

Configuration des autorisations pour le connecteur Mac et l'orbite des terminaux sécurisés avec MDM : accès complet au disque, extensions système

Table des matières

[Introduction](#)

[Profils MDM](#)

[Avis](#)

[Configuration minimale du système d'exploitation](#)

[Changements importants](#)

[Approbation des extensions Mac Connector macOS](#)

[Approbation des extensions Mac Connector macOS au niveau du terminal](#)

[Approbation des extensions Mac Connector macOS avec MDM](#)

[Retrait des extensions Mac Connector macOS avec MDM](#)

[Accès au disque complet](#)

[Approbation de l'accès au disque complet pour les versions de connecteur antérieures à 1.18.0 au niveau du terminal](#)

[Approbation de l'accès complet au disque pour Cisco Orbital au niveau du terminal](#)

[Approbation de l'accès complet au disque pour le connecteur Cisco Secure Endpoint 1.18.0 et versions ultérieures au niveau du terminal](#)

[Approbation de l'accès complet au disque pour le connecteur avec MDM](#)

[Approbation de l'accès complet au disque pour Cisco Orbital avec MDM](#)

[Exemple de profil de configuration MDM](#)

[Exemple de configuration MDM pour macOS 10.15 ou version antérieure](#)

[Nouvelle structure de répertoires](#)

[Versions 1.14.0 à 1.16.2](#)

[Versions 1.18.0 et ultérieures](#)

[Problèmes connus avec macOS 11.0 et Mac Connector 1.14.1.](#)

[Problèmes connus avec macOS 10.15/11.0 et Mac Connector 1.14.0.](#)

[Problèmes connus lors de la désinstallation des extensions système](#)

[Déploiement IntuneScript d'installation](#)

[Connecteur Mac renommé \(versions 1.18.0 et ultérieures\)](#)

[Historique de révision](#)

Introduction

Ce document décrit les modifications récentes et les étapes à suivre par les administrateurs pour déployer le connecteur Mac 1.14 et les versions ultérieures.

Profils MDM

Il est vivement recommandé de déployer le connecteur Mac avec un profil MDM qui accorde les approbations requises. Les profils MDM doivent être installés avant l'installation, la mise à niveau ou le retrait du connecteur Mac pour que les autorisations nécessaires soient reconnues. Reportez-vous à la section Problèmes connus plus loin dans ce document si MDM ne peut pas être utilisé.

Avis

La version 1.14 du connecteur Mac a introduit des modifications nécessitant une attention particulière :

- Autorisation d'accès au disque complet
- Approbation [d'extension du système](#)

Le connecteur Mac 1.14 ou version ultérieure est requis pour assurer la protection des terminaux sur macOS 11 et versions ultérieures. Les connecteurs Mac plus anciens ne fonctionnent pas sur ces versions de macOS.

La version 1.16 du connecteur Mac a introduit la prise en charge de [Cisco Orbital](#) sur le matériel Intel. Orbital peut être activé dans la politique avec le niveau Advantage ou Premier et est installé automatiquement quand activé et installé sur une version de système d'exploitation prise en charge et le matériel pris en charge. La version 1.20 du connecteur Mac intègre la prise en charge du matériel Cisco Orbital sur silicium Apple, dont la sortie est prévue avec Orbital Node 1.21. Reportez-vous aux sections Cisco Orbital de ce document pour plus de détails sur la façon d'accorder les autorisations d'accès disque complètes supplémentaires requises pour Orbital.

Configuration minimale du système d'exploitation

Cisco Secure Endpoint Mac Connector 1.14.0 prend en charge les versions macOS :

- macOS 11, avec extensions système macOS.
- macOS 10.15.5 et versions ultérieures, avec extensions système macOS.
- macOS 10.15.0 à macOS 10.15.4, avec extensions du noyau macOS.
- macOS 10.14, avec extensions du noyau macOS.

Cisco Secure Endpoint Mac Connector 1.14.1 prend en charge les versions macOS :

- macOS 11, avec extensions système macOS.
- macOS 10.15 avec extensions du noyau macOS.
- macOS 10.14, avec extensions du noyau macOS.

La prise en charge de Cisco Orbital sur le matériel Intel a été introduite dans la version 1.16.0 du connecteur Mac Secure Endpoint. La prise en charge de Cisco Orbital sur le matériel en silicium Apple a été introduite dans la version 1.20.0 du connecteur Mac Secure Endpoint.

Consultez le [Tableau de compatibilité du système d'exploitation](#) pour connaître la compatibilité actuelle du connecteur Mac.

Changements importants

Le connecteur Mac 1.14 a introduit des modifications importantes dans trois domaines :

1. Approbation des extensions macOS utilisées par le connecteur
2. Accès au disque complet
3. Nouvelle structure de répertoires

MacOS 12 a introduit une option MDM pour permettre la suppression des extensions macOS du connecteur sans invite pour les mots de passe utilisateur.

Approbation des extensions Mac Connector macOS

Le connecteur Mac utilise les extensions système ou les extensions de noyau héritées pour surveiller les activités du système, selon les besoins de la version macOS. Sur macOS 11, les [extensions système](#) remplacent les anciennes [extensions de noyau](#) qui ne sont pas prises en charge dans macOS 11 et versions ultérieures. L'approbation de l'utilisateur est requise sur toutes les versions de macOS avant que l'un ou l'autre type d'extension soit autorisé à s'exécuter. Sans approbation, certaines fonctions de connecteur, telles que l'analyse des fichiers à l'accès et le moniteur d'accès réseau, ne sont pas disponibles.

