Configureren van toegangsrechten voor Secure Endpoint Mac Connector en Orbital met MDM: volledige schijftoegang, systeemuitbreidingen

Inhoud

Inleiding

Dit document beschrijft recente wijzigingen en stappen voor beheerders om Mac-connector 1.14 en nieuwer te implementeren.

MDM-profielen

Het is sterk aanbevolen om de Mac-connector te implementeren met een MDM-profiel dat de vereiste goedkeuringen verleent. MDM-profielen moeten worden geïnstalleerd voordat de installatie, upgrade of verwijdering van de Mac-connector kan worden uitgevoerd om er zeker van te zijn dat de benodigde toegangsrechten worden herkend. Raadpleeg het gedeelte Bekende problemen later in dit document als MDM niet kan worden gebruikt.

Advisories

Versie 1.14 van de Mac-connector introduceerde veranderingen die aandacht vereisen:

- Goedkeuring van volledige schijftoegang
- Goedkeuring systeemuitbreiding

De Mac-connector 1.14 of nieuwer is vereist om eindpuntbescherming op macOS 11 en hoger te garanderen. Oudere Mac-connectors werken niet aan deze versies van macOS.

Versie 1.16 van de Mac-connector introduceerde ondersteuning voor Cisco Orbital op Intel-hardware. Orbital kan worden ingeschakeld in het beleid met de Advantage of Premier Tier en wordt automatisch geïnstalleerd als het is ingeschakeld en geïnstalleerd op een ondersteunde OS-versie en ondersteunde hardware. Versie 1.20 van de Mac-connector introduceert ondersteuningsgereedheid voor Cisco Orbital op Apple-siliciumhardware, gepland voor release met Orbital Node 1.21. Raadpleeg de secties Cisco Orbital van dit document voor meer informatie over het verlenen van de extra toegangsrechten tot de volledige schijf die nodig zijn voor Orbital.

Minimale vereisten voor besturingssysteem

Cisco Secure Endpoint Mac-connector 1.14.0 ondersteunt macOS-versies:

- macOS 11, met macOS systeemuitbreidingen.
- macOS 10.15.5 en hoger, met macOS systeemuitbreidingen.
- macOS 10.15.0 tot macOS 10.15.4, met macOS kernel extensies.
- macOS 10.14, met macOS kernel extensies.

Cisco Secure Endpoint Mac-connector 1.14.1 ondersteunt macOS-versies:

- macOS 11, met macOS systeemuitbreidingen.
- macOS 10.15 met macOS kernel extensies.
- macOS 10.14, met macOS kernel extensies.

Ondersteuning voor Cisco Orbital op Intel-hardware is geïntroduceerd in Secure Endpoint Mac-connector versie 1.16.0. Ondersteuning voor Cisco Orbital op Apple siliconen hardware werd geïntroduceerd in Secure Endpoint Mac-connector versie 1.20.0.

Raadpleeg de OS Compatibility Table voor de huidige compatibiliteit met de Mac-connector.

Belangrijke veranderingen

Mac-connector 1.14 introduceerde belangrijke wijzigingen op drie gebieden:

1. Goedkeuring van de macOS-uitbreidingen die door de connector worden gebruikt
2. Toegang tot volledige schijf
3. Nieuwe directorystructuur

MacOS 12 introduceerde een MDM-optie om verwijdering van de macOS-uitbreidingen van de connector toe te staan zonder een prompt voor gebruikerswachtwoorden.

Goedkeuring van de Mac Connector macOS-uitbreidingen

De Mac-connector gebruikt ofwel systeemuitbreidingen of legacy kerneluitbreidingen om systeemactiviteiten te monitoren, zoals nodig voor de macOS-versie. Op macOS 11 vervangt System Extensions de oude Kernel Extensions die niet worden ondersteund in macOS 11 en hoger. Gebruikersgoedkeuring is vereist voor alle versies van macOS voordat een van beide uitbreidingstypen kan worden uitgevoerd. Zonder goedkeuring zijn bepaalde connectorfuncties zoals het scannen van niet-toegankelijke bestanden en het bewaken van de netwerktoegang niet beschikbaar.

Mac-connector 1.14 introduceert twee nieuwe macOS systeemuitbreidingen:

1. Een extensie met de naam Endpoint Security, genaamd Secure Endpoint File Monitor (voorheen AMP Security Extension), om systeemgebeurtenissen te controleren
2. Een extensie voor netwerkcontentfilter, genaamd Cisco Secure Endpoint Filter (voorheen AMP Network Extension), om de netwerktoegang te bewaken

De twee bestaande Kernel Extensions, `ampfileop.kext` en `ampnetworkflow.kext`, zijn opgenomen voor achterwaartse compatibiliteit op oudere macOS versies die de nieuwe macOS System Extensions niet ondersteunen.

