Konfigurieren von Berechtigungen für Secure Endpoint Mac Connector und Orbital mit MDM: vollständiger Festplattenzugriff, Systemerweiterungen

Inhalt

Einleitung
MDM-Profile
Ratschläge
Betriebssystem-Mindestanforderungen
Wichtige Änderungen
Genehmigung der Mac Connector macOS Erweiterungen
Genehmigung der Mac Connector macOS-Erweiterungen am Endpunkt
Genehmigung der Mac Connector macOS Erweiterungen mit MDM
Entfernen der Mac Connector macOS Erweiterungen mit MDM
Vollständiger Festplattenzugriff
Genehmigung von Full Disk Access für Steckverbinderversionen, die älter als 1.18.0 am Endgerät sind
Genehmigung von vollständigem Festplattenzugriff für Cisco Orbital am Endpunkt
Genehmigung des vollständigen Festplattenzugriffs für Cisco Secure Endpoint Connector 1.18.0 und höher am Endgerät
Genehmigung des vollständigen Festplattenzugriffs für den Connector mit MDM
Genehmigung von vollständigem Festplattenzugriff für Cisco Orbital mit MDM
Beispiel für ein MDM-Konfigurationsprofil
MDM-Beispielkonfiguration für macOS 10.15 oder älter
Neue Verzeichnisstruktur
Versionen 1.14.0 bis 1.16.2
Versionen 1.18.0 und neuere Versionen
Bekannte Probleme mit macOS 11.0 und Mac Connector 1.14.1.
Bekannte Probleme mit macOS 10.15/11.0 und Mac Connector 1.14.0.
Bekannte Probleme bei der Deinstallation von Systemerweiterungen
Intune-BereitstellungInstallationsskript
Mac Connector mit Rebranding (Versionen 1.18.0 und höher)
Revisionsverlauf

Einleitung

In diesem Dokument werden die jüngsten Änderungen und Schritte für Administratoren zur Bereitstellung von Mac Connector 1.14 und höher beschrieben.

MDM-Profile

Es wird dringend empfohlen, den Mac-Connector mit einem MDM-Profil bereitzustellen, das die erforderlichen Genehmigungen erteilt. MDM-Profile müssen vor der Installation, dem Upgrade oder dem Entfernen des Mac-Connectors installiert werden, um sicherzustellen, dass die erforderlichen Berechtigungen erkannt werden. Wenn MDM nicht verwendet werden kann, lesen Sie den Abschnitt Bekannte Probleme weiter unten in diesem Dokument.

Ratschläge

In Mac Connector Version 1.14 wurden Änderungen eingeführt, die Beachtung erfordern:

- Genehmigung des vollständigen Festplattenzugriffs
- Genehmigung der Systemerweiterung

Der Mac-Anschluss 1.14 oder höher ist erforderlich, um den Schutz von Endpunkten unter Mac OS 11 und höher sicherzustellen. Ältere Mac-Anschlüsse funktionieren nicht auf diesen Versionen von macOS.

Mac Connector Version 1.16 bietet nun Unterstützung für Cisco Orbital auf Intel Hardware. Orbital kann gemäß den Richtlinien von Advantage oder Premier Tier aktiviert werden und wird automatisch installiert, wenn es aktiviert und auf einer unterstützten Betriebssystemversion und Hardware installiert wird. Der Mac-Connector Version 1.20 bietet jetzt Unterstützung für Cisco Orbital auf Apple-Chipsätzen. Die Veröffentlichung mit Orbital Node 1.21 ist geplant. In den Abschnitten zu Cisco Orbital dieses Dokuments finden Sie weitere Informationen zum Gewähren der zusätzlichen vollständigen Zugriffsberechtigungen für Festplatten für Orbital.

Betriebssystem-Mindestanforderungen

Cisco Secure Endpoint Mac Connector 1.14.0 unterstützt MacOS-Versionen:

- macOS 11, mit macOS Systemerweiterungen.
- macOS 10.15.5 und höher, mit macOS-Systemerweiterungen.
- macOS 10.15.0 bis macOS 10.15.4, mit macOS Kernel-Erweiterungen.
- macOS 10.14, mit macOS Kernel-Erweiterungen.

Cisco Secure Endpoint Mac Connector 1.14.1 unterstützt MacOS-Versionen:

- macOS 11, mit macOS Systemerweiterungen.
- macOS 10.15 mit macOS Kernel-Erweiterungen.
- macOS 10.14, mit macOS Kernel-Erweiterungen.

Unterstützung für Cisco Orbital auf Intel Hardware wurde in Secure Endpoint Mac Connector Version 1.16.0 eingeführt. Secure Endpoint Mac Connector Version 1.20.0 bietet jetzt Unterstützung für Cisco Orbital auf Apple-Chipsätzen.

Die Kompatibilität des aktuellen Mac-Connectors finden Sie in der Kompatibilitätstabelle des Betriebssystems.

Wichtige Änderungen

Der Mac-Connector 1.14 führte wichtige Änderungen in drei Bereichen ein:

1. Genehmigung der vom Connector verwendeten macOS-Erweiterungen
2. Vollständiger Festplattenzugriff
3. Neue Verzeichnisstruktur

MacOS 12 führte eine MDM-Option ein, um das Entfernen der macOS-Erweiterungen des Connectors ohne Aufforderung zur Eingabe von Benutzerkennwörtern zu ermöglichen.