Le connecteur Mac 1.14 introduit deux nouvelles extensions système macOS :

1. Une extension [Endpoint Security](#), appelée Secure Endpoint File Monitor (anciennement AMP Security Extension), pour surveiller les événements système
2. Une extension [Network Content Filter](#), nommée Cisco Secure Endpoint Filter (anciennement AMP Network Extension), pour surveiller l'accès au réseau

Les deux anciennes extensions de noyau, `ampfileop.kext` et `ampnetworkflow.kext`, sont incluses pour la rétrocompatibilité sur les versions plus anciennes de macOS qui ne prennent pas en charge les nouvelles extensions système macOS.

Les approbations requises pour macOS 11** et versions ultérieures :

- Approuver le chargement de Secure Endpoint File Monitor
- Approuver le chargement de Cisco Secure Endpoint Filter
- Autoriser Cisco Secure Endpoint Filter à filtrer le contenu du réseau

** La version 1.14.0 du connecteur Mac nécessitait également ces approbations sur macOS 10.15. Ces approbations ne sont plus requises sur macOS 10.15 pour le connecteur Mac 1.14.1 ou ultérieur.

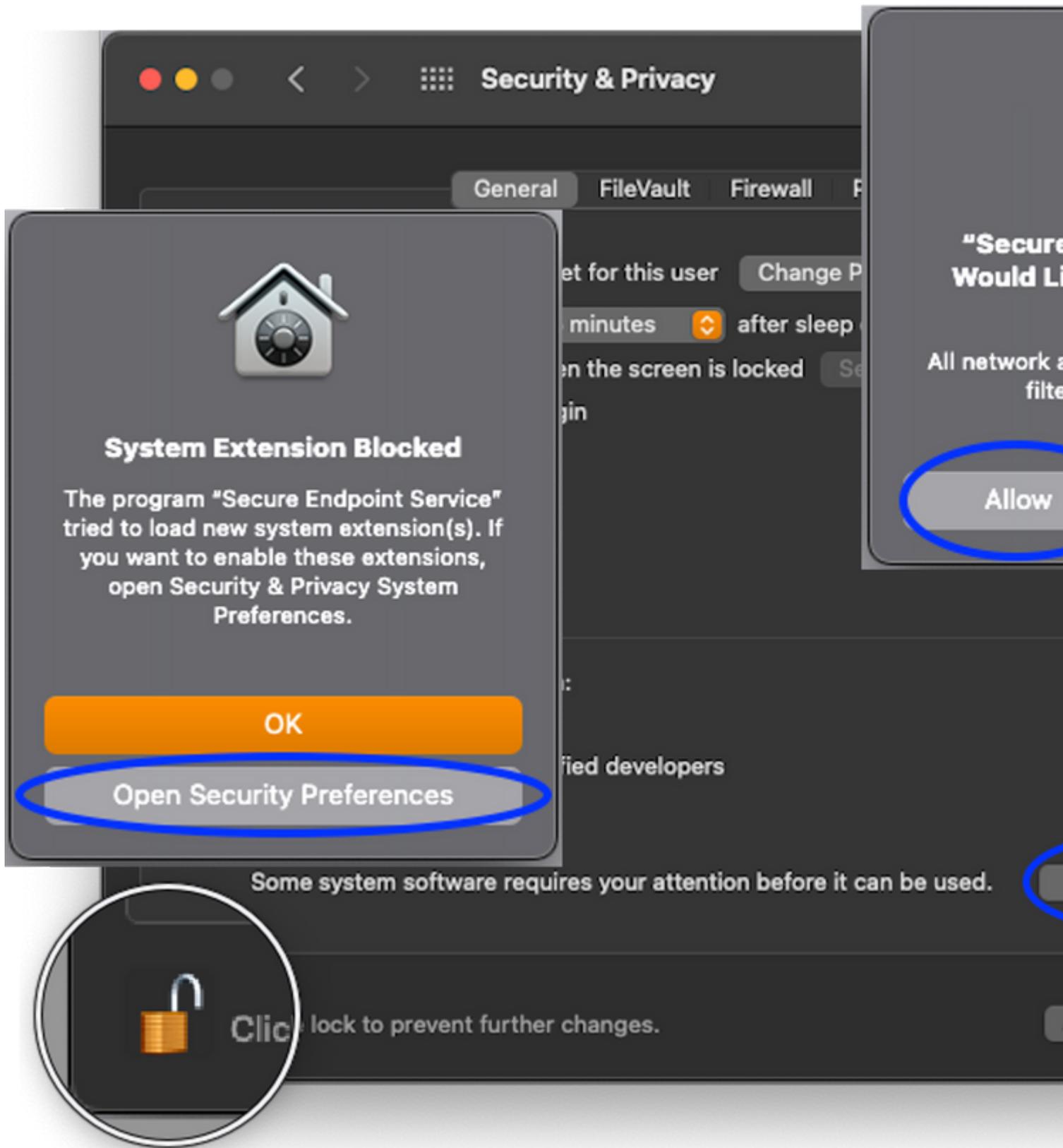
Les approbations requises pour macOS 10.14 et macOS 10.15 :

- Approuver le chargement des extensions de noyau du connecteur

Ces approbations peuvent être accordées dans les préférences de sécurité et de confidentialité macOS sur le terminal, ou via les profils [MDM \(Mobile Device Management ou gestion des appareils mobiles\)](#).

