Configurar permisos para el conector Mac de terminal seguro y orbital con MDM: acceso de disco completo, extensiones del sistema

Contenido

Introducción

Este documento describe los cambios recientes y los pasos para que los administradores implementen el conector Mac 1.14 y posterior.

Perfiles de MDM

Se recomienda encarecidamente implementar el conector Mac con un perfil de MDM que otorgue las aprobaciones necesarias. Los perfiles de MDM deben instalarse antes de la instalación, actualización o eliminación del conector Mac para garantizar que se reconocen los permisos necesarios. Consulte la sección Problemas conocidos más adelante en este documento si no se puede utilizar MDM.

Recomendaciones

La versión 1.14 del conector Mac introdujo cambios que requieren atención:

- Aprobación de acceso completo al disco
- Aprobación de extensión del sistema

Se necesita el conector Mac 1.14 o posterior para garantizar la protección de los terminales en macOS 11 y versiones posteriores. Los conectores Mac antiguos no funcionan en estas versiones de macOS.

La versión 1.16 del conector Mac introdujo el soporte para Cisco Orbital en el hardware Intel. Orbital se puede habilitar en políticas con el nivel Advantage o Premier y se instala automáticamente cuando se habilita e instala en una versión de sistema operativo compatible y hardware compatible. La versión 1.20 del conector para Mac introduce la preparación para la compatibilidad con Cisco Orbital en el hardware de silicio de Apple, cuya versión se prevé para el lanzamiento con Orbital Node 1.21. Consulte las secciones de Cisco Orbital de este documento para obtener detalles sobre cómo otorgar los permisos de acceso completo al disco adicionales necesarios para Orbital.

Requisitos mínimos del SO

Cisco Secure Endpoint Conector Mac 1.14.0 es compatible con las versiones de macOS:

- macOS 11, con extensiones de sistema macOS.
- macOS 10.15.5 y posterior, con extensiones de sistema macOS.
- macOS 10.15.0 a macOS 10.15.4, con extensiones de kernel macOS.
- macOS 10.14, con extensiones de kernel macOS.

Cisco Secure Endpoint Conector Mac 1.14.1 es compatible con las versiones de macOS:

- macOS 11, con extensiones de sistema macOS.
- macOS 10.15 con extensiones de kernel macOS.
- macOS 10.14, con extensiones de kernel macOS.

La compatibilidad con Cisco Orbital en el hardware Intel se introdujo en la versión 1.16.0 del conector Secure Endpoint para Mac. La compatibilidad con Cisco Orbital en el hardware de silicio de Apple se introdujo en la versión 1.20.0 del conector Secure Endpoint para Mac.

Consulte la Tabla de compatibilidad del sistema operativo para obtener información sobre la compatibilidad actual del conector Mac.

Cambios importantes

El conector Mac 1.14 introdujo cambios importantes en tres áreas:

1. Aprobación de las extensiones macOS utilizadas por el conector
2. Acceso a disco completo
3. Nueva estructura de directorios

MacOS 12 introdujo una opción de MDM para permitir la eliminación de las extensiones macOS del conector sin una petición de contraseñas de usuario.

Aprobación de Mac Connector macOS Extensions

El conector Mac utiliza Extensiones del sistema o Extensiones del núcleo heredadas para supervisar las actividades del sistema, según sea necesario para la versión de macOS. En macOS 11, Extensiones del sistema reemplaza las Extensiones del núcleo heredadas que no son compatibles con macOS 11 y versiones posteriores. Se requiere la aprobación del usuario en todas las versiones de macOS antes de permitir la ejecución de cualquier tipo de extensión. Sin aprobación, algunas funciones del conector, como el análisis de archivos en tiempo real y el monitor de acceso a la red, no están disponibles.

Mac connector 1.14 introduce dos nuevas extensiones del sistema macOS:

1. Una extensión de Endpoint Security, denominada Secure Endpoint File Monitor (anteriormente AMP Security Extension), para supervisar los eventos del sistema
2. Una extensión de filtro de contenido de red, denominada Cisco Secure Endpoint Filter (anteriormente AMP Network Extension), para supervisar el acceso a la red

Las dos extensiones de núcleo heredadas, `ampfileop.kext` y `ampnetworkflow.kext`, se incluyen para compatibilidad con versiones anteriores de macOS que no admiten las nuevas extensiones de sistema macOS.

