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

Approuver les extensions Mac Connector macOS

- Approbation des extensions Mac Connector macOS au niveau du terminal
- Approbation des extensions Mac Connector macOS avec MDM

Supprimer les extensions Mac Connector macOS avec MDM

Désactivation de l'extension du système de blocs avec MDM

Accès au disque complet

- Approuver l'accès complet au disque pour les versions de connecteur antérieures à 1.18.0 au niveau du terminal
- Approuver l'accès complet au disque pour Cisco Orbital au niveau du terminal
- Approuver l'accès complet au disque pour le connecteur Cisco Secure Endpoint 1.18.0 et versions ultérieures au niveau du terminal
- Approuver l'accès complet au disque pour le connecteur avec MDM
- Approuver 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 ultérieure

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 requises soient reconnues. Reportez-vous à la section Problèmes connus plus loin dans ce document si MDM n'est pas disponible.

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 introduit la compatibilité avec le 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 de 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 complet au disque

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.

Approuver les 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 du noyau, ampfileop.kext et ampnetworkflow.kext, sont incluses pour assurer la rétrocompatibilité sur les versions macOS plus anciennes 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 version ultérieure.

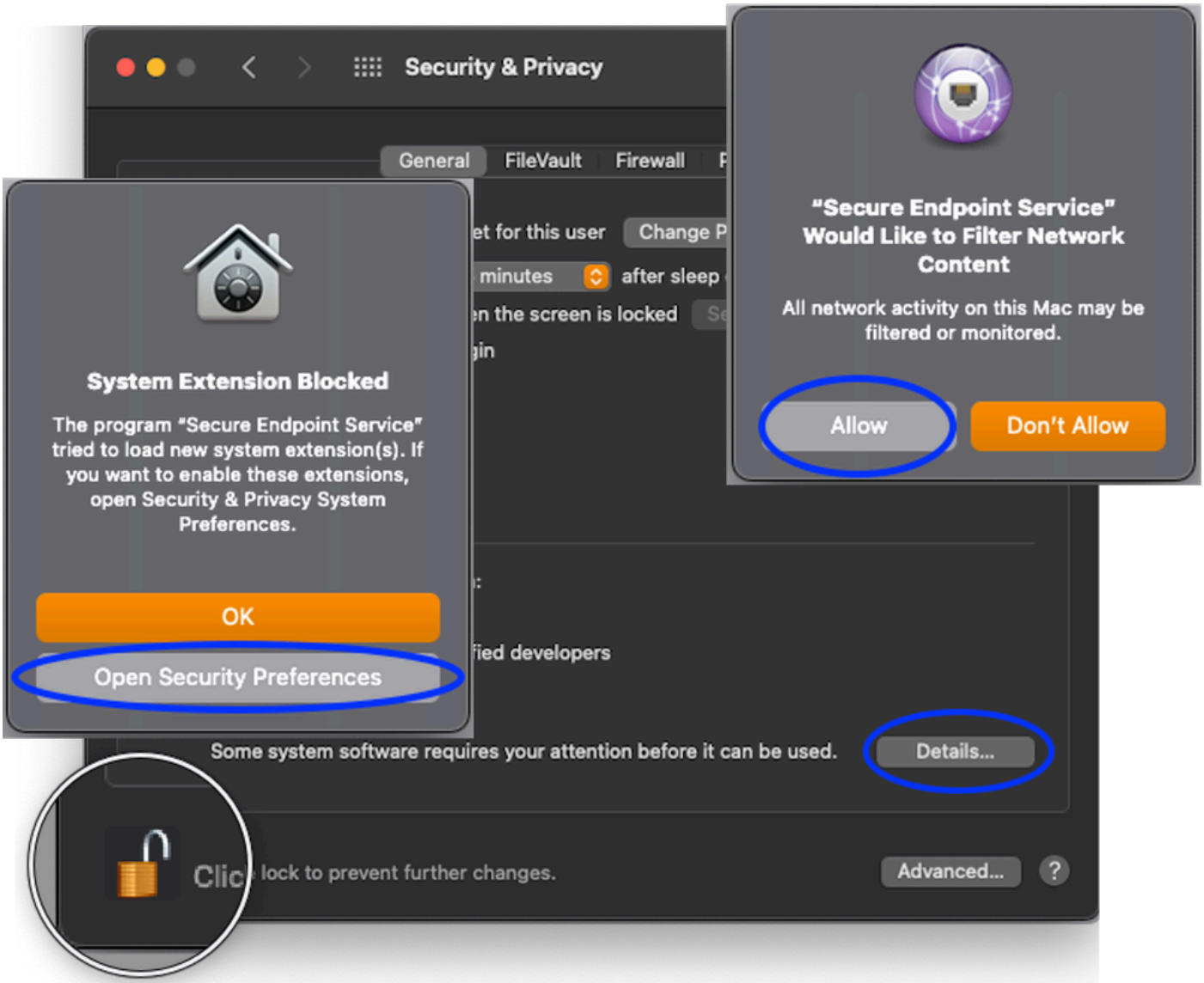
Les approbations requises pour macOS 10.14 et macOS 10.15 :