Genehmigung der Mac Connector macOS Erweiterungen

Der Mac-Connector verwendet entweder Systemerweiterungen oder ältere Kernel-Erweiterungen, um die Systemaktivitäten zu überwachen, je nach Bedarf für die macOS-Version. Unter macOS 11 ersetzen Systemerweiterungen die älteren Kernel-Erweiterungen, die in macOS 11 und höher nicht unterstützt werden. Die Genehmigung durch den Benutzer ist für alle Versionen von macOS erforderlich, bevor die Ausführung eines der beiden Erweiterungstypen zugelassen wird. Ohne Genehmigung sind bestimmte Connector-Funktionen wie Dateisuche bei Zugriff und Netzwerkzugriffsüberwachung nicht verfügbar.

Mac Connector 1.14 führt zwei neue macOS Systemerweiterungen ein:

1. Eine Endpoint Security-Erweiterung mit dem Namen Secure Endpoint File Monitor (ehemals AMP Security Extension) zur Überwachung von Systemereignissen
2. Eine Network Content Filter-Erweiterung mit dem Namen Cisco Secure Endpoint Filter (ehemals AMP Network Extension) zur Überwachung des Netzwerkzugriffs

Die beiden älteren Kernel-Erweiterungen `ampfileop.kext` und `ampnetworkflow.kext` sind für Abwärtskompatibilität bei älteren macOS-Versionen enthalten, die die neuen macOS-Systemerweiterungen nicht unterstützen.

Erforderliche Genehmigungen für macOS 11** und höher:

- Laden von Secure Endpoint File Monitor genehmigen
- Laden von Cisco Secure Endpoint-Filter genehmigen
- Filtern von Netzwerkinhalten nach Cisco Secure Endpoint Filter zulassen

** Mac Connector Version 1.14.0 erforderte diese Genehmigungen auch unter macOS 10.15. Diese Genehmigungen sind für macOS 10.15 für Mac Connector 1.14.1 oder neuer nicht mehr erforderlich.

Die für macOS 10.14 und macOS 10.15 erforderlichen Genehmigungen:

- Konnektor-Kernel-Erweiterungen zum Laden genehmigen

Diese Genehmigungen können in den macOS-Einstellungen für Sicherheit und Datenschutz am Endgerät oder über Mobile Device Management (MDM)-Profile erteilt werden.

Genehmigung der Mac Connector macOS-Erweiterungen am Endpunkt

System- und Kernel-Erweiterungen können manuell im Bereich macOS-Sicherheits- und Datenschutzeinstellungen genehmigt werden.

Genehmigung der Mac Connector macOS Erweiterungen mit MDM

HINWEIS: macOS-Erweiterungen können nicht rückwirkend über MDM genehmigt werden. Wenn das MDM-Profil vor der Installation des Connectors nicht bereitgestellt wird, werden die Genehmigungen nicht erteilt, und es ist ein zusätzlicher Eingriff in einer von zwei Formen erforderlich:

1. Manuelle Genehmigung der macOS-Erweiterungen auf Endpunkten, auf denen das Managementprofil rückwirkend bereitgestellt wurde.

2. Aktualisieren Sie den Mac-Connector auf eine neuere Version als die derzeit bereitgestellte. Endgeräte mit rückwirkend bereitgestelltem Verwaltungsprofil erkennen das Verwaltungsprofil nach einem Upgrade und erhalten nach Abschluss des Upgrades eine Genehmigung.

Secure Endpoint-Erweiterungen können mit einem Verwaltungsprofil mit den folgenden Payloads und Eigenschaften genehmigt werden:

Nutzlast	Eigenschaft	Wert
Systemerweiterungen	ZulässigeSystemerweiterungen	com.cisco.endpoint.svc.securityexte com.cisco.endpoint.svc.networkexte
	ZulässigeSystemerweiterungstypen	EndpointSecurityExtension, NetworkExtension
	ZulässigeTeamIdentifier	DE8Y96K9QP
SystemPolicyKernelErweiterungen	ZulässigeKernelErweiterungen	com.cisco.amp.fileop, com.cisco.an
	ZulässigeTeamIdentifier	TDNYQP7VRK
WebContentFilter	AutoFilter aktiviert	falsch
	FilterDatenanbieterPaketBezeichner	com.cisco.endpoint.svc.networkexte
	FilterDataProviderDesignatedAnforderung	Ankerapple generisch und Kennung "com.cisco.endpoint.svc.networkex und (Zertifikatblatt[field.1.2.840.11363 /* existiert */ oder Zertifikat 1[field.1.2.840.113635.100.6.2.6] /* */ und Zertifikatblatt[field.1 1.2.840.113635.100.6.1.13] /* exist Zertifikatsblatt[subject.OU] = DE8
	Filtergrad	Firewall
	FilterBrowser	falsch
	FilterPakete	falsch
	FilterSockets	wahr
	PluginBundleID	com.cisco.endpoint.svc
	Benutzerdefinierter Name	Cisco Secure Endpoint Filter (AMP Netzwerkerweiterung, wenn Conne Version älter als 1.18.0)

Entfernen der Mac Connector macOS Erweiterungen mit MDM

Mit MacOS 12 und höher können macOS-Erweiterungen mit der Eigenschaft RemovableSystemExtensions wie unten beschrieben als entfernbar markiert werden.
HINWEIS: Wenn macOS Extension Removable-Berechtigung erlaubt ist, hat jeder Benutzer oder Prozess mit Root-Berechtigungen die Möglichkeit, die Erweiterung ohne Aufforderung zur Eingabe des Benutzerkennworts zu entfernen. Daher muss die RemovableSystemExtensions-Eigenschaft nur verwendet werden, wenn der Administrator die Deinstallation des Connectors automatisieren möchte.
HINWEIS: macOS-Erweiterungen können nicht rückwirkend über MDM entfernt werden. Wenn das MDM-Profil vor der Deinstallation des Connectors nicht bereitgestellt wird, wird die Genehmigung zum Entfernen von macOS-Erweiterungen nicht erteilt, und der Benutzer muss während der Deinstallation des Connectors manuell ein Kennwort für den Endpunkt eingeben, um die macOS-Erweiterungen zu entfernen.