Las aprobaciones requeridas para macOS 11** y versiones posteriores:

- Aprobar Secure Endpoint File Monitor para cargar
- Aprobar Cisco Secure Endpoint Filter para cargar
- Permitir que Cisco Secure Endpoint Filter filtre el contenido de la red

** La versión 1.14.0 del conector Mac también requería estas aprobaciones en macOS 10.15. Estas aprobaciones ya no son necesarias en macOS 10.15 para el conector Mac 1.14.1 o posterior.

Las aprobaciones requeridas para macOS 10.14 y macOS 10.15:

- Aprobar extensiones de núcleo de conector para cargar

Estas aprobaciones se pueden conceder en las preferencias de privacidad y seguridad de macOS en el terminal o a través de los perfiles de gestión de dispositivos móviles (MDM).

Aprobación de Mac Connector macOS Extensions en el terminal

Las extensiones del sistema y del núcleo se pueden aprobar manualmente desde el panel Preferencias de privacidad y seguridad de macOS.

Aprobación de Mac Connector macOS Extensions with MDM

NOTA: Las extensiones macOS no pueden aprobarse retroactivamente mediante MDM. Si el perfil de MDM no se implementa antes de la instalación del conector, no se conceden las aprobaciones y se requiere una intervención adicional de una de estas dos formas:

1. Aprobación manual de las extensiones macOS en los terminales que tenían el perfil de administración implementado retroactivamente.
2. Actualice el conector Mac a una versión más reciente que la implementada actualmente. Los terminales que tenían implementado el perfil de administración de forma retroactiva reconocen el perfil de administración después de una actualización y obtienen la aprobación

una vez que se completa la actualización.

Las extensiones de terminales seguros se pueden aprobar con un perfil de gestión con estas cargas útiles y propiedades:

Carga útil	Propiedad	Valor
ExtensionesDelSistema	ExtensionesSistemaPermitidas	com.cisco.enc com.cisco.enc
	TiposDeExtensiónDelSistemaPermitido	EndpointSecu NetworkExten
	IdentificadoresDeEquipoPermitido	DE8Y96K9QP
ExtensionesNúcleoDeDirectivaDelSistema	ExtensionesNúcleoPermitido	com.cisco.am
	IdentificadoresDeEquipoPermitido	TDNYQP7VR
FiltroContenidoWeb	AutofiltroActivado	falso
	IdentificadorAgrupamientoProveedorDatosFiltro	com.cisco.enc
	FilterDataProviderDesignatedRequirement	delimitador de identificador "com.cisco.en y (certificate le [field.1.2.840. o certificate 1[field.1.2.840 */ y certificate [field.1.2.840. */ y certificate DE8Y96K9QP
	GradoFiltro	firewall
	FilterBrowsers	falso
	FilterPackets	falso
	FilterSockets	verdadero
	PluginBundleID	com.cisco.enc
	NombreDefinidoPorUsuario	Cisco Secure red AMP si la anterior a la 1

Eliminación de Mac Connector macOS Extensions con MDM

MacOS 12 y posteriores permiten que las extensiones macOS se marquen como extraíbles con la propiedad RemovableSystemExtensions, tal como se describe a continuación.
NOTA: Cuando se permite el permiso extraíble Extensión macOS, cualquier usuario o proceso con privilegios de root tiene la capacidad de quitar la extensión sin solicitar la contraseña de usuario. Por tanto, la propiedad RemovableSystemExtensions sólo se debe utilizar cuando el administrador desea automatizar la desinstalación del conector.
NOTA: Las extensiones macOS no se pueden eliminar retroactivamente mediante MDM. Si el

perfil MDM no se implementa antes de desinstalar el conector, no se concede la aprobación de eliminación de extensiones macOS y el usuario debe introducir manualmente una contraseña en el terminal durante el proceso de desinstalación del conector para quitar las extensiones macOS.

Las extensiones de Secure Endpoint se pueden quitar como parte de la desinstalación del conector si se instala un perfil de administración con la propiedad RemovableSystemExtensions agregada a la carga de Extensiones del sistema. La propiedad RemovableSystemExtensions debe contener los identificadores de conjunto de ambas extensiones de punto final seguro:

Carga útil	Propiedad	Valor
ExtensionesDelSistema	ExtensionesDelSistemaExtraíbles	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Bloqueo de la desactivación de extensión del sistema con MDM

MacOS 15 y posterior permite extensiones macOS:

- no se puede quitar con la propiedad NonRemovableSystemExtensions.
- para no poder deshabilitarse en Configuración del sistema con la propiedad NonRemovableFromUISystemExtensions

NOTA: Las claves no extraíbles solo se deben aplicar a los dispositivos macOS Sequoia 15. Esta configuración de administración no se aplicará cuando se actualicen versiones antiguas de macOS a macOS Sequoia 15.
NOTA: La clave NonRemovableSystemExtensions no se puede utilizar con la clave RemovableSystemExtensions; la instalación del perfil fallará.