- Approuver le chargement des extensions de noyau du connecteur

Ces approbations sont 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 sont 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 de l'une des manières 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.securityextension, com.cisco.endpoint.svc.networkextension
Extensions système	TypesExtensionSystèmeAutorisés	ExtensionSécuritéTerminaux, ExtensionRéseau
Extensions système	IdentificateursÉquipeAutorisés	DE8Y96K9QP

Charge Utile	Propriété	Valeur
ExtensionsNoyauPolitiqueSystème	ExtensionsNoyauAutorisées	com.cisco.amp.fileop, com.cisco.amp.nke
ExtensionsNoyauPolitiqueSystème	IdentificateursÉquipeAutorisés	TDNYQP7VRK

Charge Utile	Propriété	Valeur
FiltreContenuWeb	FiltreAutomatiqueActivé	falsifié
FiltreContenuWeb	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.networkextension
FiltreContenuWeb	FilterDataProviderDesignatedRequirement	anchor apple generic and identifier "com.cisco.endpoint.svc.networkextension" 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] = DE8Y96K9QP)
FiltreContenuWeb	CatégorieFiltre	cloison pare-feu
FiltreContenuWeb	FiltrerNavigateurs	falsifié
FiltreContenuWeb	PaquetsFiltres	falsifié
FiltreContenuWeb	FilterSockets	vrai
FiltreContenuWeb	IDbundlePlugin	com.cisco.endpoint.svc
FiltreContenuWeb	NomDéfiniUtilisateur	Cisco Secure Endpoint Filter (AMP Network Extension si la version du connecteur est antérieure à 1.18.0)

Supprimer les 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.

⚠ Mise en garde : Lorsque l'autorisation de suppression d'extension macOS est autorisée, tout utilisateur ou processus disposant de privilèges root 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 la procédure 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 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

Désactivation de l'extension du système de blocs avec MDM

macOS 15 et versions ultérieures autorise les extensions macOS :

- à ne pas supprimer avec la propriété NonRemovableSystemExtensions.
- pour ne pas pouvoir être désactivé dans les paramètres système avec la propriété NonRemovableFromUISystemExtensions

Remarque : Les clés non amovibles doivent être appliquées uniquement aux périphériques macOS Sequoia 15. Ce paramètre de gestion n'est pas appliqué lors de la mise à jour d'anciennes versions de macOS vers macOS Sequoia 15.

Remarque : La clé NonRemovableSystemExtensions ne peut pas être utilisée avec la clé RemovableSystemExtensions ; l'installation du profil échoue.

Remarque : La clé NonRemovableFromUISystemExtensions peut être utilisée avec la clé RemovableSystemExtensions.

Les propriétés non amovibles doivent contenir les identificateurs de bundle des deux extensions Secure Endpoint :

Charge Utile	Propriété	Valeur
Extensions système	ExtensionsSystèmeUISnonAmovibles	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension
	ExtensionsSystèmeNonAmovibles	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 complet au disque dur au programme ampdaemon. 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 :