Approbation des extensions Mac Connector macOS au niveau du terminal

Les extensions système et noyau peuvent être approuvées manuellement à partir du volet des préférences de sécurité et de confidentialité de macOS.



Approbation des extensions Mac Connector macOS avec MDM

REMARQUE : les extensions macOS ne peuvent pas être approuvées rétroactivement via MDM. Si le profil MDM n'est pas déployé avant l'installation du connecteur, les approbations ne sont pas accordées et une intervention supplémentaire est requise sous l'une des deux formes suivantes :

1. Approbation manuelle des extensions macOS sur les terminaux dont le profil de gestion a été déployé rétroactivement.

2. Mettez à niveau le connecteur Mac vers une version plus récente que celle actuellement déployée. Les terminaux dont le profil de gestion a été déployé reconnaissent rétroactivement le profil de gestion après une mise à niveau et obtiennent l'approbation une fois la mise à niveau terminée.

Les extensions Secure Endpoint peuvent être approuvées avec un profil de gestion avec les charges utiles et propriétés suivantes :

Charge Utile	Propriété	Valeur
Extensions système	ExtensionsSystèmeAutorisées	com.cisco.endpoint.svc.securityexte com.cisco.endpoint.svc.networkexte
	TypesExtensionSystèmeAutorisés	ExtensionSécuritéTerminaux, ExtensionRéseau
	IdentificateursÉquipeAutorisés	DE8Y96K9QP
ExtensionsNoyauPolitiqueSystème	ExtensionsNoyauAutorisées	com.cisco.amp.fileop, com.cisco.am
	IdentificateursÉquipeAutorisés	TDNYQP7VRK
FiltreContenuWeb	FiltreAutomatiqueActivé	falsifié
	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.networkexte
	FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc.networkexte and (certificate leaf[field.1.2.840.113635.100.6.1.9] existing */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* existing */ and certificate leaf[field.1.2.840.113635.100.6.1.1] existing */ and certificate leaf[subje = DE9Y96K QP)
	CatégorieFiltre	cloison pare-feu
	FiltrerNavigateurs	falsifié
	PaquetsFiltres	falsifié
	FilterSockets	vrai
	IDbundlePlugin	com.cisco.endpoint.svc
NomDéfiniUtilisateur	Cisco Secure Endpoint Filter (AMP Network Extension si la version du connecteur est antérieure à 1.18.0)	

Retrait des extensions Mac Connector macOS avec MDM

MacOS 12 et versions ultérieures permet de marquer les extensions macOS comme amovibles avec la propriété [RemovableSystemExtensions](#) comme décrit ci-dessous.

REMARQUE : lorsque l'autorisation d'accès amovible Extension macOS est autorisée, tout utilisateur ou processus disposant de privilèges racine peut supprimer l'extension sans être invité à saisir le mot de passe utilisateur. Ainsi, la propriété `RemovableSystemExtensions` ne doit être utilisée que lorsque l'administrateur souhaite automatiser la désinstallation du connecteur.

REMARQUE : les extensions macOS ne peuvent pas être supprimées rétroactivement via MDM. Si le profil MDM n'est pas déployé avant la désinstallation du connecteur, l'approbation de la suppression des extensions macOS n'est pas accordée et l'utilisateur doit entrer manuellement un mot de passe sur le terminal pendant le processus de désinstallation du connecteur pour supprimer les extensions macOS.

Les extensions Secure Endpoint peuvent être supprimées lors de la désinstallation du connecteur lorsqu'un profil de gestion avec la propriété RemovableSystemExtensions ajoutée à la charge utile SystemExtensions est installé. La propriété RemovableSystemExtensions doit contenir les identificateurs d'ensemble des deux extensions Secure Endpoint :

Charge Utile	Propriété	Valeur
Extensions système	ExtensionsSystèmeAmovibles	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Accès au disque complet

MacOS 10.14 et versions ultérieures nécessitent une approbation avant qu'une application puisse accéder à des parties du système de fichiers qui contiennent des données utilisateur personnelles (par exemple, Contacts, Photos, Calendrier et autres applications). Certaines fonctions de connecteur, telles que l'analyse des fichiers à l'accès, ne peuvent pas analyser ces fichiers sans approbation.