De vereiste goedkeuringen voor macOS 11** en hoger:

- Goedkeuren Secure Endpoint File Monitor voor laden
- Goedkeuren van het te laden Cisco Secure Endpoint filter
- Toestaan dat Cisco Secure Endpoint Filter netwerkinhoud filtert

** Mac-connector versie 1.14.0 vereiste ook deze goedkeuringen op macOS 10.15. Deze goedkeuringen zijn niet langer vereist op macOS 10.15 voor Mac-connector 1.14.1 of nieuwer.

De vereiste goedkeuringen voor macOS 10.14 en macOS 10.15:

- Kernel-uitbreidingen goedkeuren voor laden

Deze goedkeuringen kunnen worden verleend in de macOS Security & Privacy Voorkeuren op het eindpunt, of via Mobile Device Management (MDM) profielen.

Goedkeuring van de Mac Connector macOS-uitbreidingen op het eindpunt

Uitbreidingen van het systeem en van de Kernel kunnen handmatig worden goedgekeurd vanuit het macOS Security & Privacy Preferences-venster.

Goedkeuring van de Mac Connector macOS-uitbreidingen met MDM

OPMERKING: macOS-uitbreidingen kunnen niet retroactief worden goedgekeurd via MDM. Als het MDM-profiel niet is geïmplementeerd voor de installatie van de connector, worden de goedkeuringen niet verleend en is een extra interventie in een van de volgende twee vormen vereist:

1. Handmatige goedkeuring van de macOS-uitbreidingen op endpoints waarvoor het beheerprofiel met terugwerkende kracht is geïmplementeerd.

2. Upgrade de Mac-connector naar een nieuwere versie dan de huidige versie. Endpoints die het beheerprofiel met terugwerkende kracht hadden geïmplementeerd, herkennen het beheerprofiel na een upgrade en krijgen goedkeuring zodra de upgrade is voltooid.

Secure Endpoint extensies kunnen worden goedgekeurd met een beheerprofiel met deze payloads en eigenschappen:

payload	Eigendom	Waarde
Systeemuitbreidingen	Toegestane systeemuitbreidingen	com.cisco.endpoint.svc.security extensie, com.cisco.endpoint.svc.networkextensie
	Toegestane systeemuitbreidingstypen	Endpoint Security Extension, Network Extension
	Toegestane TeamIdentifiers	DE8Y96K9QP
Uitbreidingen van System Policy Core	Toegestane kerneluitbreidingen	com.cisco.amp.fileop, com.cisco.amp.nke
	Toegestane TeamIdentifiers	TDNYQP7VRK
WebContentFilter	AutoFilter ingeschakeld	onwaar
	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.net werkextensie
	Aangewezen vereiste voor FilterDataProvider	ankerappel-generiek en identificatiecode "com.cisco.endpoint.svc.networkextension" en (certificaatblad[field.1.2.840.113635.100.6.1.9] /* bestaat */ of certificaat 1[field.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[field.1.2.840.113635.100.6.1.13] /* bestaat */ en certificaatblad[subject.OU] = DE8Y8Y 6K9QP)
	Filterkwaliteit	firewall
	Filterbrowsers	onwaar
	Filterpakketten	onwaar
	Contacten voor filters	echt
	Plugin-bundel	com.cisco.endpoint.svc
	Door gebruiker gedefinieerde naam	Cisco Secure Endpoint Filter (AMP Network Extension indien de connectorversie ouder is dan 1.18.0)

Verwijdering van de Mac Connector macOS-uitbreidingen met MDM

MacOS 12 en hoger laat toe macOS Extensions te markeren als verwijderbaar met de eigenschap RemovableSystemExtensions zoals hieronder beschreven.
OPMERKING: Als macOS Extension removable toestemming is toegestaan, heeft elke gebruiker of elk proces met root privileges de mogelijkheid om de extensie te verwijderen zonder een prompt voor het gebruikerswachtwoord. Aldus, moet het bezit RemovableSystemExtensions slechts worden gebruikt wanneer de beheerder het uninstall van de connector wil automatiseren.
OPMERKING: macOS-uitbreidingen kunnen niet retroactief worden verwijderd via MDM. Als het MDM-profiel niet is geïmplementeerd voordat de connector wordt verwijderd, wordt geen toestemming verleend voor het verwijderen van macOS Extensions en moet de gebruiker tijdens het proces voor het verwijderen van de connector handmatig een wachtwoord invoeren op het eindpunt om de macOS Extensions te

verwijderen.