Sichere Endpunkterweiterungen können im Rahmen der Connector-Deinstallation entfernt werden, wenn ein Verwaltungsprofil mit der RemovableSystemExtensions-Eigenschaft installiert wird, das der SystemExtensions-Nutzlast hinzugefügt wurde. Die RemovableSystemExtensions-Eigenschaft muss die Bündelbezeichner beider sicherer Endpunkterweiterungen enthalten:

Nutzlast	Eigenschaft	Wert
Systemerweiterungen	ErweiterungenWechselsystem	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Vollständiger Festplattenzugriff

MacOS 10.14 und höher erfordern eine Genehmigung, bevor eine Anwendung auf Teile des Dateisystems zugreifen kann, die persönliche Benutzerdaten enthalten (z. B. Kontakte, Fotos, Kalender und andere Anwendungen). Bestimmte Connector-Funktionen wie die Dateisuche bei Zugriff können diese Dateien nicht ohne Genehmigung auf Bedrohungen durchsuchen.

Frühere Mac-Connector-Versionen erforderten, dass der Benutzer dem `ampdaemon`-Programm vollständigen Festplattenzugriff gewährt. Mac-Anschluss 1.14 erfordert vollständigen Festplattenzugriff für:

- "AMP für Endgeräte Service"
- "AMP Security Extension"

Für den Mac-Anschluss 1.16.0 und höher ist zusätzlicher vollständiger Festplattenzugriff erforderlich für:

- "Cisco Orbital" bei Aktivierung in Richtlinie, verfügbar mit Advantage- und Premier-Zugriff

Der Mac-Anschluss 1.18 und höher erfordert vollständigen Festplattenzugriff für:

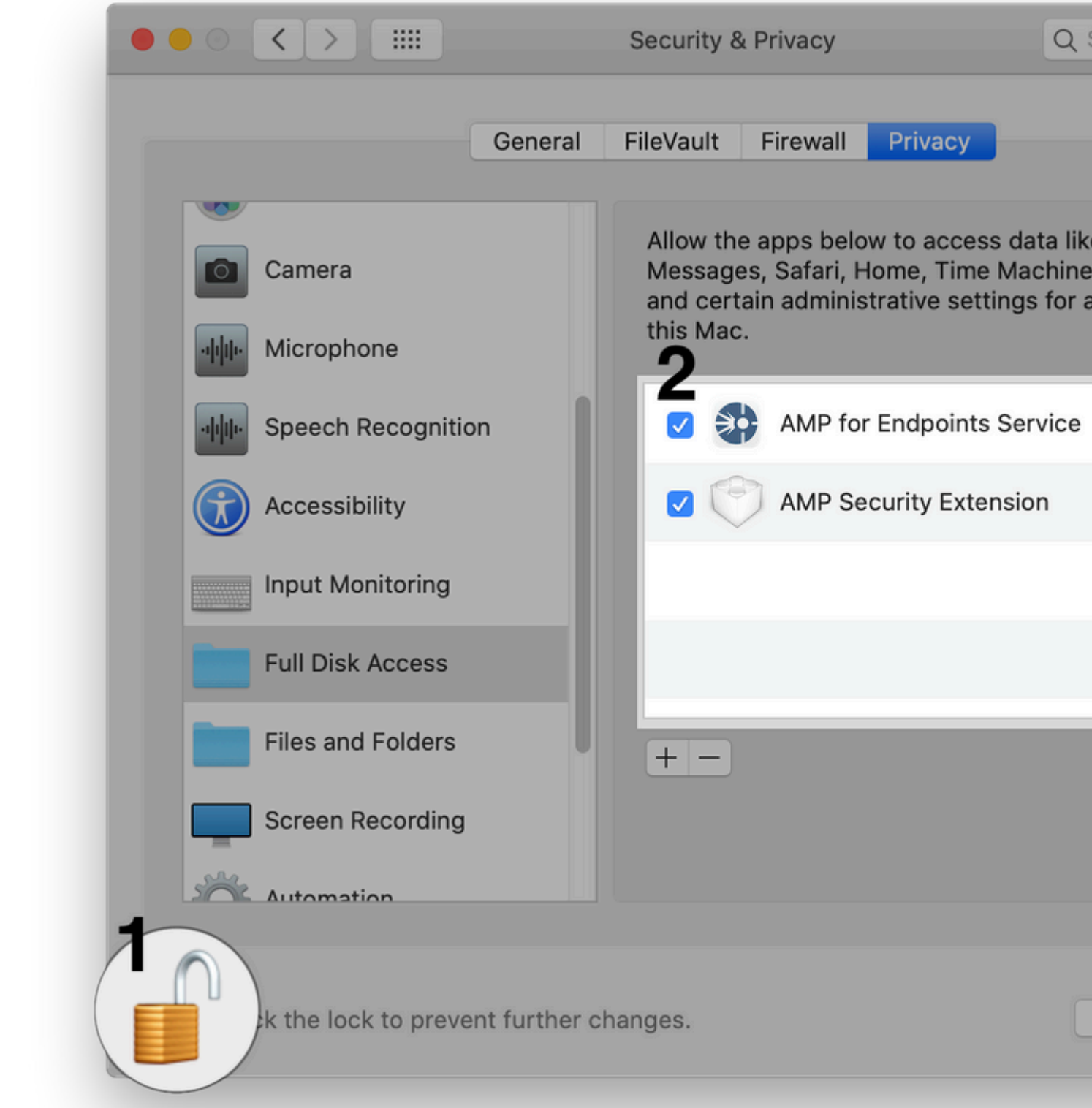
- "Secure Endpoint Service"
- "Secure Endpoint System Monitor"
- "Cisco Orbital", wenn Orbital in Richtlinie aktiviert ist (verfügbar mit Advantage- und Premier-Stufen)

Das Programm `ampdaemon` benötigt nicht mehr Full Disk Access mit Mac Connector Version 1.14 und neuer.