NOTA: La clave NonRemovableFromUISystemExtensions se puede utilizar con la clave RemovableSystemExtensions.

Las propiedades no extraíbles deben contener los identificadores de conjunto de ambas extensiones de Secure Endpoint:

Carga útil	Propiedad	Valor
ExtensionesDelSistema	ExtensionesDeSistemaUISnoExtraíbles	com.cisco.endpoint.svc.securityextensior com.cisco.endpoint.svc.networkextensior
	ExtensionesSistemaNoExtraíbles	com.cisco.endpoint.svc.securityextensior com.cisco.endpoint.svc.networkextensior

Acceso a disco completo

MacOS 10.14 y versiones posteriores requieren aprobación antes de que una aplicación pueda acceder a partes del sistema de archivos que contienen datos personales del usuario (por ejemplo, Contactos, Fotos, Calendario y otras aplicaciones). Ciertas funciones del conector, como el análisis de archivos en tiempo real, no pueden analizar estos archivos en busca de amenazas sin aprobación.

Las versiones anteriores del conector Mac requerían que el usuario concediera acceso de disco completo al programa `ampdaemon`. El conector Mac 1.14 requiere acceso de disco completo para:

- "Servicio de AMP para terminales"
- "Extensión de seguridad de AMP"

El conector Mac 1.16.0 y las versiones más recientes requieren acceso de disco completo adicional para:

- "Cisco Orbital" cuando está habilitado en la política, disponible con Advantage y acceso Premier

El conector Mac 1.18 y las versiones posteriores requieren acceso de disco completo para:

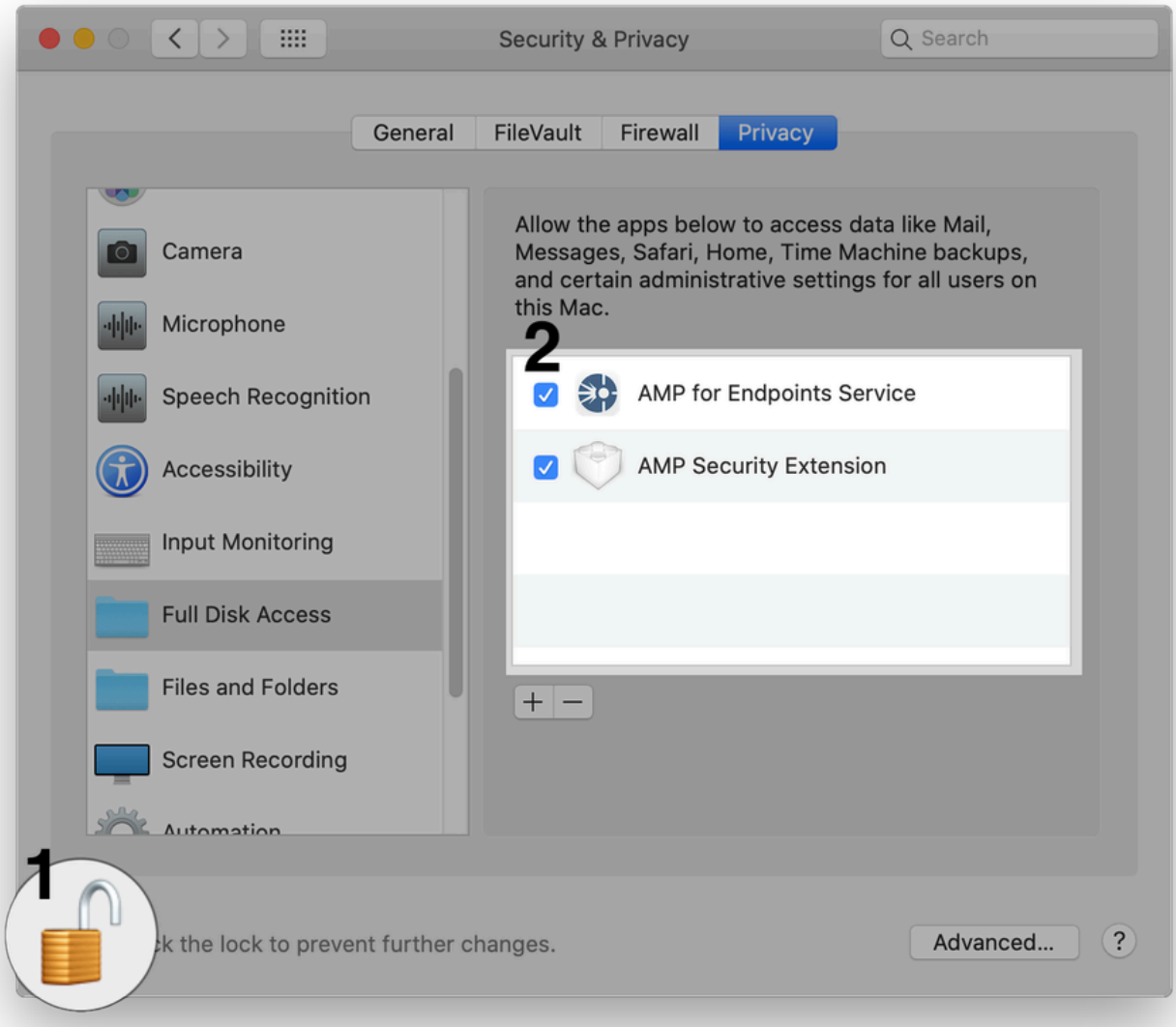
- "Servicio de terminal seguro"
- "Monitor de sistema de terminales seguros"
- "Cisco Orbital" cuando Orbital está habilitado en la política (disponible con los niveles Advantage y Premier)