Secure Endpoint-extensies kunnen worden verwijderd als onderdeel van de connector-verwijdering door wanneer een beheerprofiel met de eigenschap RemovableSystemExtensions toegevoegd aan de SystemExtensions-payload is geïnstalleerd. De eigenschap RemovableSystemExtensions moet de bundelherkenningstekens van beide Secure Endpoint-uitbreidingen bevatten:

payload	Eigendom	Waarde
Systeemuitbreidingen	Uitbreidingen van verwijderbaar systeem	com.cisco.endpoint.svc.security extensie, com.cisco.endpoint.svc.networkextensie

Toegang tot volledige schijf

MacOS 10.14 en later vereist goedkeuring voordat een toepassing toegang kan krijgen tot delen van het bestandssysteem die persoonlijke gebruikersgegevens bevatten (bijvoorbeeld Contactgegevens, Foto's, Agenda en andere toepassingen). Bepaalde connectorfuncties zoals het scannen van niet-toegankelijke bestanden zijn niet in staat om deze bestanden zonder goedkeuring te scannen op bedreigingen.

Eerdere versies van de Mac-connector vereisten de gebruiker om volledige schijftoegang tot het `ampdaemon`-programma te verlenen. Mac-connector 1.14 vereist volledige schijftoegang voor:

- "Advanced Malware Protection voor endpoints-service"
- "AMP security uitbreiding"

Voor Mac-connector 1.16.0 en nieuwer is extra volledige schijftoegang nodig voor:

- "Cisco Orbital" indien ingeschakeld in het beleid, beschikbaar met Advantage en Premier access

Voor Mac-connector 1.18 en nieuwer is volledige schijftoegang vereist voor:

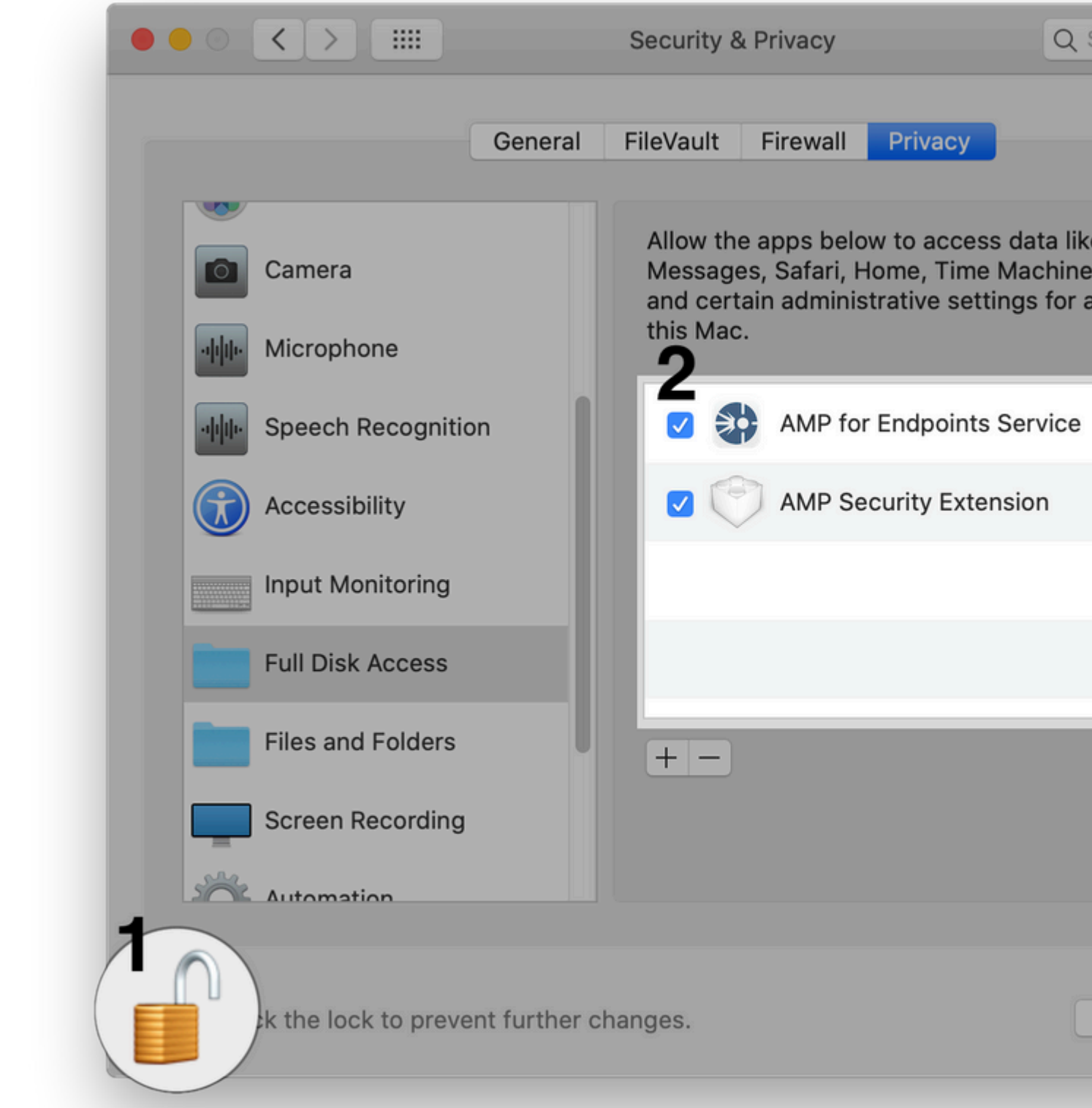
- "Secure Endpoint Service"
- "Secure Endpoint System Monitor"
- "Cisco Orbital" wanneer Orbital is ingeschakeld in het beleid (beschikbaar met Advantage- en Premier-tiers)

Het `ampdaemon`-programma heeft geen volledige schijftoegang meer nodig met de Mac-connector versie 1.14 en nieuwer.