Les versions précédentes des connecteurs Mac nécessitaient que l'utilisateur accorde un accès disque complet au programme ampd daemon. Le connecteur Mac 1.14 nécessite un accès complet au disque pour :

- "Service AMP for Endpoints"
- "Extension de sécurité AMP"

Le connecteur Mac 1.16.0 et les versions ultérieures nécessitent un accès disque complet supplémentaire pour :

- « Cisco Orbital » lorsqu'il est activé dans la politique, disponible avec l'accès Advantage et Premier

Le connecteur Mac 1.18 et les versions ultérieures nécessitent un accès complet au disque pour :

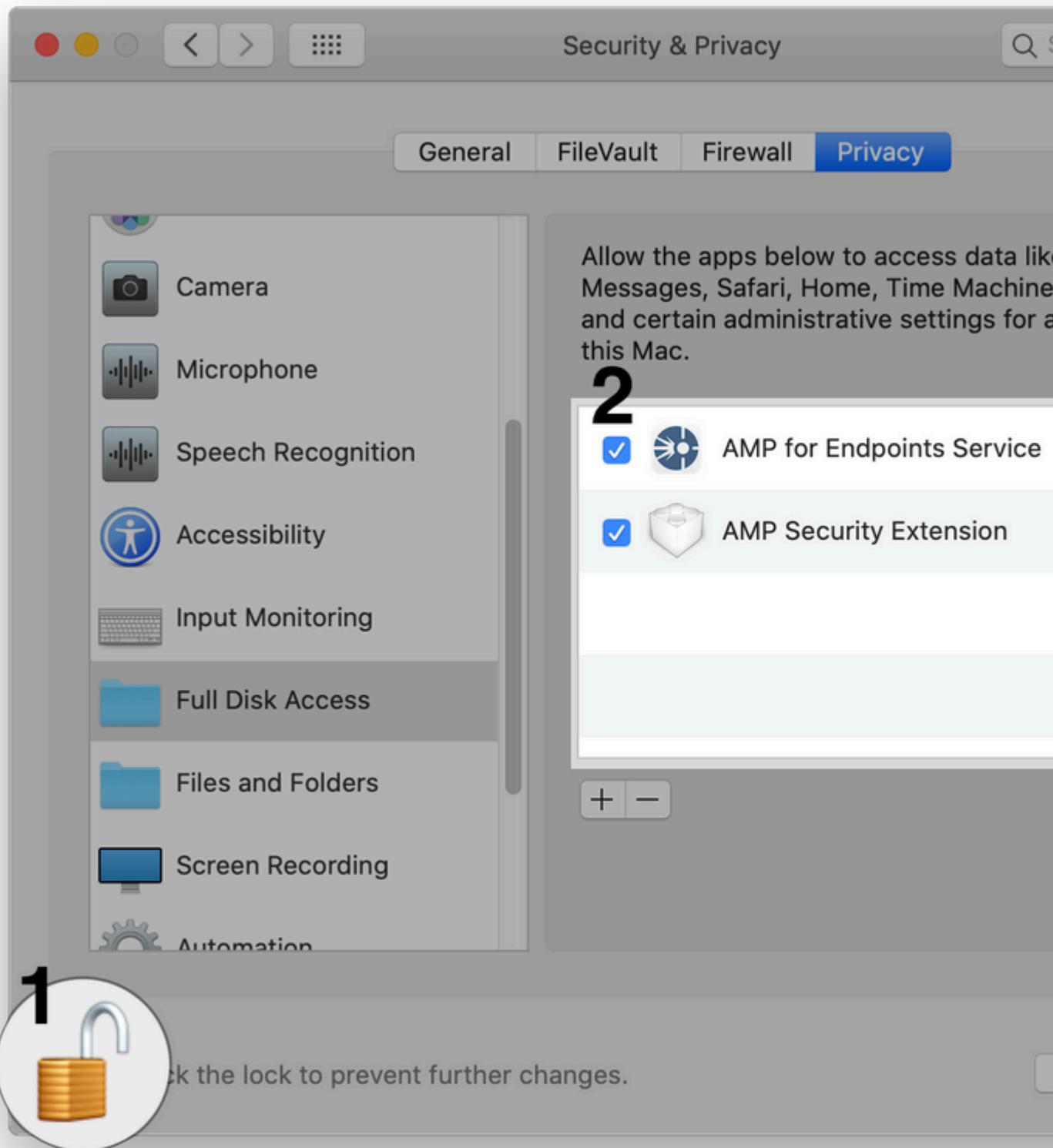
- « Secure Endpoint Service »
- "Secure Endpoint System Monitor"
- « Cisco Orbital » lorsque l'option Orbital est activée dans la stratégie (disponible avec les niveaux Advantage et Premier)

Le programme ampd daemon ne nécessite plus l'accès complet au disque avec le connecteur Mac version 1.14 et plus récente.

Les approbations d'accès complet au disque peuvent être accordées dans les préférences de sécurité et de confidentialité macOS sur le terminal, ou via les profils [MDM \(Mobile Device Management ou gestion des appareils mobiles\)](#).