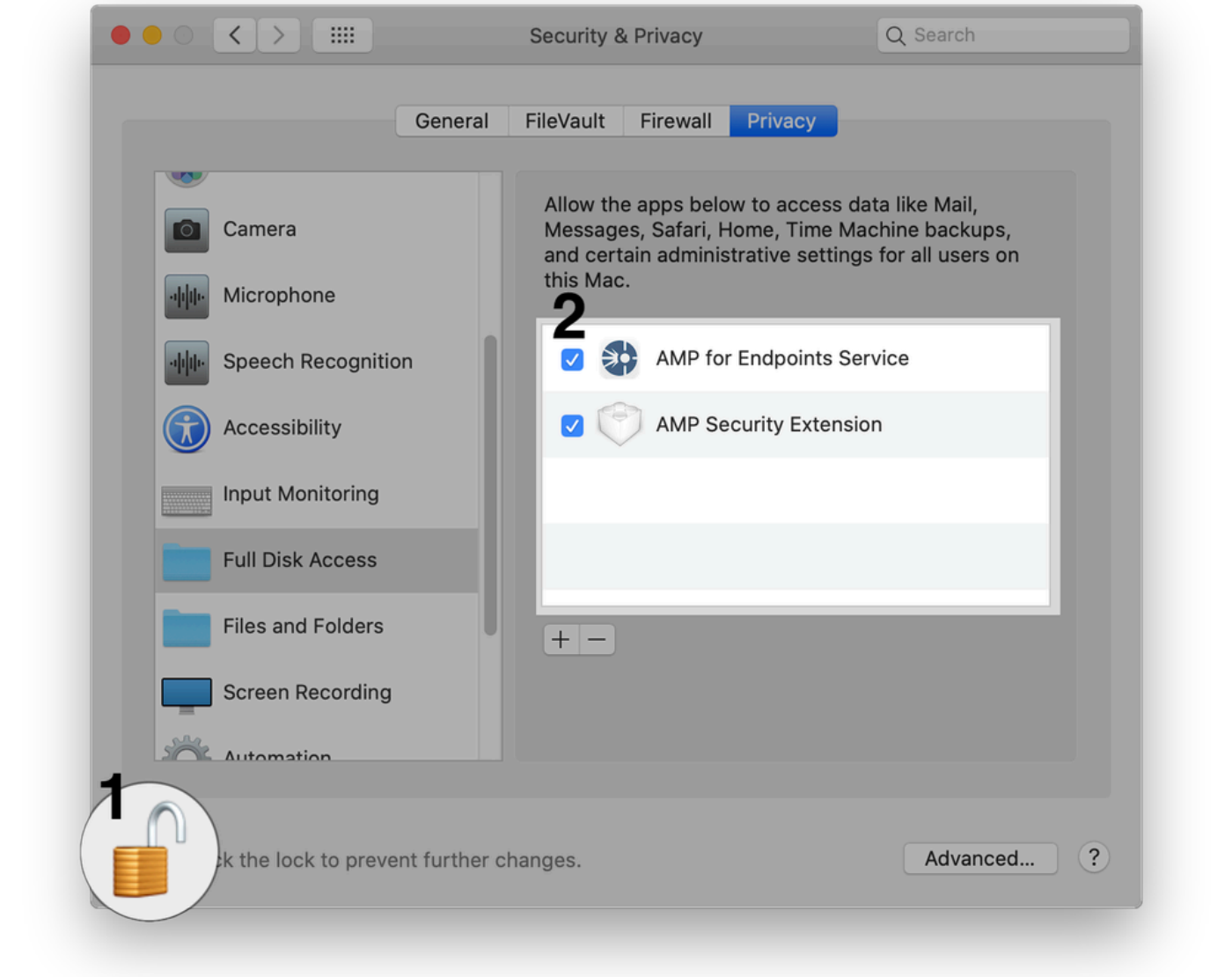
- Secure Endpoint Service
- Secure Endpoint System Monitor
- Cisco Orbital lorsque l'option Orbital est activée dans la stratégie (disponible avec les niveaux Advantage et Premier)

Le programme ampdaemon ne nécessite plus l'accès complet au disque avec le connecteur Mac version 1.14 et ultérieure.

Les autorisations d'accès complet aux disques sont accordées dans les préférences de sécurité et de confidentialité macOS sur le terminal ou par le biais des profils MDM (Mobile Device Management, gestion des appareils mobiles).

Approuver l'accès complet au disque 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.