Goedkeuringen voor volledige schijftoegang kunnen worden verleend in de voorkeuren voor beveiliging en privacy van macOS op het eindpunt of via profielen voor mobiel apparaatbeheer (MDM).

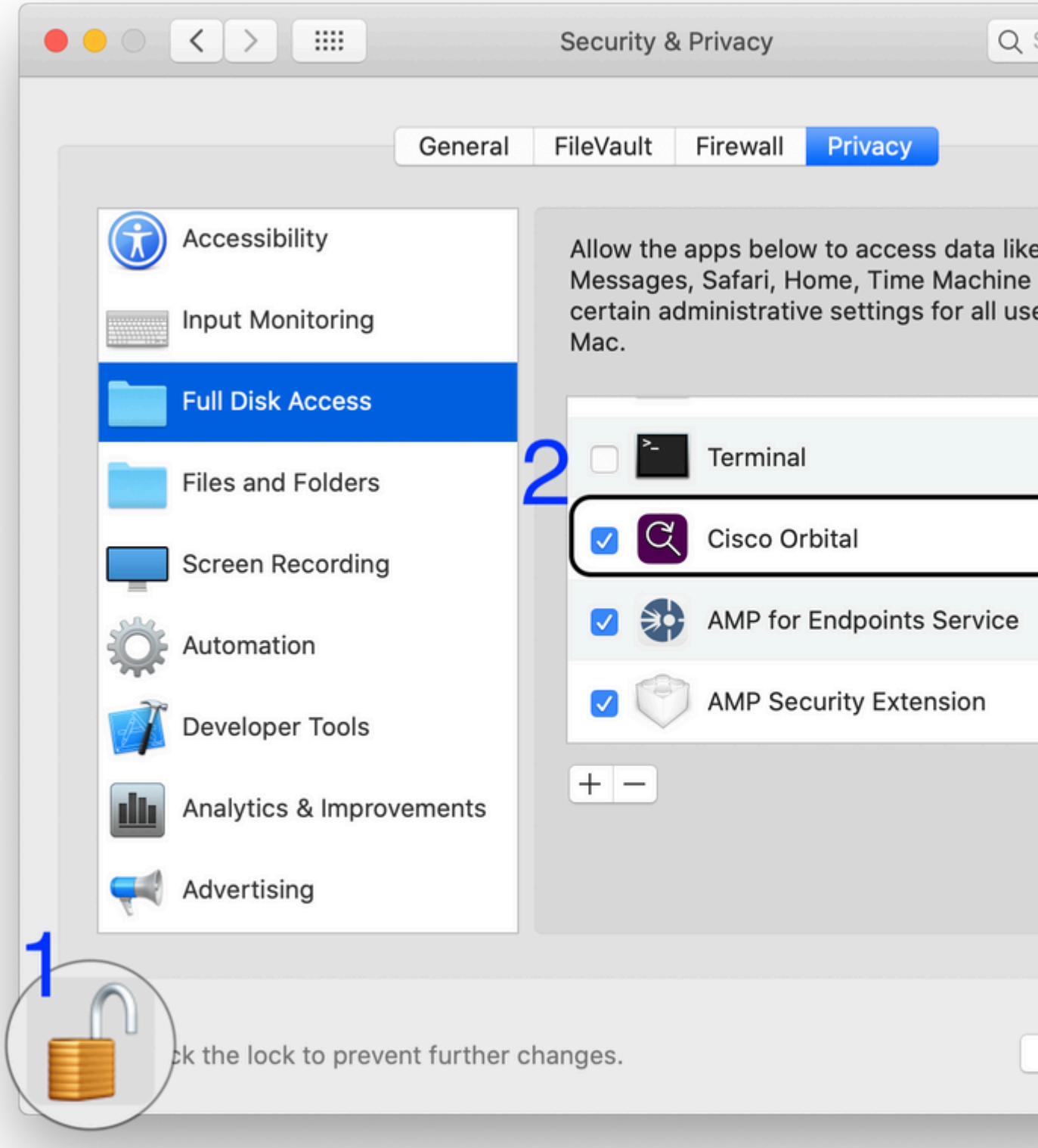
Goedkeuring van volledige schijftoegang voor connectorversies ouder dan 1.18.0 op het eindpunt

Full Disk Access kan handmatig worden goedgekeurd vanuit het deelvenster met voorkeuren voor beveiliging en privacy van macOS.