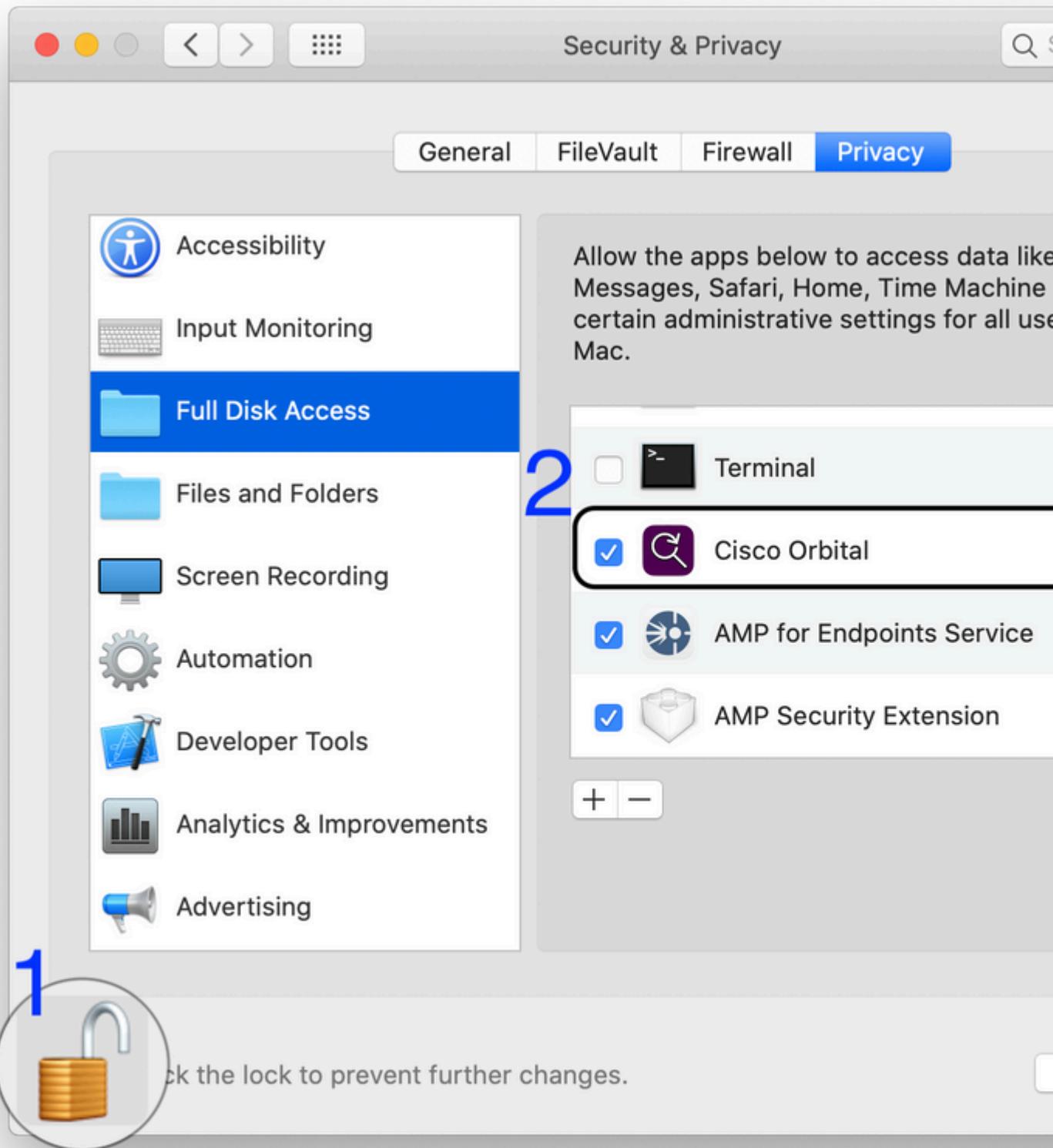
Approbation de l'accès au disque complet pour les versions de connecteur antérieures à 1.18.0 au niveau du terminal

L'accès complet au disque peut être approuvé manuellement à partir du volet des préférences de sécurité et de confidentialité de macOS.



Approbation de l'accès complet au disque pour Cisco Orbital au niveau du terminal