El programa `ampdaemon` ya no requiere acceso de disco completo con conector Mac versión 1.14 y posterior.

Las aprobaciones de Full Disk Access se pueden conceder en las preferencias de privacidad y seguridad de macOS en el terminal o a través de los perfiles de gestión de dispositivos móviles (MDM).

Aprobación de Full Disk Access para versiones de conector anteriores a la 1.18.0 en el terminal

El acceso a disco completo se puede aprobar manualmente desde el panel de preferencias de privacidad y seguridad de macOS.

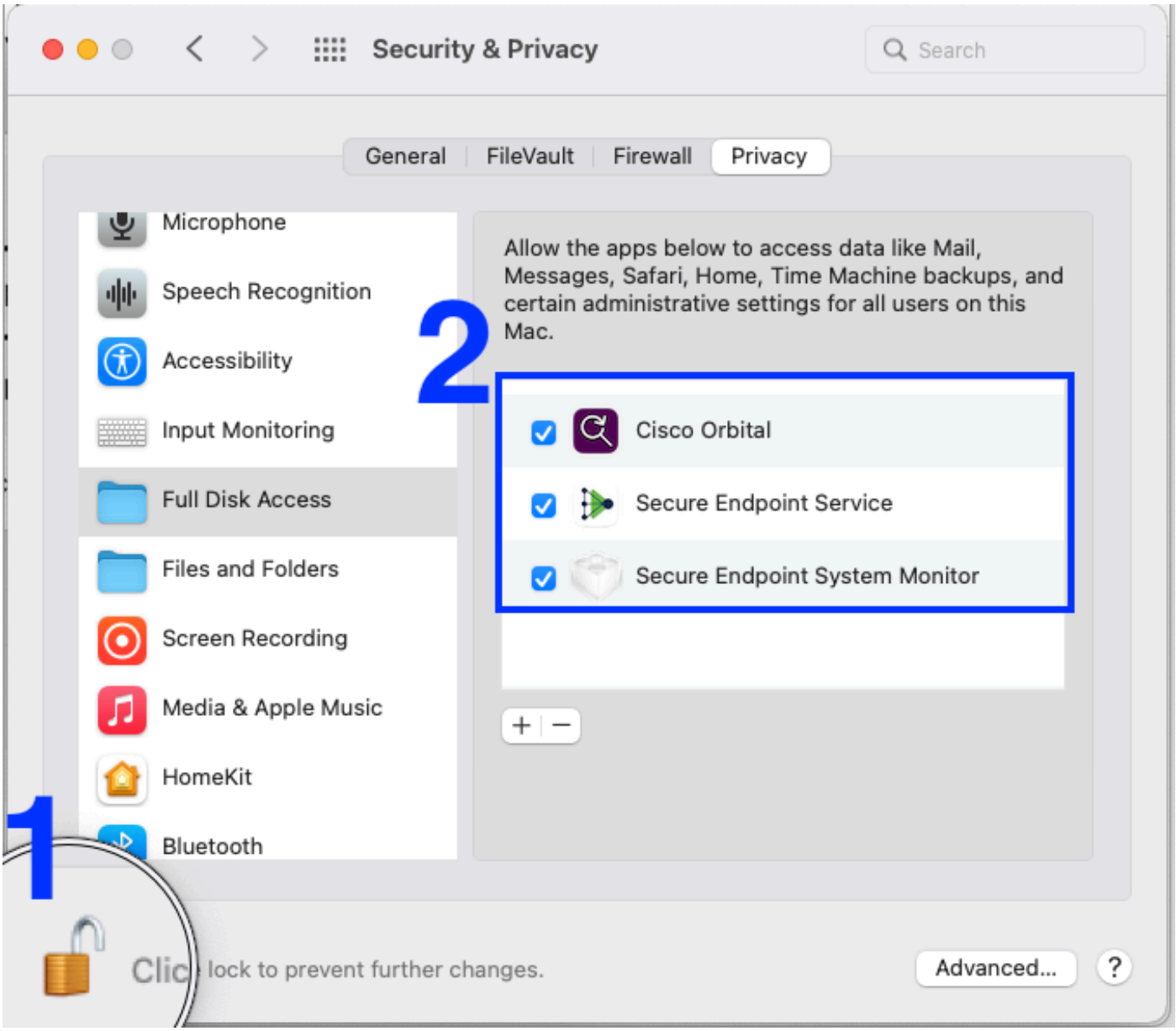


Aprobación del acceso a disco completo para Cisco Orbital en el terminal

El acceso a disco completo se puede aprobar manualmente desde el panel de preferencias de privacidad y seguridad de macOS.

Aprobación del acceso a disco completo para Cisco Secure Endpoint Connector 1.18.0 y versiones más recientes en el terminal

El acceso a disco completo se puede aprobar manualmente desde el panel de preferencias de privacidad y seguridad de macOS.



Aprobación del acceso a disco completo para el conector con MDM

NOTA: Las extensiones macOS no pueden aprobarse retroactivamente mediante MDM. Si el perfil de MDM no se implementa antes de la instalación del conector, no se conceden las aprobaciones y se requiere una intervención adicional de una de estas dos formas:

1. Aprobación manual de las extensiones macOS en los terminales que tenían el perfil de administración implementado retroactivamente.
2. Actualice el conector Mac a una versión más reciente que la implementada actualmente. Los terminales que tenían el perfil de gestión implementado de forma retroactiva reconocen el perfil de gestión después de la actualización y obtienen la aprobación una vez que se completa la actualización.