Goedkeuring van volledige schijftoegang voor Cisco Orbital op het Endpoint

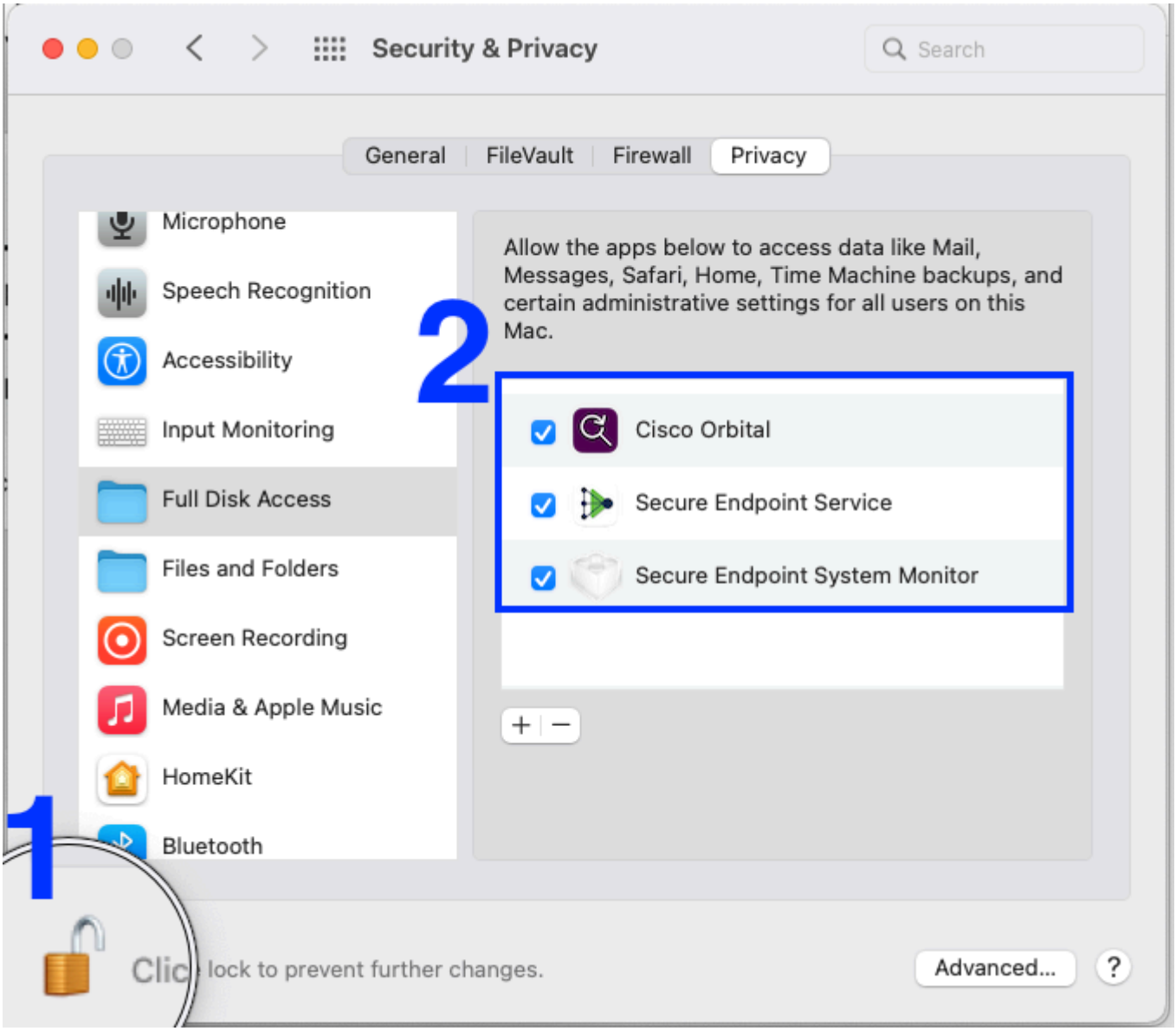
Full Disk Access kan handmatig worden goedgekeurd vanuit het deelvenster met voorkeuren voor beveiliging en privacy van macOS.



Goedkeuring van volledige schijftoegang voor Cisco Secure Endpoint-connector 1.18.0 en nieuwer op het Endpoint

Full Disk Access kan handmatig worden goedgekeurd vanuit het deelvenster met voorkeuren voor

beveiliging en privacy van macOS.