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

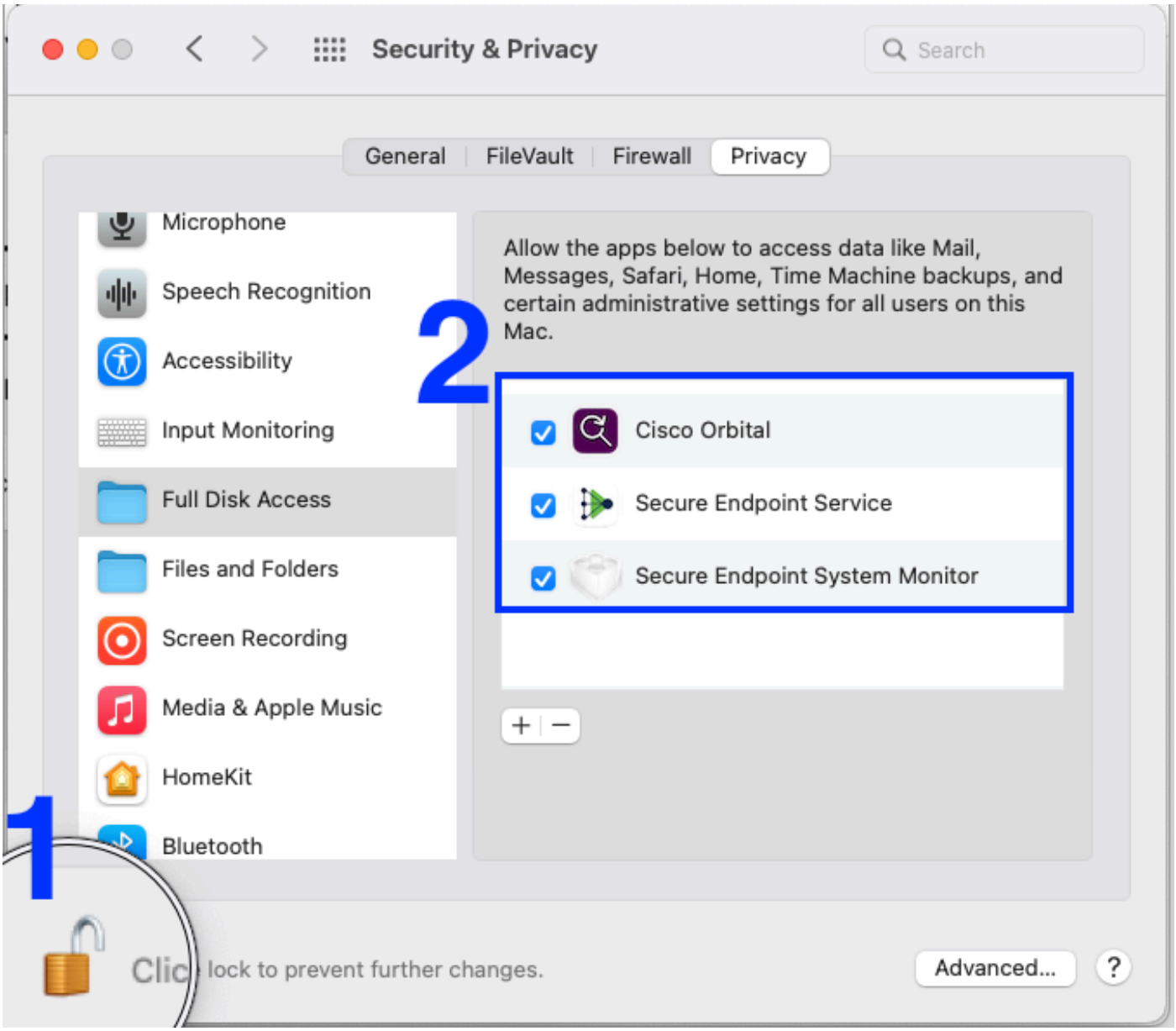
L'accès complet au disque peut être approuvé manuellement à partir du volet des préférences de

sécurité et de confidentialité de macOS.



Approuver 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.



Approuver 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 est 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 de système de point de terminaison sécurisé (AMP Security Extension pour les versions de connecteur antérieures à 1.18.0) :

Charge Utile	Propriété	Valeur
Contrôle de la politique de confidentialité : Secure Endpoint Service (AMP for Endpoints Service)	Autorisé	vrai
Contrôle de la politique de confidentialité : Secure Endpoint Service (AMP for Endpoints Service)	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)
Contrôle de la politique de confidentialité : Secure Endpoint Service (AMP for Endpoints Service)	Identifiant	com.cisco.endpoint.svc
Contrôle de la politique de confidentialité : Secure Endpoint Service (AMP for Endpoints Service)	IdentifierType	bundleID
Contrôle de la politique de confidentialité : Moniteur système de point d'extrémité sécurisé (AMP Security Extension)	Autorisé	vrai
Contrôle de la politique de confidentialité : Moniteur système de point d'extrémité sécurisé (AMP Security Extension)	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] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)