El acceso a disco completo se puede aprobar mediante un perfil de administración Preferencias de privacidad Control de políticas con una propiedad SystemPolicyAllFiles con dos entradas, una para `Secure Endpoint Service (AMP para terminales Service para las versiones de conector anteriores a la 1.18.0)` y otra para `Secure Endpoint System Monitor (AMP Security Extension para`

las versiones de conector anteriores a la 1.18.0):

Descripción	Propiedad	Valor
Servicio de terminales seguros (servicio AMP para terminales)	PERMITIDO	verdadero
	CódigoRequisito	delimitador de manzana genérico e identificador "com.cisco.endpoint.svc" y (hoja de certificado [field.1.2.840.113635.100.6.1.9] /* existe */ o certificado 1[field.1.2.840.113635.100.6.2.6] /* existe */ y hoja de certificado [field.1.2.840.113635.100.6.1.13] /* existe */ y hoja de certificado [subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.svc
	TipoDeIdentificador	bundleID
Monitor de sistema de terminales seguros (AMP Security Extension)	PERMITIDO	verdadero
	CódigoRequisito	delimitador de manzana genérico e identificador "com.cisco.endpoint.svc.securityextension" y (hoja de certificado [field.1.2.840.113635.100.6.1.9] /* existe */ o certificado 1[field.1.2.840.113635.100.6.2.6] /* existe */ y hoja de certificado [field.1.2.840.113635.100.6.1.13] /* existe */ y hoja de certificado [subject OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.svc.securityextension
	TipoDeIdentificador	bundleID