Genehmigungen für vollständigen Festplattenzugriff können in den macOS-Einstellungen für Sicherheit und Datenschutz am Endgerät oder über Mobile Device Management (MDM)-Profile erteilt werden.

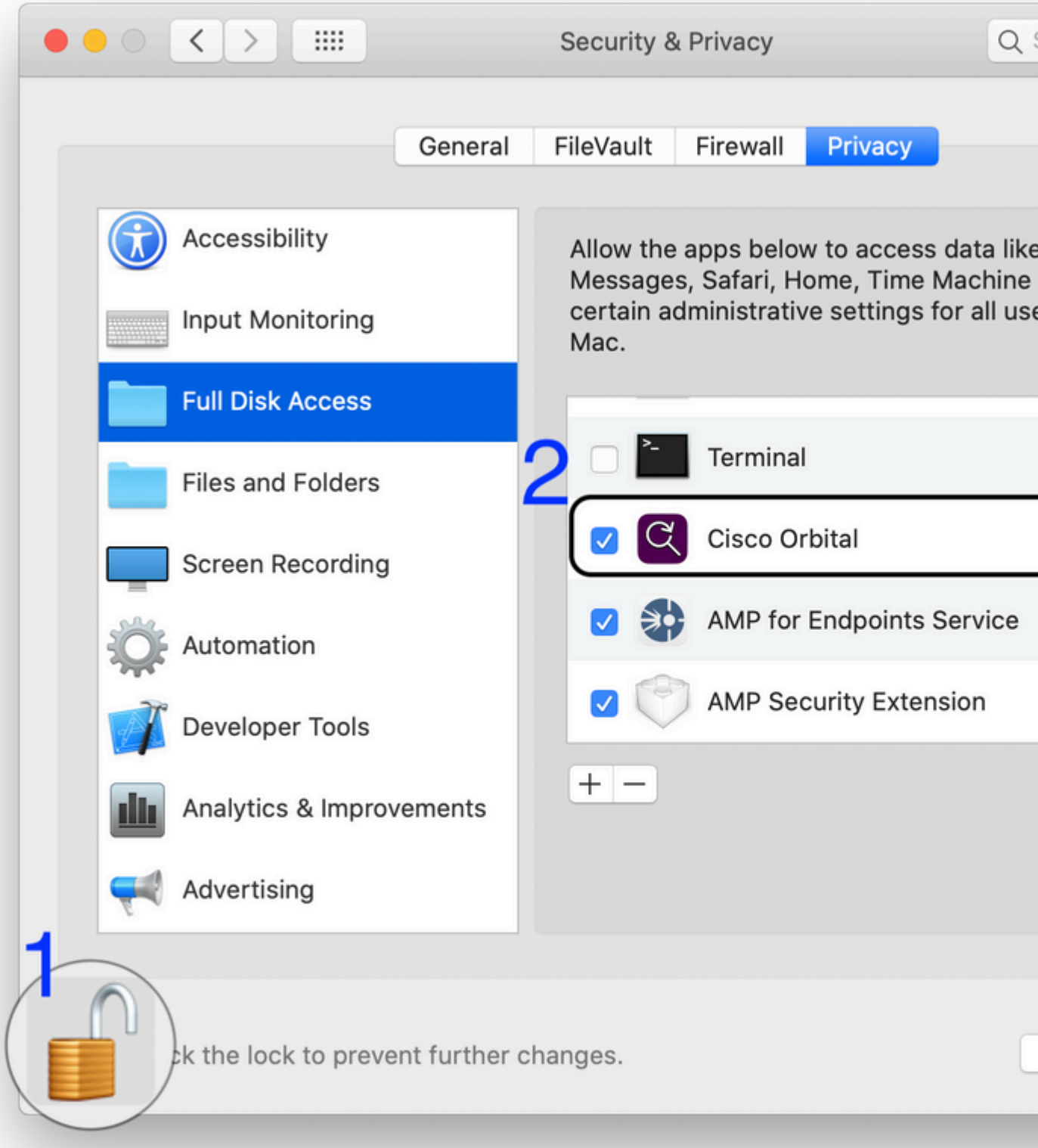
Genehmigung von Full Disk Access für Steckverbinderversionen, die älter als 1.18.0 am Endgerät sind

Vollständiger Festplattenzugriff kann manuell im Bereich "macOS-Sicherheit und -Datenschutzeinstellungen" genehmigt werden.