Goedkeuring van volledige schijftoegang voor de connector met MDM

OPMERKING: macOS-uitbreidingen kunnen niet retroactief worden goedgekeurd via MDM. Als het MDM-profiel niet is geïmplementeerd voor de installatie van de connector, worden de goedkeuringen niet verleend en is een extra interventie in een van de volgende twee vormen vereist:

1. Handmatige goedkeuring van de macOS-uitbreidingen op endpoints waarvoor het beheerprofiel met terugwerkende kracht is geïmplementeerd.
2. Upgrade de Mac-connector naar een nieuwere versie dan de huidige versie. Endpoints die het met terugwerkende kracht geïmplementeerde beheerprofiel hadden, herkennen het beheerprofiel na de upgrade en krijgen goedkeuring zodra de upgrade is voltooid.

Volledige schijftoegang kan worden goedgekeurd door een beheerprofiel Privacy Preferences Policy Control payload met een SystemPolicyAllFiles eigenschap met twee ingangen, één voor de `Secure Endpoint Service (AMP voor Endpoints Service voor connectorversies ouder dan 1.18.0)` en één voor de `Secure Endpoint System Monitor (AMP Security Extension voor connectorversies ouder dan 1.18.0)`:

Beschrijving	Eigendom	Waarde
Secure Endpoint	TOEGESTAAN	echt

Beschrijving	Eigendom	Waarde
Service (AMP voor endpoints-service)	Codevereiste	ankerappel generiek en identificator "com.cisco.endpoint.svc" en (certificaatblad[field.1.2.840.113635.100.6.1.9] /* bestaat */ of certificaat 1[field.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[field.1.2.840.113635.100.6.1.13] /* bestaat */ en certificaatblad[subject.OU] = DE9Y96K P)
	Identificatie	com.cisco.endpoint.svc
	Identificatietype	bundel-ID
Secure Endpoint System Monitor (AMP Security Extension)	TOEGESTAAN	echt
	Codevereiste	ankerappel-generiek en identificatiecode "com.cisco.endpoint.svc.security extension" en (certificaatblad[field.1.2.840.113635.100.6.1.9] /* bestaat */ of certificaat 1[field.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[field.1.2.840.113635.100.6.1.13] /* bestaat */ en certificaatblad[subject.OU] = DE8DE 96K9QP)
	Identificatie	com.cisco.endpoint.svc.security extensie
	Identificatietype	bundel-ID

Als uw implementatie computers bevat met connector versie 1.12.7 of ouder geïnstalleerd, is deze extra ingang nog steeds vereist om volledige schijftoegang tot `ampdaemon` te verlenen voor die computers:

Beschrijving	Eigendom	Waarde
ampdaemon	TOEGESTAAN	echt
	Codevereiste	identificatiecode ampdaemon en ankerappel generiek en certificaat 1[field.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[field.1.2.840.113635.100.6.1.13] /* bestaat */ en certificaatblad[subject.OU] = TDNYQP7VRK
	Identificatie	/opt/cisco/amp/ampdaemon
	Identificatietype	weg

Goedkeuring van volledige schijftoegang voor Cisco Orbital met MDM

Als uw implementatie computers bevat met Cisco Secure Endpoint Mac-connectorversies 1.16.0 of nieuwer, op computers met macOS 10.15 of nieuwer, en Orbital is ingeschakeld in het beleid, is deze extra vermelding nog steeds vereist om volledige schijftoegang tot Orbital te verlenen voor die computers:

Beschrijving	Eigendom	Waarde
Cisco orbitaal	TOEGESTAAN	echt
	Codevereiste	ankerappel generiek en identificator "com.cisco.endpoint.orbital.app" en (certificaatblad[field.1.2.840.113635.100.6.1.9] /* bestaat */ of certificaat 1[field.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[field.1.2.840.113635.100.6.1.13] /* bestaat */ en certificaatblad[subject.OU] = DE8Y99QP)
	Identificatie	com.cisco.endpoint.orbital.app
	Identificatietype	bundel-ID

MDM-configuratieprofiel als voorbeeld

Dit voorbeeld-MDM-configuratieprofiel kan als referentie worden gebruikt.

- Goedkeuring van systeemuitbreidingen voor Secure Endpoint Mac-connector.
- Verleent volledige schijftoegang voor de Secure Endpoint Mac-connector en Orbital.
- Maakt het mogelijk om systeemuitbreidingen op stille wijze te verwijderen wanneer de connector wordt verwijderd.
  OPMERKING: Als toestemming is verleend voor het verwijderen van de extensie van het systeem, heeft elke gebruiker of elk proces met de basisrechten de mogelijkheid om de systeemuitbreiding te verwijderen zonder een prompt voor het gebruikerswachtwoord. Aldus, moet het bezit RemovableSystemExtensions slechts worden gebruikt wanneer de beheerder het uninstall van de connector wil automatiseren.