Si la implementación incluye equipos con el conector versión 1.12.7 o posterior instalado, esta entrada adicional sigue siendo necesaria para conceder acceso completo al disco a `ampdaemon` para esos equipos:

Descripción	Propiedad	Valor
ampdaemon	PERMITIDO	verdadero
	CódigoRequisito	identificador ampdaemon y delimitador apple generic y certificado 1[field.1.2.840.113635.100.6.2.6] /* exists */ y certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ y certificate leaf[subject.OU] = TDNYQP7VRK
	Identifier	/opt/cisco/amp/ampdaemon
	TipoDeIdentificador	ruta

Aprobación del acceso a disco completo para Cisco Orbital con MDM

Si su implementación incluye equipos con Cisco Secure Endpoint Mac connector versiones 1.16.0 o posterior, en equipos con macOS 10.15 o posterior, y Orbital está habilitado en la directiva, esta entrada adicional sigue siendo necesaria para conceder acceso completo de disco a Orbital para esos equipos:

Descripción	Propiedad	Valor
Cisco Orbital	PERMITIDO	verdadero

Descripción	Propiedad	Valor
	CódigoRequisito	delimitador de manzana genérico e identificador "com.cisco.endpoint.orbital.app" y (hoja de certificado [field.1.2.840.113635.100.6.1.9] /* existe */ o certificado 1[field.1.2.840.113635.100.6.2.6] /* existe */ y hoja de certificado [field.1.2.840.113635.100.6.1.13] /* existe */ y hoja de certificado [subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.orbital.app
	TipoDeIdentificador	bundleID

Ejemplo de perfil de configuración de MDM

Este perfil de configuración de MDM de ejemplo se puede utilizar como referencia.

- Aprobación de extensiones del sistema para el conector Secure Endpoint Mac.
- Otorga acceso completo al disco para el conector Secure Endpoint Mac y Orbital.
- Permite la desinstalación silenciosa de las extensiones del sistema cuando se desinstala el conector.
  NOTA: Cuando se permite el permiso RemovableSystemExtensions, cualquier usuario o proceso con privilegios raíz tiene la capacidad de quitar la Extensión del sistema sin que se le pida la contraseña de usuario. Por tanto, la propiedad RemovableSystemExtensions sólo se debe utilizar cuando el administrador desea automatizar la desinstalación del conector.

```
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

Ejemplo de configuración de MDM para macOS 10.15 o posterior

- La aprobación de las extensiones del núcleo y concede acceso completo al disco para los conectores.
    - NOTA: M1 y los productos Apple más recientes no pueden utilizar perfiles que contengan esta configuración

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

Nueva estructura de directorios

Versiones 1.14.0 a 1.16.2

El conector Mac 1.14 introduce dos cambios en la estructura de directorios:

1. El nombre del directorio Applications ha cambiado de `Cisco AMP` a `Cisco AMP para terminales`.
2. La utilidad de línea de comandos `ampcli` se ha movido de `/opt/cisco/amp` a `/Applications/Cisco AMP para terminales/AMP para terminales Connector.app/Contents/MacOS`.

El directorio `/opt/cisco/amp` contiene un enlace simbólico al programa `ampcli` en su nueva ubicación.

La estructura de directorios completa para las versiones 1.14.0 a 1.16.2 del conector Mac es la siguiente:

```
├── 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
```

Versiones 1.18.0 y posteriores

El conector Mac 1.18 introduce un cambio en la estructura de directorios de las aplicaciones:

1. El nombre del directorio Applications ha cambiado de `Cisco AMP para terminales` a `Cisco Secure Endpoint`.

La estructura de directorios completa para las versiones 1.18.0 y posteriores del conector Mac es la siguiente:

```
├── 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
```

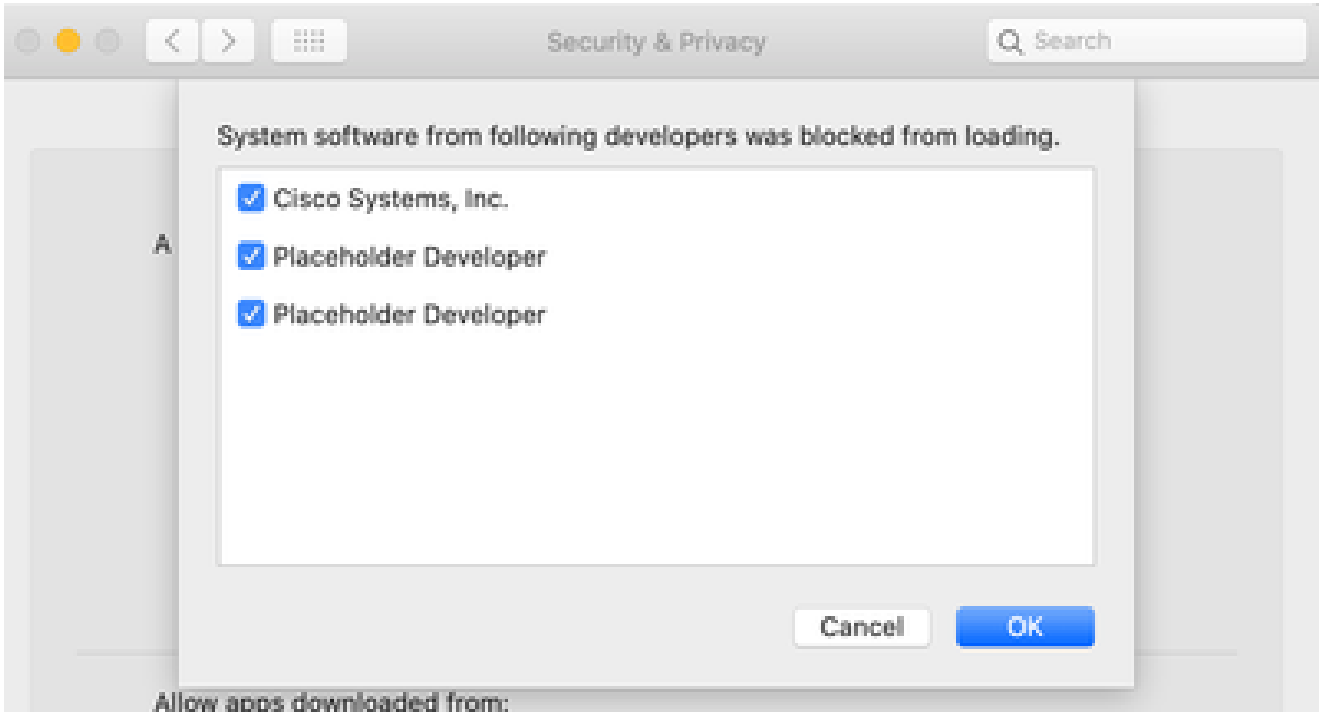
Problemas conocidos con macOS 11.0 y el conector Mac 1.14.1.

- La guía para el fallo 10, "Reboot required to load kernel module or system extension" (Reinicio necesario para cargar el módulo del núcleo o la extensión del sistema), puede ser incorrecta si hay cuatro o más filtros de contenido de red instalados en el equipo. Refiérase al artículo Errores del Conector Mac de Cisco Secure Endpoint para obtener más detalles.

Problemas conocidos con macOS 10.15/11.0 y Mac Connector 1.14.0.

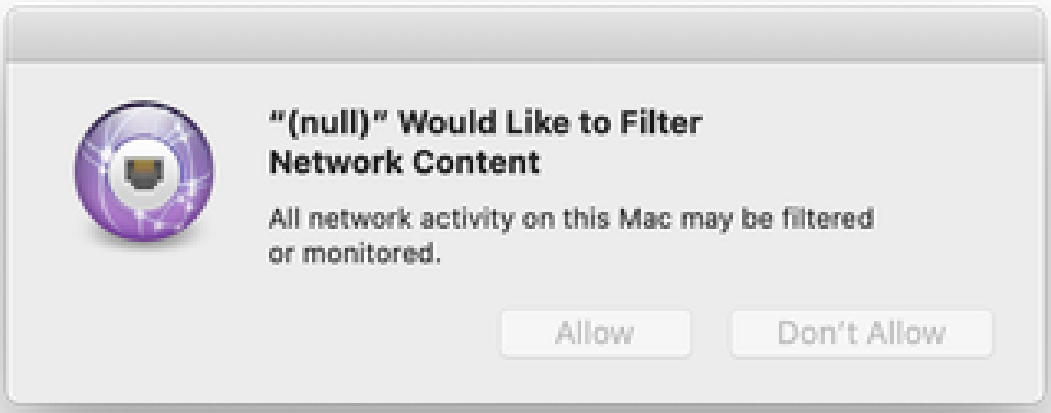
- Algunos fallos provocados por el conector Mac pueden producirse de forma inesperada. Refiérase al artículo Errores del Conector Mac de Cisco Secure Endpoint para obtener más detalles.
    - Fault 13, Too many Network Content Filter system extensions, se puede generar después de una actualización. Un reinicio del equipo resuelve el fallo en esta situación.