Genehmigung von vollständigem Festplattenzugriff für Cisco Orbital am Endpunkt

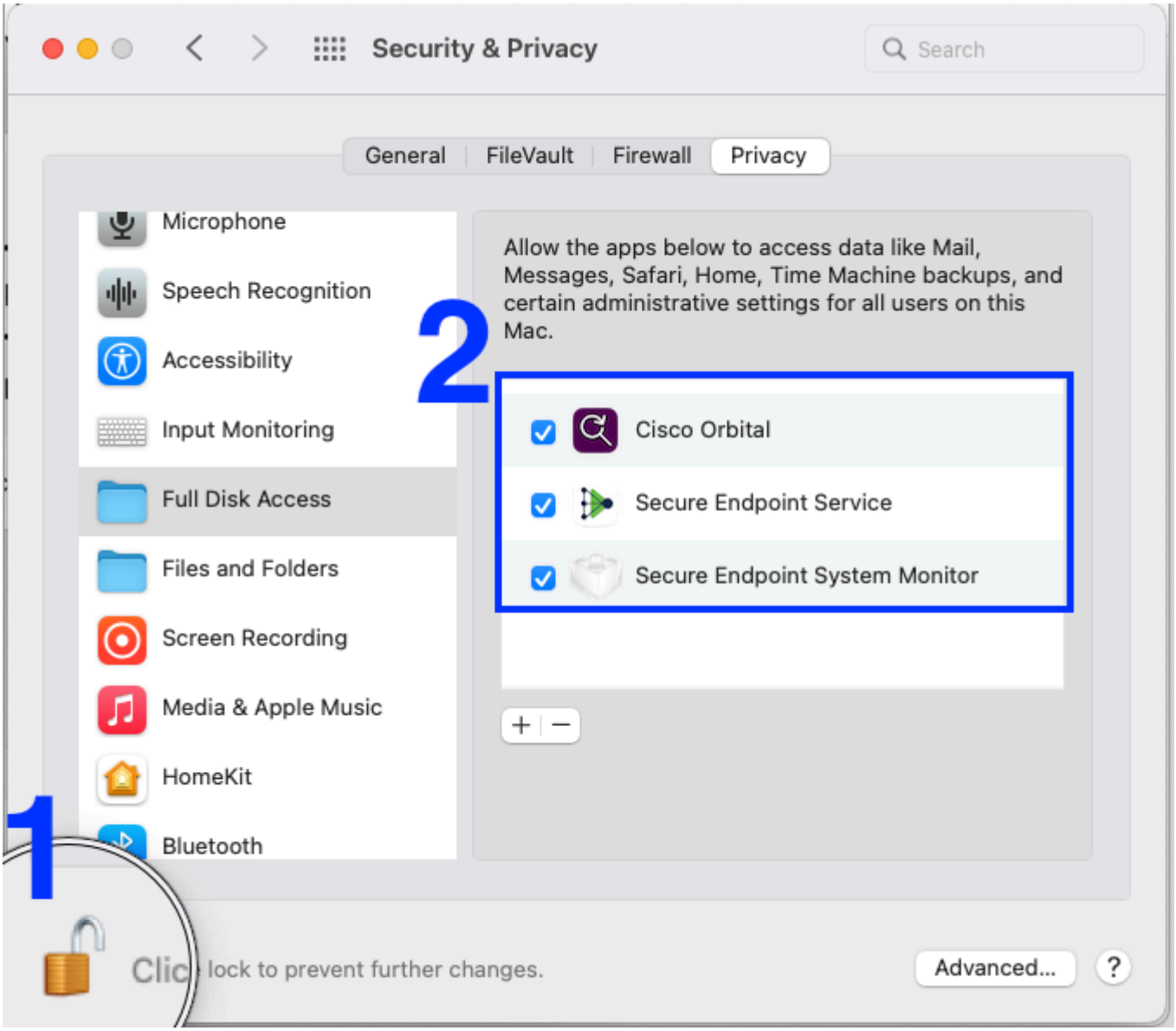
Vollständiger Festplattenzugriff kann manuell im Bereich "macOS-Sicherheit und -Datenschutzeinstellungen" genehmigt werden.



Genehmigung des vollständigen Festplattenzugriffs für Cisco Secure Endpoint Connector 1.18.0 und höher am Endgerät

Vollständiger Festplattenzugriff kann manuell im Bereich "macOS-Sicherheit und -

Datenschutzeinstellungen" genehmigt werden.



Genehmigung des vollständigen Festplattenzugriffs für den Connector mit MDM

HINWEIS: macOS-Erweiterungen können nicht rückwirkend über MDM genehmigt werden. Wenn das MDM-Profil vor der Installation des Connectors nicht bereitgestellt wird, werden die Genehmigungen nicht erteilt, und es ist ein zusätzlicher Eingriff in einer von zwei Formen erforderlich:

1. Manuelle Genehmigung der macOS-Erweiterungen auf Endpunkten, auf denen das Managementprofil rückwirkend bereitgestellt wurde.
2. Aktualisieren Sie den Mac-Connector auf eine neuere Version als die derzeit bereitgestellte. Endgeräte, auf denen das Verwaltungsprofil rückwirkend bereitgestellt wurde, erkennen das Verwaltungsprofil nach dem Upgrade und erhalten nach Abschluss des Upgrades eine Genehmigung.

Vollständiger Festplattenzugriff kann über ein Verwaltungsprofil genehmigt werden Datenschutzeinstellungen Nutzlast für die Richtlinienkontrolle mit einer SystemPolicyAllFiles-Eigenschaft mit zwei Einträgen, einer für den `Secure Endpoint Service (AMP für Endpoints-Dienst für Connector-Versionen vor 1.18.0)` und einer für den `Secure Endpoint System Monitor (AMP Security Extension für Connector-Versionen vor 1.18.0)`:

Beschreibung	Eigenschaft	Wert
Secure Endpoint Service (AMP für Endpoints-Service)	ZUGELASSEN	wahr
	CodeAnforderung	Ankerapple generisch und Kennung "com.cisco.endpoint.svc" und (Zertifikatblatt[Feld.1.2.840.113635.100.6.1.9] /* existiert */ oder Zertifikat 1[Feld.1.2.840.113635.100.6.2.6] /* existiert */ und Zertifikatblatt[Feld.1.2.2.840.113635.100.6.1.13] /* existiert */ und Zertifikatsblatt[subject.OU] = DE8Y96K9QP)
	Identifikator	com.cisco.endpoint.svc
	BezeichnerTyp	PaketID
Secure Endpoint System Monitor (AMP-Sicherheitserweiterung)	ZUGELASSEN	wahr
	CodeAnforderung	Ankerapple generisch und Kennung "com.cisco.endpoint.svc.securityextension" und (Zertifikatblatt[field.1.2.840.113635.100.6.1.9] /* existiert */ oder Zertifikat 1[field.1.2.840.113635.100.6.2.6] /* existiert */ und Zertifikatblatt[field 1.1.2.840.113635.100.6.1.13] /* existiert */ und Zertifikatsblatt [subject.OU] = DE8Y96K9QP)
	Identifikator	com.cisco.endpoint.svc.securityerweiterung
	BezeichnerTyp	PaketID

