.securityextension</string> <string>com.cisco.endpoint.svc.networkextension</string> </array> </dict> </dict>
<dict> <key>PayloadDescription</key> <string></string> <key>PayloadDisplayName</key> <string>Privacy Preferences Policy
Control</string> <key>PayloadEnabled</key> <true/> <key>PayloadIdentifier</key> <string>290AAF9E-D9F1-4470-B802-
2468AC836142</string> <key>PayloadOrganization</key> <string>Cisco Systems, Inc.</string> <key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string> <key>PayloadUUID</key> <string>290AAF9E-D9F1-4470-B802-
2468AC836142</string> <key>PayloadVersion</key> <integer>1</integer> <key>Services</key> <dict> <key>SystemPolicyAllFiles</key>
<array> <dict> <key>Allowed</key> <integer>1</integer> <key>CodeRequirement</key> <string>anchor apple generic and identifier
"com.cisco.endpoint.svc" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /*
exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)</string>
<key>Identifier</key> <string>com.cisco.endpoint.svc</string> <key>IdentifierType</key> <string>bundleID</string>
<key>StaticCode</key> <integer>0</integer> </dict> <dict> <key>Allowed</key> <integer>1</integer> <key>CodeRequirement</key>
<string>identifier ampdaemon and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TDNYQP7VRK</string> <key>Identifier</key>
<string>/opt/cisco/amp/ampdaemon</string> <key>IdentifierType</key> <string>path</string> <key>StaticCode</key> <integer>0</integer>
</dict> <dict> <key>Allowed</key> <integer>1</integer> <key>CodeRequirement</key> <string>anchor apple generic and identifier
"com.cisco.endpoint.orbital.app" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6]
/* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)</string>
<key>Identifier</key> <string>com.cisco.endpoint.orbital.app</string> <key>IdentifierType</key> <string>bundleID</string>
<key>StaticCode</key> <integer>0</integer> </dict> </array> </dict> </dict> <dict> <key>FilterDataProviderBundleIdentifier</key>
<string>com.cisco.endpoint.svc.networkextension</string> <key>FilterDataProviderDesignatedRequirement</key> <string>anchor apple
generic and identifier "com.cisco.endpoint.svc.networkextension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate
1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
DE8Y96K9QP)</string> <key>FilterGrade</key> <string>firewall</string> <key>FilterPackets</key> <false/> <key>FilterSockets</key>
<true/> <key>FilterType</key> <string>Plugin</string> <key>PayloadDisplayName</key> <string>Web Content Filter Payload</string>
<key>PayloadIdentifier</key> <string>F630E2F3-F917-47F5-93E9-343C4C787C28</string> <key>PayloadOrganization</key> <string>Cisco
Systems, Inc.</string> <key>PayloadType</key> <string>com.apple.webcontent-filter</string> <key>PayloadUUID</key>
<string>F630E2F3-F917-47F5-93E9-343C4C787C28</string> <key>PayloadVersion</key> <integer>1</integer>
<key>PluginBundleID</key> <string>com.cisco.endpoint.svc</string> <key>UserDefinedName</key> <string>AMP Network
Extension</string> <key>VendorConfig</key> <dict/> </dict> </array> <key>PayloadDescription</key> <string></string>
<key>PayloadDisplayName</key> <string>Cisco Secure Endpoint Settings [DEMO]</string> <key>PayloadEnabled</key> <true/>
<key>PayloadIdentifier</key> <string>36DAAE4E-5BA2-497B-8381-D58FCB62FA1B</string> <key>PayloadOrganization</key>
<string>Cisco Systems, Inc.</string> <key>PayloadRemovalDisallowed</key> <true/> <key>PayloadScope</key> <string>System</string>
```

```
<key>PayloadType</key> <string>Configuration</string> <key>PayloadUUID</key> <string>36DAAE4E-5BA2-497B-8381-
D58FCB62FA1B</string> <key>PayloadVersion</key> <integer>1</integer> </dict> </plist>
```

Sample MDM configuration for macOS 10.15 or older

- Approval of kernel extensions and grants full disk access for connectors.