Charge Utile	Propriété	Valeur
Contrôle de la politique de confidentialité : Moniteur système de point d'extrémité sécurisé (AMP Security Extension)	Identifiant	com.cisco.endpoint.svc.securityextension
Contrôle de la politique de confidentialité : Moniteur système de point d'extrémité sécurisé (AMP Security Extension)	IdentifierType	bundleID

Pour les déploiements qui incluent des ordinateurs équipés d'un connecteur version 1.12.7 ou antérieure, cette entrée supplémentaire est requise pour accorder un accès complet au disque à ampdaemon :

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
	IdentifierType	sentier

Approuver 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 :

Charge Utile	Propriété	Valeur
Contrôle de la politique de confidentialité : Orbite Cisco	Autorisé	vrai
Contrôle de la politique de confidentialité : Orbite Cisco	CodeRequirement	anchor apple générique et identificateur "com.cisco.endpoint.orbital.app" 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

Charge Utile	Propriété	Valeur
		leaf[subject.OU] = DE8Y96K9QP)
Contrôle de la politique de confidentialité : Orbite Cisco	Identifiant	com.cisco.endpoint.orbital.app
Contrôle de la politique de confidentialité : Orbite Cisco	IdentifierType	bundleID

Exemple de profil de configuration MDM

Cet exemple de profil de configuration MDM sert de 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.

⚠ Mise en garde : 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.

```
<?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 (certi
                    <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
                    <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" an
                    <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 (
        <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>
```

Exemple de configuration MDM pour macOS 10.15 ou version ultérieure

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

Nouvelle structure de répertoires

Versions 1.14.0 à 1.16.2

Le connecteur Mac 1.14 apporte deux modifications à la structure du répertoire :

1. Le répertoire Applications a été renommé Cisco AMP en Cisco AMP for Endpoints.
2. L'utilitaire ampcli de l'interface de ligne de commande (CLI) 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 :