Wenn Ihre Bereitstellung Computer mit installiertem Connector (Version 1.12.7 oder älter) umfasst, ist dieser zusätzliche Eintrag weiterhin erforderlich, um `ampdaemon` für diese Computer den vollständigen Festplattenzugriff zu gewähren:

Beschreibung	Eigenschaft	Wert
Ampdaemon	ZUGELASSEN	wahr
	CodeAnforderung	bezeichner ampdaemon und anker apple generisch und zertifikat 1[field.1.2.840.113635.100.6.2.6] /* existiert */ und zertifikat leaf[field.1.2.840.113635.100.6.1.13] /* existiert */ und zertifikat leaf[subject.OU] = TDNYQP7VRRR K
	Identifikator	/opt/cisco/amp/ampdaemon
	BezeichnerTyp	Pfad

Genehmigung von vollständigem Festplattenzugriff für Cisco Orbital mit MDM

Wenn Ihre Bereitstellung Computer mit Cisco Secure Endpoint Mac Connector Version 1.16.0 oder neuer auf Computern mit macOS 10.15 oder neuer umfasst und Orbital in der Richtlinie aktiviert ist, ist dieser zusätzliche Eintrag weiterhin erforderlich, um Orbital vollständigen Festplattenzugriff für diese Computer zu gewähren:

Beschreibung	Eigenschaft	Wert
Cisco Orbital	ZUGELASSEN	wahr
	CodeAnforderung	Ankerapple generisch und Kennung "com.cisco.endpoint.orbital.app" und (Zertifikatblatt[field.1.2.840.113635.100.6.1.9] /* existiert */ oder Zertifikat 1[field.1.2.840.113635.100.6.2.6] /* existiert */ und Zertifikat leaf[field.1.1.2.840.113635.100.6.1.13] /* existiert */ und

Beschreibung	Eigenschaft	Wert
		Zertifikatsblatt[subject.OU] = DE8Y96K9QP)
	Identifikator	com.cisco.endpoint.orbital.app
	BezeichnerTyp	PaketID

Beispiel für ein MDM-Konfigurationsprofil

Dieses MDM-Beispielkonfigurationsprofil kann als Referenz verwendet werden.

- Genehmigung von Systemerweiterungen für Secure Endpoint Mac Connector.
- Gewährt vollständigen Festplattenzugriff für den Secure Endpoint Mac-Anschluss und Orbital
- Ermöglicht die automatische Deinstallation von Systemerweiterungen, wenn der Connector deinstalliert wird.
  HINWEIS: Wenn die RemovableSystemExtensions-Berechtigung zulässig ist, kann jeder Benutzer oder Prozess mit Root-Berechtigungen die Systemerweiterung ohne Aufforderung zur Eingabe des Benutzerkennworts entfernen. Daher muss die RemovableSystemExtensions-Eigenschaft nur verwendet werden, wenn der Administrator die Deinstallation des Connectors automatisieren möchte.

http://www.apple.com/DTDs/PropertyList-1.0.dtd">

PayloadContent

AllowUserOverrides

AllowedSystemExtensions

DE8Y96K9QP

com.cisco.endpoint.svc.securityextension

com.cisco.endpoint.svc.networkextension

PayloadDescription

PayloadDisplayName

System Extensions

PayloadEnabled

PayloadIdentifier

92624553-06C3-4BE0-9000-91D8A260CC65

PayloadOrganization

Cisco Systems, Inc.

PayloadType

com.apple.system-extension-policy

PayloadUUID

92624553-06C3-4BE0-9000-91D8A260CC65

PayloadVersion

1

RemovableSystemExtensions

DE8Y96K9QP

com.cisco.endpoint.svc.securityextension

com.cisco.endpoint.svc.networkextension

PayloadDescription

PayloadDisplayName

Privacy Preferences Policy Control

PayloadEnabled

PayloadIdentifier

290AAF9E-D9F1-4470-B802-2468AC836142

PayloadOrganization

Cisco Systems, Inc.

PayloadType

com.apple.TCC.configuration-profile-policy

PayloadUUID

290AAF9E-D9F1-4470-B802-2468AC836142

PayloadVersion

1

Services

SystemPolicyAllFiles

Allowed

1

CodeRequirement

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)

Identifier

com.cisco.endpoint.svc

IdentifierType

bundleID

StaticCode

0

Allowed

1

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

StaticCode

0

Allowed

1

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

StaticCode

0

FilterDataProviderBundleIdentifier

com.cisco.endpoint.svc.networkextension

FilterDataProviderDesignatedRequirement

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)

FilterGrade

firewall

FilterPackets

FilterSockets

FilterType

Plugin

PayloadDisplayName

Web Content Filter Payload

PayloadIdentifier

F630E2F3-F917-47F5-93E9-343C4C787C28

PayloadOrganization

Cisco Systems, Inc.