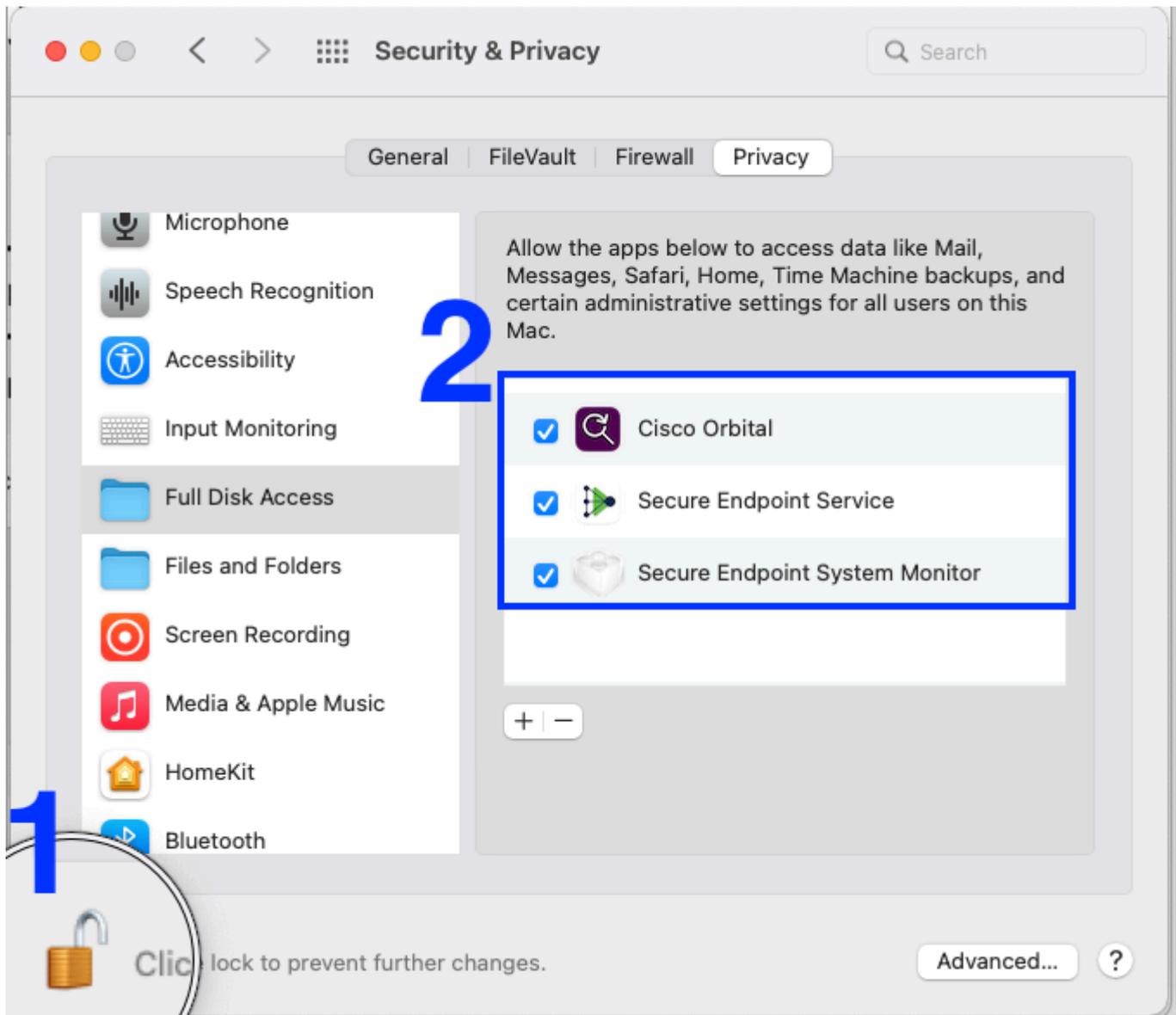
L'accès complet au disque peut être approuvé manuellement à partir du volet des préférences de sécurité et de confidentialité de macOS.



Approbation de l'accès complet au disque pour le connecteur Cisco Secure Endpoint 1.18.0 et versions ultérieures au niveau du terminal

L'accès complet au disque peut être approuvé manuellement à partir du volet des préférences de sécurité et

de confidentialité de macOS.



Approbation de l'accès complet au disque pour le connecteur avec MDM

REMARQUE : les extensions macOS ne peuvent pas être approuvées rétroactivement via MDM. Si le profil MDM n'est pas déployé avant l'installation du connecteur, les approbations ne sont pas accordées et une intervention supplémentaire est requise sous l'une des deux formes suivantes :

1. Approbation manuelle des extensions macOS sur les terminaux dont le profil de gestion a été déployé rétroactivement.
2. Mettez à niveau le connecteur Mac vers une version plus récente que celle actuellement déployée. Les terminaux dont le profil de gestion a été déployé reconnaissent rétroactivement le profil de gestion après la mise à niveau et obtiennent l'approbation une fois la mise à niveau terminée.

L'accès au disque complet peut être approuvé par une charge utile [Contrôle de la politique de préférences de confidentialité du](#) profil de gestion avec une propriété [SystemPolicyAllFiles](#) avec deux entrées, une pour le service de point de terminaison sécurisé (AMP for Endpoints Service pour les versions de connecteur antérieures à 1.18.0) et une pour le Moniteur système de point de terminaison sécurisé (AMP Security Extension pour les versions de connecteur antérieures à 1.18.0) :

Description	Propriété	Valeur
Secure Endpoint Service (AMP for Endpoints Service)	Autorisé	vrai
	CodeRequirement	anchor apple générique et identificateur « com.cisco.endpoint.svc » et (certificat leaf[field.1.2.840.113635.100.6.1.9] /* existe */ ou certificat 1[field.1.2.840.113635.100.6.2.6] /* existe */ et certificat leaf[field.1.2.840.113635.100.6.1.13] /* existe */ et certificat leaf[subject.OU] = DE8Y96K QP)
	Identifiant	com.cisco.endpoint.svc
	IdentifiantType	bundleID
Moniteur système de point d'extrémité sécurisé (AMP Security Extension)	Autorisé	vrai
	CodeRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc.securityextension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* existing */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* existing */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* existing */ and certificate leaf[subject.OU] = 6DE8Y9 K9QP)
	Identifiant	com.cisco.endpoint.svc.securityextension
	IdentifiantType	bundleID

Si votre déploiement inclut des ordinateurs équipés d'un connecteur version 1.12.7 ou antérieure, cette entrée supplémentaire est toujours requise pour accorder un accès complet au disque à ampdaemon pour ces ordinateurs :

Description	Propriété	Valeur
ampdaemon	Autorisé	vrai
	CodeRequirement	identifier ampdaemon et anchor apple générique et certificat 1[field.1.2.840.113635.100.6.2.6] /* existe */ et certificat leaf[field.1.2.840.113635.100.6.1.13] /* existe */ et certificat leaf[subject.OU] = TDNYQP7VRK
	Identifiant	/opt/cisco/amp/ampdaemon
	IdentifiantType	sentier