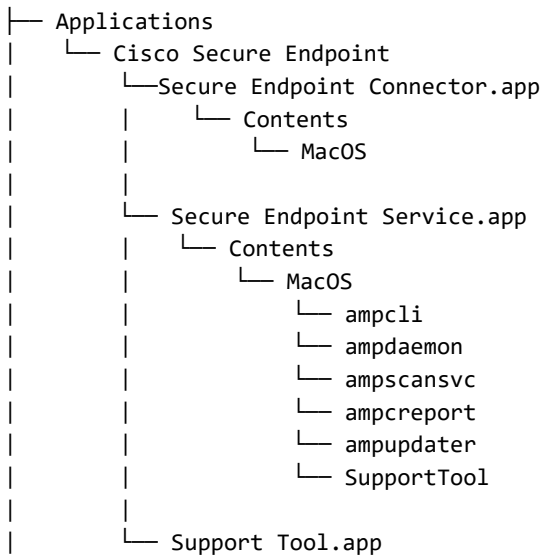
```
├── Applications
│   └── Cisco AMP for Endpoints
│       └── AMP for Endpoints Connector.app
│       │   └── Contents
│       │       └──MacOS
│       │
│       └── AMP for Endpoints Service.app
│       │   └── Contents
│       │       └──MacOS
│       │           └── ampcli
│       │           └── ampdaemon
│       │           └── amscansvc
│       │           └── ampcreport
│       │           └── ampupdater
│       │           └── SupportTool
│       │
│       └── Support Tool.app
├── Library
│   ├── Application Support
│   │   └── Cisco
│   │       └── AMP for Endpoints Connector
│   │           └── SupportTool
│   └── Logs
│       └── Cisco
├── Users
│   └── *
│       └── Library
│           └── Logs
│               └── Cisco
└── opt
    └── cisco
        └── amp
            └── 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 :



Problèmes connus avec macOS 11.0 et Mac Connector 1.14.1.

- Les indications pour l'erreur 10, Redémarrage requis pour charger le module du noyau ou l'extension du système, peuvent être incorrectes si quatre filtres de contenu réseau ou plus sont installés sur l'ordinateur. Reportez-vous à l'article Cisco Secure Endpoint Mac Connector Faults pour plus de détails.

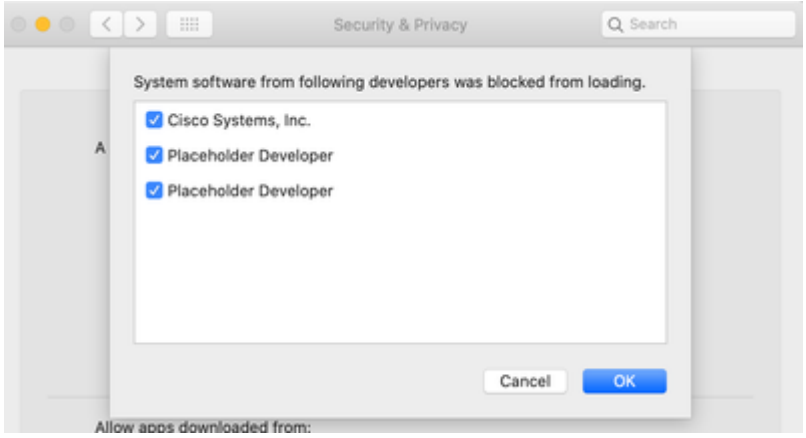
Problèmes connus avec macOS 10.15/11.0 et Mac Connector 1.14.0.

- 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.

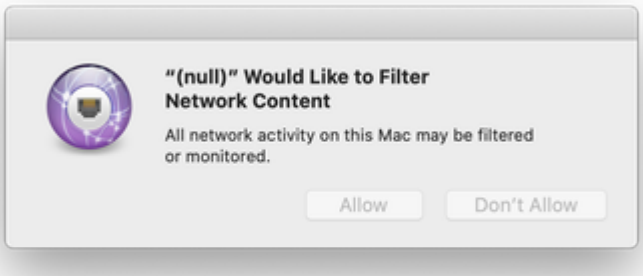
- Fault 15, System Extension require Full Disk Access, peut être déclenché après le redémarrage en raison d'un bogue dans macOS 11.0.0. Ce problème est résolu dans macOS 11.0.1. Le problème peut être résolu par une nouvelle autorisation d'accès complet au disque dans le volet Security & Privacy dans les préférences système de macOS.

- Pendant l'installation, le volet Sécurité et confidentialité peut afficher Espace réservé Développeur comme nom d'application lorsque macOS demande l'autorisation d'exécuter les extensions du système de connecteur Mac. Ceci est dû à un bogue dans macOS 10.15. Cochez les cases en regard de « Espace réservé Développeur » pour permettre au connecteur Mac de protéger l'ordinateur.

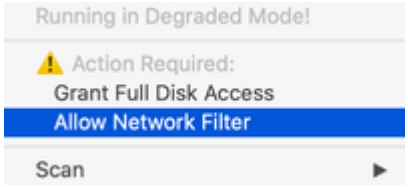


  - La commande systemextensionsctl list peut être utilisée pour déterminer les extensions système qui doivent être approuvées. Les extensions système avec l'état [activé en attente d'utilisateur] dans cette sortie sont affichées comme "Développeur d'espace réservé" dans la page de préférences macOS montrée précédemment. Si plus de deux entrées Espace réservé pour 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 présentée sous la forme com.cisco.endpoint.svc.networkextension.
    - L'extension Endpoint Security affiche com.cisco.endpoint.svc.securityextension.

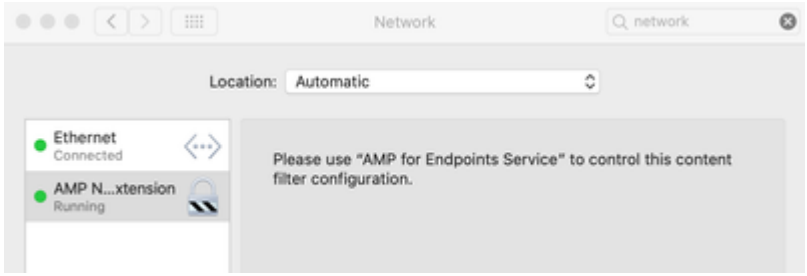
- Pendant l'installation, l'invite permettant au filtre de contenu de surveiller le trafic réseau peut afficher (null) comme nom d'application. Ceci est causé par un bogue dans macOS 10.15. L'utilisateur doit sélectionner Allow to pour assurer la protection de l'ordinateur.



- 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  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 qui installe le connecteur Secure Endpoint sur macOS géré par Microsoft est hébergé ici :

Script d'installation du connecteur Mac Cisco AMP pour terminaux

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.