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-voorbeeldconfiguratie voor macOS 10.15 of hoger

- Goedkeuring van kernel extensies en verleent volledige schijftoegang voor connectors.
    - OPMERKING: M1 en nieuwere Apple-producten kunnen geen profielen gebruiken die deze configuratie bevatten

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

1

Nieuwe directorystructuur

Versies 1.14.0 tot en met 1.16.2

Mac-connector 1.14 introduceert twee wijzigingen in de directorystructuur:

1. De directory Toepassingen is hernoemd van `Cisco Advanced Malware Protection` naar `Cisco Advanced Malware Protection voor endpoints`.
2. De `versterker` van het opdrachtregel-hulpprogramma is verplaatst van `/opt/cisco/amp` naar `/Application/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS`. De directory `/opt/cisco/amp` bevat een symlink naar het `ampcli`-programma op de nieuwe locatie.

De volledige directorystructuur voor de Mac-connector versies 1.14.0 tot en met 1.16.2 is als volgt:

```
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
```

Versies 1.18.0 en nieuwer

Mac-connector 1.18 introduceert een wijziging in de structuur van de toepassingsdirectory:

1. De directory Toepassingen is hernoemd van `Cisco Advanced Malware Protection for Endpoints` naar `Cisco Secure Endpoint`.

De volledige directory structuur voor Mac connector versies 1.18.0 en nieuwer is als volgt:

```
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
```

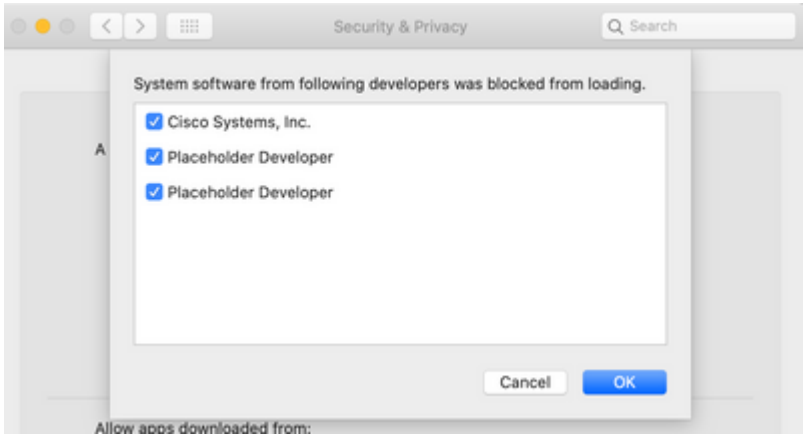
Bekende problemen met macOS 1.0 en Mac Connector 1.14.1.

- De richtlijnen voor fout 10, "Reboot vereist om pit module of systeemuitbreiding te laden,"kunnen onjuist zijn als vier of meer Filters van de Inhoud van het Netwerk op de computer worden geïnstalleerd. Raadpleeg het artikel Cisco Secure Endpoint Mac Connector voor meer informatie.

Bekende problemen met macOS 10.15/11.0 en Mac Connector 1.14.0.

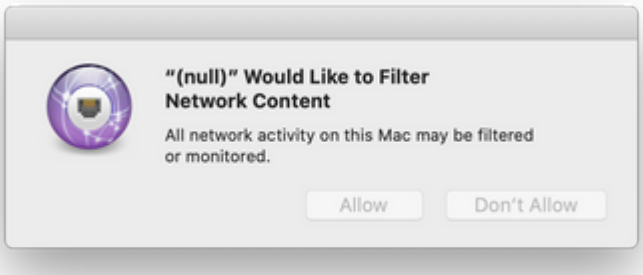
- Sommige fouten die door de Mac-connector worden opgeroepen, kunnen onverwacht worden verhoogd. Raadpleeg het artikel Cisco Secure Endpoint Mac Connector voor meer informatie.
    - Fout 13, Teveel systeemuitbreidingen van de Filter van de Netwerkinhoud, kan na een verbetering worden opgeheven. Door de computer opnieuw op te starten, wordt de fout in deze situatie opgelost.
    - Fout 15, System Extension vereist Full Disk Access, kan worden verhoogd na reboot vanwege een bug in macOS 11.0.0. Dit probleem is opgelost in macOS 11.0.1. De fout kan worden opgelost door opnieuw volledige schijftoegang te verlenen in het Security & Privacy-venster in macOS System Preferences.

- Tijdens de installatie kan het Security & Privacy-venster "Placeholder Developer" als de naam van de toepassing weergeven wanneer macOS om toestemming vraagt voor het uitvoeren van de Mac-connector systeemuitbreidingen. Dit komt door een bug in macOS 10.15. Schakel de selectievakjes naast "Plaatsaanduiding Ontwikkelaar" in om de Mac-connector in staat te stellen de computer te beschermen.