Approbation de l'accès complet au disque pour Cisco Orbital avec MDM

Si votre déploiement inclut des ordinateurs équipés du connecteur Mac Cisco Secure Endpoint versions 1.16.0 ou ultérieures, sur des ordinateurs équipés de macOS 10.15 ou ultérieures, et si Orbital est activé dans la stratégie, cette entrée supplémentaire est toujours requise pour accorder un accès disque complet à Orbital pour ces ordinateurs :

Description	Propriété	Valeur
Orbite Cisco	Autorisé	vrai
	CodeRequirement	anchor apple générique et identificateur « com.cisco.endpoint.orbital.app » et (certificat leaf[field.1.2.840.113635.100.6.1.9] /* existing */ ou certificate 1[field.1.2.840.113635.100.6.2.6] /* existing */ et certificat leaf[field.1.2.840.113635.100.6.1.13] /* existing */ et certificat leaf[subject.OU] = DE8Y96K QQU).
	Identifiant	com.cisco.endpoint.orbital.app

Description	Propriété	Valeur
	IdentifieurType	bundleID

Exemple de profil de configuration MDM

Cet exemple de profil de configuration MDM peut être utilisé comme référence.

- Approbation des extensions système pour le connecteur Mac Secure Endpoint.
- Accorde un accès complet au disque pour le connecteur Mac Secure Endpoint et Orbital.
- Permet la désinstallation silencieuse des extensions système lorsque le connecteur est désinstallé.
REMARQUE : lorsque l'autorisation RemovableSystemExtensions est autorisée, tout utilisateur ou processus disposant de privilèges racine peut supprimer l'extension système sans être invité à saisir le mot de passe utilisateur. Ainsi, la propriété RemovableSystemExtensions ne doit être utilisée que lorsque l'administrateur souhaite automatiser la désinstallation du connecteur.

<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

Exemple de configuration MDM pour macOS 10.15 ou version antérieure

- L'approbation des extensions du noyau et accorde un accès complet au disque pour les connecteurs.
 - REMARQUE : Les produits M1 et les produits Apple plus récents ne peuvent pas utiliser de profils contenant cette configuration

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

Nouvelle structure de répertoires

Versions 1.14.0 à 1.16.2

Le connecteur Mac 1.14 apporte deux modifications à la structure des répertoires :

1. Le répertoire Applications a été renommé de Cisco AMP en Cisco AMP for Endpoints.
2. L'utilitaire de ligne de commande ampcli a été déplacé de /opt/cisco/amp vers /Applications/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS. Le répertoire /opt/cisco/amp contient un lien symbolique vers le programme ampcli à son nouvel emplacement.

La structure de répertoires complète pour les versions 1.14.0 à 1.16.2 du connecteur Mac est la suivante :

```
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 et ultérieures

Le connecteur Mac 1.18 introduit une modification dans la structure de répertoires des applications :

1. Le répertoire Applications a été renommé Cisco AMP for Endpoints en Cisco Secure Endpoint.

La structure de répertoires complète pour les versions 1.18.0 et ultérieures du connecteur Mac est la suivante :