    - NOTE: M1 and newer Apple products cannot use profiles that contain this configuration

```
<dict> <key>AllowNonAdminUserApprovals</key> <false/> <key>AllowUserOverrides</key> <true/>
<key>AllowedKernelExtensions</key> <dict> <key>TDNYQP7VRK</key> <array> <string>com.cisco.amp.nke</string>
<string>com.cisco.amp.fileop</string> </array> </dict> <key>PayloadDescription</key> <string></string> <key>PayloadDisplayName</key>
<string>Approved Kernel Extensions</string> <key>PayloadEnabled</key> <true/> <key>PayloadIdentifier</key> <string>A872B6D5-D67C-
41FE-BE64-3DD674C43C4F</string> <key>PayloadOrganization</key> <string>Cisco Systems, Inc.</string> <key>PayloadType</key>
<string>com.apple.syspolicy.kernel-extension-policy</string> <key>PayloadUUID</key> <string>A872B6D5-D67C-41FE-BE64-
3DD674C43C4F</string> <key>PayloadVersion</key> <integer>1</integer> </dict>
```

New Directory Structure

Versions 1.14.0 to 1.16.2

Mac connector 1.14 introduces two changes to the directory structure:

1. The Applications directory has been renamed from `Cisco AMP` to `Cisco AMP for Endpoints`.
2. The command-line utility `ampcli` has been moved from `/opt/cisco/amp` to `/Applications/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS`. The directory `/opt/cisco/amp` contains a symlink to the `ampcli` program at its new location.

The complete directory structure for the Mac connector versions 1.14.0 to 1.16.2 is as follows:

```
â”œâ”€â”€ Applications
â”‚   â””â”€â”€ Cisco AMP for Endpoints
â”‚       â””â”€â”€ AMP for Endpoints Connector.app
â”‚       â”‚   â””â”€â”€ Contents
â”‚       â”‚       â””â”€â”€MacOS
â”‚       â”‚
â”‚       â””â”€â”€ AMP for Endpoints Service.app
â”‚       â”‚   â””â”€â”€ Contents
â”‚       â”‚       â””â”€â”€MacOS
â”‚       â”‚           â””â”€â”€ ampcli
â”‚       â”‚           â””â”€â”€ ampdaemon
â”‚       â”‚           â””â”€â”€ amscansvc
â”‚       â”‚           â””â”€â”€ ampcreport
â”‚       â”‚           â””â”€â”€ ampupdater
â”‚       â”‚           â””â”€â”€ SupportTool
â”‚       â”‚
â”‚       â””â”€â”€ Support Tool.app
â”œâ”€â”€ Library
â”‚   â”œâ”€â”€ Application Support
â”‚   â”‚   â””â”€â”€ Cisco
â”‚   â”‚       â””â”€â”€ AMP for Endpoints Connector
â”‚   â”‚           â””â”€â”€ SupportTool
â”‚   â””â”€â”€ Logs
â”‚       â””â”€â”€ Cisco
â”œâ”€â”€ Users
â”‚   â””â”€â”€ *
```

```
â”‚         â””â”€â”€ Library
â”‚             â””â”€â”€ Logs
â”‚                 â””â”€â”€ Cisco
â””â”€â”€ opt
    â””â”€â”€ cisco
        â””â”€â”€ amp
            â””â”€â”€ ampcli
```

Versions 1.18.0 and Newer

Mac connector 1.18 introduces a change to the applications directory structure:

1. The Applications directory has been renamed from `Cisco AMP for Endpoints` to `Cisco Secure Endpoint`.

The complete directory structure for Mac connector versions 1.18.0 and newer is as follows:

```
â”œâ”€â”€ Applications
|   â””â”€â”€ Cisco Secure Endpoint
|       â””â”€â”€Secure Endpoint Connector.app
|       |    â””â”€â”€ Contents
|       |        â””â”€â”€ MacOS
|       |
|       â””â”€â”€ Secure Endpoint Service.app
|       |   â””â”€â”€ Contents
|       |       â””â”€â”€ MacOS
|       |           â””â”€â”€ ampcli
|       |           â””â”€â”€ ampdaemon
|       |           â””â”€â”€ ampscansvc
|       |           â””â”€â”€ ampcreport
|       |           â””â”€â”€ ampupdater
|       |           â””â”€â”€ SupportTool
|       |
|       â””â”€â”€ Support Tool.app
```

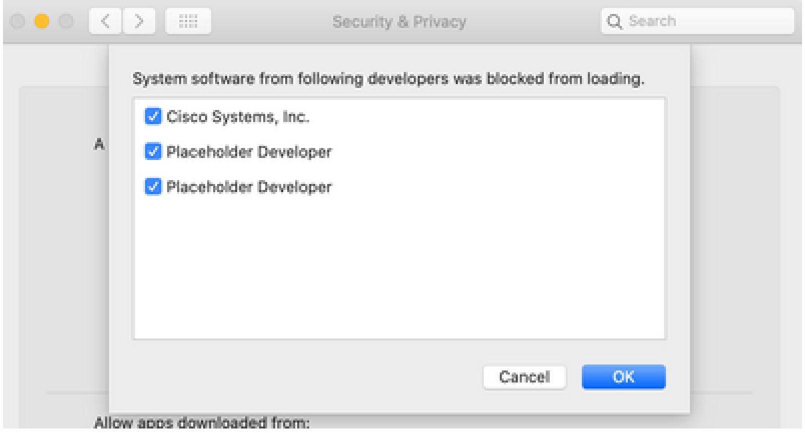
Known Issues with macOS 11.0 and Mac Connector 1.14.1.

- Guidance for fault 10, "Reboot required to load kernel module or system extension," can be incorrect if four or more Network Content Filters are installed on the computer. Refer to the Cisco Secure Endpoint Mac Connector Faults article for more details.

Known Issues with macOS 10.15/11.0 and Mac Connector 1.14.0.

- Some faults raised by the Mac connector can be raised unexpectedly. Refer to the Cisco Secure Endpoint Mac Connector Faults article for more details.
  - Fault 13, Too many Network Content Filter system extensions, can be raised after an upgrade. A reboot of the computer resolves the fault in this situation.
  - Fault 15, System Extension requires Full Disk Access, can be raised after reboot due to a bug in macOS 11.0.0. This issue is fixed in macOS 11.0.1. The fault can be resolved by a re-grant of full disk access in the Security & Privacy pane in macOS System Preferences.

- During installation, the Security & Privacy pane can display "Placeholder Developer" as the application name when macOS asks for permission for the Mac connector system extensions to run. This is due to a bug in macOS 10.15. Check the boxes beside "Placeholder Developer" to allow the Mac connector to protect the computer.

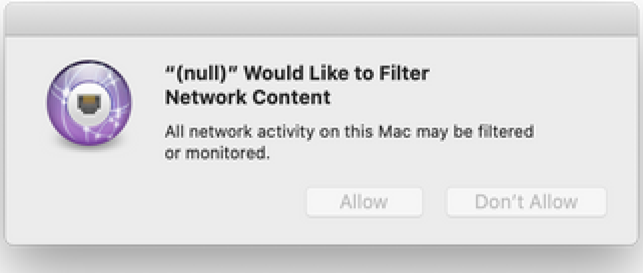


System software from following developers was blocked from loading.

☑ Cisco Systems, Inc.
☑ Placeholder Developer
☑ Placeholder Developer

  - The `systemextensionsctl list`command can be used to determine which system extensions are need approval. System extensions with the state `[activated waiting for user]`in this output are displayed as "Placeholder Developer" in the macOS preferences page shown previously. If more than two "Placeholder Developer" entries are shown in the preferences page, uninstall all software that uses system extensions (include the Mac connector) so that no system extensions need approval, and then reinstall the Mac connector.