PayloadType

com.apple.webcontent-filter

PayloadUUID

F630E2F3-F917-47F5-93E9-343C4C787C28

PayloadVersion

1

PluginBundleID

com.cisco.endpoint.svc

UserDefinedName

AMP Network Extension

VendorConfig

PayloadDescription

PayloadDisplayName

Cisco Secure Endpoint Settings [DEMO]

PayloadEnabled

PayloadIdentifier

36DAAE4E-5BA2-497B-8381-D58FCB62FA1B

PayloadOrganization

Cisco Systems, Inc.

PayloadRemovalDisallowed

PayloadScope

System

PayloadType

Configuration

PayloadUUID

36DAAE4E-5BA2-497B-8381-D58FCB62FA1B

PayloadVersion

1

MDM-Beispielkonfiguration für macOS 10.15 oder älter

- Genehmigung von Kernel-Erweiterungen und voller Festplattenzugriff für Konnektoren.
    - HINWEIS: M1- und neuere Apple-Produkte können keine Profile verwenden, die diese Konfiguration enthalten

AllowNonAdminUserApprovals

AllowUserOverrides

AllowedKernelExtensions

TDNYQP7VRK

com.cisco.amp.nke

com.cisco.amp.fileop

PayloadDescription

PayloadDisplayName

Approved Kernel Extensions

PayloadEnabled

PayloadIdentifier

A872B6D5-D67C-41FE-BE64-3DD674C43C4F

PayloadOrganization

Cisco Systems, Inc.

PayloadType

com.apple.syspolicy.kernel-extension-policy

PayloadUUID

A872B6D5-D67C-41FE-BE64-3DD674C43C4F

PayloadVersion

Neue Verzeichnisstruktur

Versionen 1.14.0 bis 1.16.2

Der Mac-Connector 1.14 führt zwei Änderungen an der Verzeichnisstruktur ein:

1. Das Verzeichnis "Applications" (Anwendungen) wurde von `Cisco AMP` in `Cisco AMP für Endgeräte` umbenannt.
2. Das Kommandozeilen-Dienstprogramm `ampcli` wurde von `/opt/cisco/amp` auf /`Applications/Cisco AMP für Endgeräte/AMP für Endgeräte Connector.app/Contents/MacOS` verschoben. Das Verzeichnis `/opt/cisco/amp` enthält einen Symlink zum `ampcli` Programm an seinem neuen Standort.

Die vollständige Verzeichnisstruktur für die Mac-Connector-Versionen 1.14.0 bis 1.16.2 ist wie folgt:

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

Versionen 1.18.0 und neuere Versionen

Der Mac-Connector 1.18 führt eine Änderung der Verzeichnisstruktur der Anwendungen ein:

1. Das Anwendungsverzeichnis wurde von `Cisco AMP für Endgeräte` in `Cisco Secure Endpoint` umbenannt.

Die vollständige Verzeichnisstruktur für Mac Connector-Versionen 1.18.0 und höher sieht wie folgt aus:

```
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
```

Bekannte Probleme mit macOS 11.0 und Mac Connector 1.14.1.

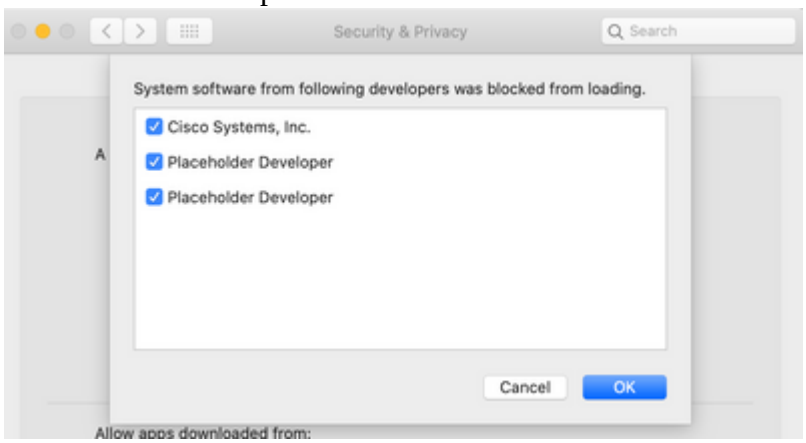
- Die Anleitung für Fehler 10, "Neustart zum Laden des Kernelmoduls oder der Systemerweiterung erforderlich", kann falsch sein, wenn vier oder mehr Netzwerkinhaltsfilter auf dem Computer installiert sind. Weitere Informationen finden Sie im Artikel Cisco Secure Endpoint Mac Connector Faults (Fehler bei Mac-Connectors).

Bekannte Probleme mit macOS 10.15/11.0 und Mac Connector 1.14.0.

- Einige Fehler, die durch den Mac-Anschluss ausgelöst werden, können unerwartet ausgelöst werden. Weitere Informationen finden Sie im Artikel Cisco Secure Endpoint Mac Connector Faults (Fehler bei Mac-Connectors).
    - Fehler 13, Zu viele Systemerweiterungen für den Netzwerkinhaltsfilter, können nach einem Upgrade ausgelöst werden. Ein Neustart des Computers behebt den Fehler in dieser Situation.
    - Fehler 15, Systemerweiterung erfordert vollständigen Festplattenzugriff, kann nach einem Neustart aufgrund eines Fehlers in macOS 11.0.0 ausgelöst werden. Dieses Problem wurde in macOS 11.0.1 behoben. Der Fehler kann behoben werden, indem der volle Festplattenzugriff im Bereich "Sicherheit und Datenschutz" in den macOS-Systemeinstellungen erneut gewährt wird.