```
Applications
├── Cisco Secure Endpoint
│   ├── Secure Endpoint Connector.app
│   │   ├── Contents
│   │   └── MacOS
│   └── Secure Endpoint Service.app
│       ├── Contents
│       └── MacOS
│           ├── ampcli
│           ├── ampdaemon
│           ├── ampscansvc
│           ├── ampcreport
│           ├── ampupdater
│           └── SupportTool
└── Support Tool.app
```

Problèmes connus avec macOS 11.0 et Mac Connector 1.14.1.

- Les indications pour l'erreur 10, « Reboot required to load kernel module or system extension », peuvent être incorrectes si quatre filtres de contenu réseau ou plus sont installés sur l'ordinateur. Référez-vous à l'article [Défauts du connecteur Mac du point d'extrémité sécurisé Cisco](#) pour plus de détails.

Problèmes connus avec macOS 10.15/11.0 et Mac Connector 1.14.0.

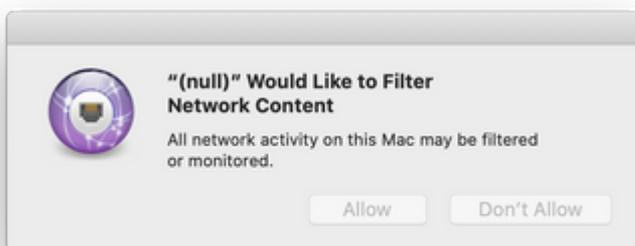
- Certaines défaillances survenues par le connecteur Mac peuvent être survenues de manière inattendue. Référez-vous à l'article [Défauts du connecteur Mac du point d'extrémité sécurisé Cisco](#) pour plus de détails.
 - Fault 13, Too many Network Content Filter system extensions, peut être déclenché après une mise à niveau. Un redémarrage de l'ordinateur résout le problème dans cette situation.
 - Fault 15, System Extension requiert un accès complet au disque, peut être déclenché après le redémarrage en raison d'un bogue dans macOS 11.0.0. Ce problème est corrigé dans macOS 11.0.1. La panne peut être résolue par une nouvelle autorisation d'accès complet au disque dans le volet Security & Privacy des préférences système de macOS.
- Lors de l'installation, le volet Security & Privacy peut afficher « Placeholder Developer » comme nom d'application lorsque macOS demande l'autorisation d'exécuter les extensions du système du connecteur Mac. Ceci est dû à un [bogue dans macOS 10.15](#). Cochez les cases en regard de « Espace réservé au développeur » pour permettre au connecteur Mac de protéger l'ordinateur.



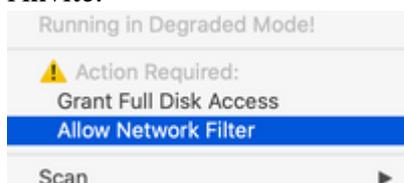
- La commande `systemextensionsctl list` peut être utilisée pour déterminer les extensions du système qui doivent être approuvées. Extensions système avec l'état [activé en attente de l'utilisateur] dans ce résultat sont affichés comme "Développeur d'espace réservé" dans la page de préférences macOS montrée précédemment. Si plus de deux entrées « Espace réservé au développeur » sont affichées dans la page des préférences, désinstallez tous les logiciels qui utilisent des extensions système (y compris le connecteur Mac) de sorte qu'aucune extension système n'ait besoin d'une approbation, puis réinstallez le connecteur Mac.

Les extensions du système de connecteurs Mac sont identifiées comme suit :

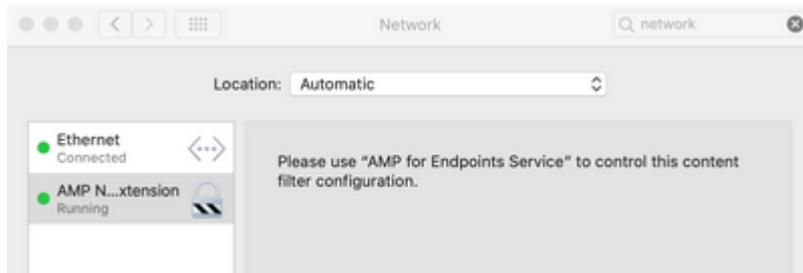
- L'extension réseau est affichée sous la forme `com.cisco.endpoint.svc.networkextension`.
 - L'extension Endpoint Security est affichée avec `com.cisco.endpoint.svc.securityextension`.
- Lors de l'installation, l'invite permettant au filtre de contenu de surveiller le trafic réseau peut afficher « (null) » comme nom d'application. Ceci est causé par un bogue dans macOS 10.15. L'utilisateur doit sélectionner Autoriser pour assurer la protection de l'ordinateur.



- Si l'invite a été rejetée parce que « Ne pas autoriser » a été choisi, sélectionnez « Autoriser le filtre réseau » dans le menu déroulant de l'icône Agent réseau dans la barre de menus pour rouvrir l'invite.



- Une fois activé, le filtre Secure Endpoint Network Extension est répertorié dans la page Network Preferences.



- Sur macOS 11, lorsqu'une mise à niveau du connecteur Mac 1.12 vers le connecteur Mac 1.14 est effectuée, Fault 4, System Extension Failed to Load, peut être levé temporairement pendant que le connecteur passe des extensions du noyau aux nouvelles extensions du système.

Problèmes connus lors de la désinstallation des extensions système

- Avant macOS 12, ou lorsque MDM n'est pas utilisé, lorsqu'une désinstallation du connecteur Mac est effectuée, l'utilisateur est invité à entrer son mot de passe deux fois afin que les extensions système puissent être désinstallées. Il s'agit d'une limitation de macOS et a été quelque peu amélioré dans macOS 12 avec l'ajout de la clé de profil MDM RemovableSystemExtensions décrite dans ce document.

Script d'installation du déploiement Intune

- Un script permettant d'installer le connecteur Secure Endpoint sur macOS géré par Microsoft est hébergé ici :

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

Connecteur Mac renommé (versions 1.18.0 et ultérieures)

REMARQUE : les configurations MDM existantes pour les versions de connecteur antérieures à 1.18.0 fonctionnent sans intervention pour les mises à niveau vers les versions de connecteur 1.18.0 et ultérieures. Voir [Rebranding Mac de point de terminaison sécurisé](#) pour plus d'informations.

Historique de révision

1er déc. 2020

- Le connecteur Mac 1.14.1 n'utilise plus les extensions système sur macOS 10.15.
- Conseils supplémentaires sur la vérification du terminal pour savoir quels extensions système « Espace réservé au développeur » doivent être approuvées avec le connecteur Mac 1.14.0.

9 nov. 2020

- ID d'ensemble corrigé dans le code d'accès complet au disqueExigence de données utiles MDM.

3 nov. 2020

- La date de sortie du connecteur Mac 1.14.0 est novembre 2020.
- Le connecteur Mac 1.14.0 utilise les extensions système avec macOS 10.15.5 et versions ultérieures. Auparavant, il s'agissait de 10.15.6.
- Ajout de la section Problèmes connus
- Structure de répertoire mise à jour.

3 juin 2021

- Ajout d'instructions pour accorder un accès complet au disque pour Cisco Orbital.

13 oct. 2021

- Ajout du retrait des extensions Mac Connector macOS avec la section MDM.
- Ajout de problèmes connus pour la section Désinstallation des extensions système.

25 février 2022

- Rebranding

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.