    The Mac connector sysem extensions are identified as follows:
    - The Network Extension is shown as `com.cisco.endpoint.svc.networkextension`.
    - The Endpoint Security extension is shown has `com.cisco.endpoint.svc.securityextension`.

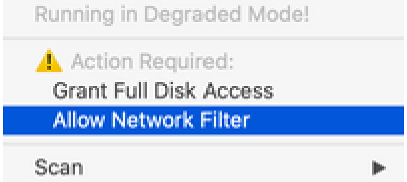
- During install, the prompt to allow the Content Filter to monitor network traffic can display "(null)" as the application name. This is caused by a bug in macOS 10.15. The user needs to select "Allow" to to ensure protection of the computer.



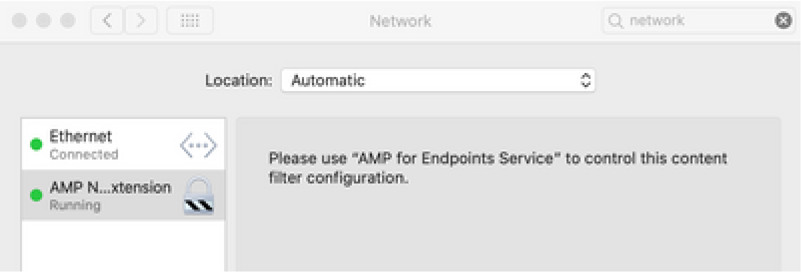
"(null)" Would Like to Filter Network Content

All network activity on this Mac may be filtered or monitored.

- If the prompt was dismissed because "Don't Allow" was chosen then select the "Allow Network Filter" from the drop-down menu in the Agent icon in the menu bar to open the prompt again.



- Once enabled, the Secure Endpoint Network Extension filter is listed on the Network Preferences page.



Please use "AMP for Endpoints Service" to control this content filter configuration.

- On macOS 11, when an upgrade from Mac connector 1.12 to Mac connector 1.14 is performed, Fault 4, System Extension Failed to Load, can be raised temporarily while the connector transitions from the kernel extensions to the new system extensions.

Known Issues During Uninstall of System Extensions

- Prior to macOS 12, or when MDM is not used, when an uninstall of the Mac connector is performed the user is prompted to enter their password twice so that the system extensions can be uninstalled. This is a limitation of macOS and has been improved somewhat in macOS 12 with the addition of the RemovableSystemExtensions MDM profile key described in this document.

Intune Deployment Installation Script

- A script that will help install Secure Endpoint connector on macOS maintained by Microsoft is hosted here:

https://github.com/microsoft/shell-intune-samples/tree/master/macOS/Apps/Cisco%20AMP

Rebranded Mac Connector (Versions 1.18.0 and newer)

NOTE: Existing MDM configurations for connector versions older than 1.18.0 work without intervention for upgrades to connector versions 1.18.0 and newer. See Secure Endpoint Mac Rebrand for more information.

Revision History

Dec 1, 2020

- Mac connector 1.14.1 no longer uses system extensions on macOS 10.15.
- Additional guidance on terminal check which "Placeholder Developer" System Extensions need approval with Mac connector 1.14.0.

Nov 9, 2020

- Corrected bundle ID in full disk access CodeRequirement MDM payload.

Nov 3, 2020

- The release date for 1.14.0 Mac connector is November 2020.
- The 1.14.0 Mac connector uses System Extensions with macOS 10.15.5 and later. Previously this was 10.15.6.
- Added Known Issues section.
- Updated directory structure outline.

June 3, 2021

- Added directions to grant full disk access for Cisco Orbital.

Oct 13, 2021

- Added Removal of Mac Connector macOS Extensions with MDM section.
- Added Known Issues for the Uninstall of System Extensions section.

Feb 25, 2022

- Rebrand