- Während der Installation kann im Bereich "Sicherheit und Datenschutz" "Platzhalter-Entwickler" als Anwendungsname angezeigt werden, wenn macOS um die Berechtigung für die Ausführung der Systemerweiterungen des Mac-Connectors bittet. Dies ist auf einen Fehler in macOS 10.15

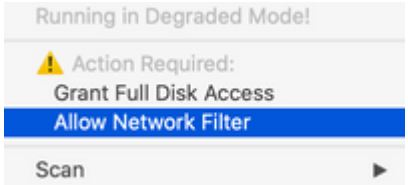
zurückzuführen. Markieren Sie die Kästchen neben "Platzhalter-Entwickler", damit der Mac-Anschluss den Computer schützen kann.



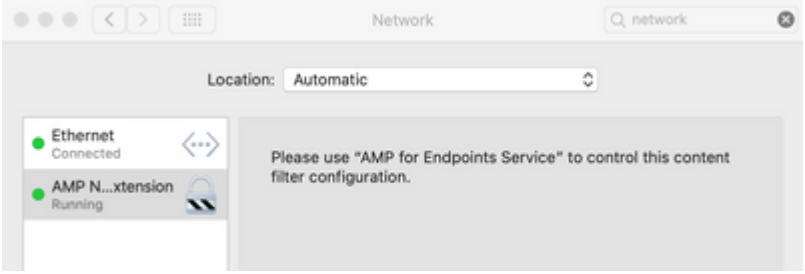
  - Mit dem Befehl `systemextensionsctl` list kann bestimmt werden, welche Systemerweiterungen genehmigt werden müssen. Systemerweiterungen mit dem Status `[enabled waiting for user]`in dieser Ausgabe werden als "Platzhalter-Entwickler" auf der zuvor gezeigten macOS-Einstellungsseite angezeigt. Wenn mehr als zwei "Platzhalter-Entwickler"-Einträge auf der Einstellungsseite angezeigt werden, deinstallieren Sie alle Software, die Systemerweiterungen verwendet (einschließlich des Mac-Anschlusses), sodass keine Systemerweiterungen genehmigt werden müssen, und installieren Sie dann den Mac-Anschluss neu.
    Die Systemerweiterungen für den Mac-Anschluss sind wie folgt gekennzeichnet:
    - Die Netzwerkerweiterung wird als `com.cisco.endpoint.svc.networkextension` angezeigt.
    - Die Endpoint Security-Erweiterung hat `com.cisco.endpoint.svc.securityextension`.

- Während der Installation kann die Aufforderung, dem Content-Filter die Überwachung des Netzwerkverkehrs zu gestatten, "(null)" als Anwendungsname anzeigen. Dies wird durch einen Fehler in macOS 10.15 verursacht. Der Benutzer muss "Zulassen" auswählen, um den Schutz des Computers zu gewährleisten.

- Wenn die Aufforderung abgelehnt wurde, weil "Nicht zulassen" ausgewählt wurde, wählen Sie die Option "Netzwerkfilter zulassen" aus dem Dropdown-Menü im Symbol "Agent" aus.  in der Menüleiste, um die Eingabeaufforderung erneut zu öffnen.



- Nach der Aktivierung wird der Filter für sichere Endpunkt-Netzwerkerweiterungen auf der Seite Netzwerkeinstellungen aufgeführt.



- Wenn unter macOS 11 ein Upgrade von Mac-Connector 1.12 auf Mac-Connector 1.14 durchgeführt wird, kann Fehler 4, Systemerweiterung konnte nicht geladen werden, vorübergehend ausgelöst werden, während der Connector von den Kernel-Erweiterungen zu den neuen Systemerweiterungen wechselt.

Bekannte Probleme bei der Deinstallation von Systemerweiterungen

- Vor macOS 12 oder wenn MDM nicht verwendet wird, wird der Benutzer bei einer Deinstallation des Mac-Connectors aufgefordert, sein Kennwort zweimal einzugeben, damit die Systemerweiterungen deinstalliert werden können. Dies ist eine Einschränkung von macOS und wurde in macOS 12 durch den in diesem Dokument beschriebenen Profilschlüssel RemovableSystemExtensions MDM etwas verbessert.

Intune Deployment-Installationsskript

- Ein Skript, das bei der Installation von Secure Endpoint Connector auf MacOS von Microsoft hilft, wird hier gehostet:

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

Mac Connector mit Rebranding (Versionen 1.18.0 und höher)

HINWEIS: Bestehende MDM-Konfigurationen für Connector-Versionen vor 1.18.0 funktionieren ohne Eingriff für Upgrades auf Connector-Versionen 1.18.0 und höher. Weitere Informationen finden Sie unter Secure Endpoint Mac Rebrand.

Revisionsverlauf

01.12.2020

- Der Mac-Connector 1.14.1 verwendet keine Systemerweiterungen auf macOS 10.15 mehr.
- Zusätzliche Hinweise zur Terminalprüfung, welche "Platzhalter-Entwickler"-Systemerweiterungen mit dem Mac-Anschluss 1.14.0 genehmigt werden müssen.

9. November 2020

- Korrigierte Paket-ID im vollständigen FestplattenzugriffscodeMDM-Nutzlast erforderlich.

03.11.2020

- Das Veröffentlichungsdatum für 1.14.0 Mac Connector ist November 2020.
- Der Mac-Connector 1.14.0 verwendet Systemerweiterungen mit macOS 10.15.5 und höher. Zuvor war dies 10.15.6.

- Abschnitt zu bekannten Problemen hinzugefügt.
- Die Gliederung der aktualisierten Verzeichnisstruktur.

3. Juni 2021

- Hinzugefügt, um den vollen Festplattenzugriff für Cisco Orbital zu gewähren.

13.10.2021

- Hinzufügen Entfernung von Mac Connector macOS Erweiterungen mit MDM Abschnitt.
- Known Issues for the Uninstall of System Extensions (Bekannte Probleme für die Deinstallation von Systemerweiterungen) hinzugefügt.

25.02.2022

- Rebrand

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.