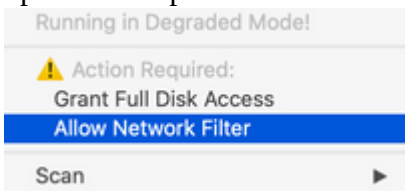


- De `systemextensionsctl` listcommando kan worden gebruikt om te bepalen welke systeemextensies goedkeuring nodig hebben. Uitbreidingen van het systeem met de staat `[geactiveerd wachten op gebruiker]`in deze uitvoer worden weergegeven als "Placeholder Developer" op de macOS voorkeuren pagina eerder weergegeven. Als meer dan twee "Plaatsaanduiding Ontwikkelaar"-vermeldingen worden weergegeven in de voorkeurpagina, verwijder dan alle software die systeemextensies gebruikt (inclusief de Mac-connector), zodat geen systeemuitbreidingen goedkeuring nodig hebben, en installeer vervolgens de Mac-connector opnieuw.
  De Mac-connector systeemuitbreidingen worden als volgt geïdentificeerd:
  - De uitbreiding van het netwerk wordt getoond als `com.cisco.endpoint.svc.net-extensie`.
  - De uitbreiding Endpoint Security wordt weergegeven met: `com.cisco.endpoint.svc.security extensie`.

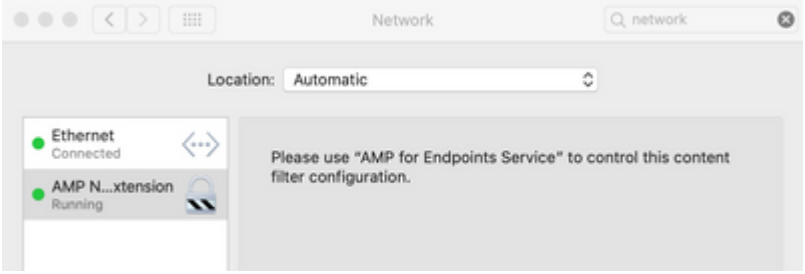
- Tijdens de installatie kan de prompt om het contentfilter toe te staan netwerkverkeer te bewaken "(null)" als de toepassingsnaam weergeven. Dit wordt veroorzaakt door een bug in macOS 10.15. De gebruiker moet Toestaan selecteren om de computer te kunnen beveiligen.



- Als de prompt werd afgewezen omdat "Niet toestaan" was gekozen, selecteer dan "Netwerkfilter toestaan" in het vervolgkeuzemenu in het pictogram Agent  in de menubalk om de prompt opnieuw te openen.



- Als deze optie is ingeschakeld, wordt het filter Secure Endpoint Network Extension vermeld op de pagina Netwerkvoorkeuren.



- Op macOS 11, wanneer een upgrade van Mac-connector 1.12 naar Mac-connector 1.14 wordt uitgevoerd, kan Fault 4, System Extension Cannot Load tijdelijk worden verhoogd, terwijl de connector overgaat van de kernel-extensies naar de nieuwe systeemextensies.

Bekende problemen tijdens verwijdering van systeemuitbreidingen

- Voorafgaand aan macOS 12, of wanneer MDM niet wordt gebruikt, wanneer een verwijdering van de Mac-connector wordt uitgevoerd, wordt de gebruiker gevraagd om hun wachtwoord tweemaal in te voeren zodat de systeemextensies kunnen worden verwijderd. Dit is een beperking van macOS en is enigszins verbeterd in macOS 12 met de toevoeging van de RemovableSystem Extensions MDM-profielsleutel die in dit document wordt beschreven.

Intune-installatiescript voor implementatie

- Een script dat zal helpen bij het installeren van Secure Endpoint connector op macOS onderhouden door Microsoft wordt hier gehost:

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

Rebranded Mac Connector (versies 1.18.0 en nieuwer)

OPMERKING: Bestaande MDM-configuraties voor connectorversies ouder dan 1.18.0 werken zonder tussenkomst voor upgrades naar connector versies 1.18.0 en nieuwer. Zie Secure Endpoint voor meer informatie.

Revisiegeschiedenis

1 dec. 2020

- Mac-connector 1.14.1 gebruikt geen systeemuitbreidingen meer op macOS 10.15.
- Aanvullende richtlijnen voor terminalcontrole die "Placeholder Developer" System Extensions moet worden goedgekeurd met Mac-connector 1.14.0.

9 nov. 2020

- Gecorrigeerde bundel-ID in volledige schijftoegangscodeVereiste MDM payload.

3 nov. 2020

- De release datum voor 1.14.0 Mac-connector is november 2020.
- De 1.14.0 Mac-connector maakt gebruik van System Extensions met macOS 10.15.5 en hoger. Voorheen was dit 10.15.6.
- Toegevoegd Gekende Problemen sectie.
- Bijgewerkt overzicht van de directorystructuur.

3 juni 2021

- Toegevoegd richtlijnen voor het verlenen van volledige schijftoegang voor Cisco Orbital.

13 okt. 2021

- Toegevoegd Verwijdering van Mac Connector macOS Uitbreidingen met MDM sectie.
- Toegevoegd Bekende Problemen voor het verwijderen van systeemuitbreidingen sectie.

25 feb. 2022

- rebranderen

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.