    - Fault 15, extensión del sistema requiere acceso completo al disco, puede ser provocado después de reiniciar debido a un error en macOS 11.0.0. Este problema se corrige en macOS 11.0.1. El fallo se puede resolver mediante una reconcesión del acceso completo al disco en el panel Seguridad y privacidad en las preferencias del sistema de macOS.

- Durante la instalación, el panel Seguridad y privacidad puede mostrar "Placeholder Developer" como el nombre de la aplicación cuando macOS solicita permiso para que se ejecuten las extensiones del sistema del conector Mac. Esto se debe a un error en macOS 10.15. Marque las casillas situadas junto a "Placeholder Developer" para permitir que el conector Mac proteja el ordenador.

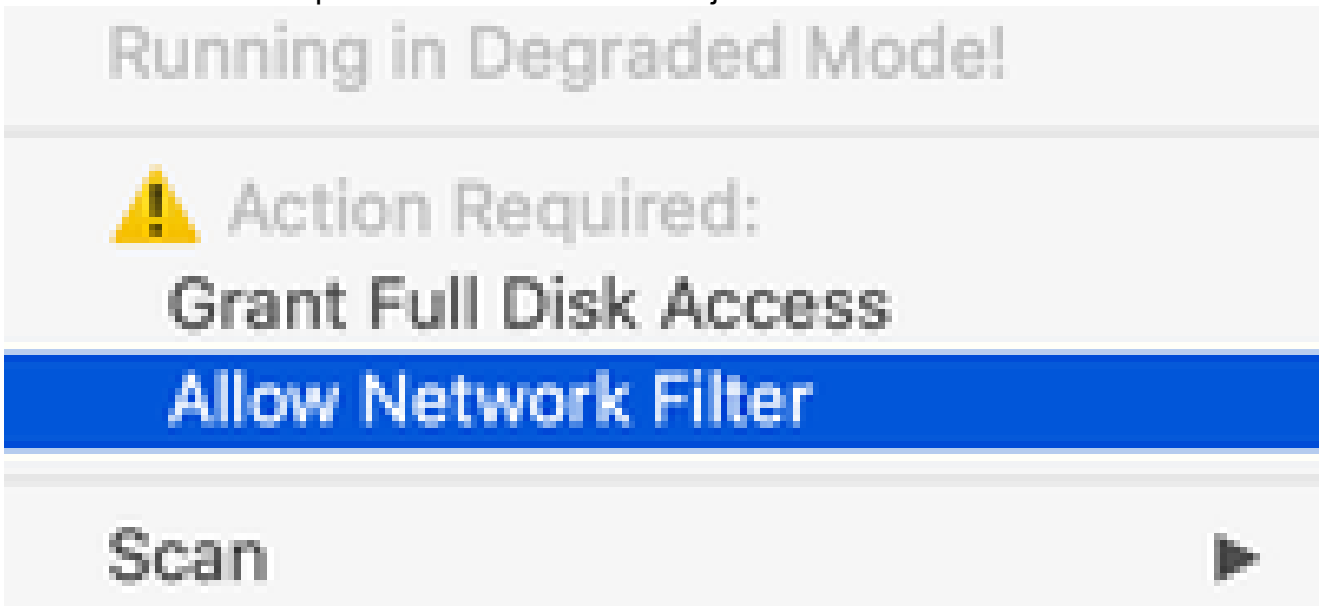


  - El comando `systemextensionsctl` listlist se puede utilizar para determinar qué extensiones del sistema necesitan aprobación. Extensiones del sistema con el estado `[activated waiting for user]` en esta salida se muestra como "Placeholder Developer" en la página de preferencias de macOS mostrada anteriormente. Si se muestran más de dos entradas "Placeholder Developer" en la página de preferencias, desinstale todo el software que utilice extensiones del sistema (incluido el conector Mac) para que ninguna extensión del sistema necesite aprobación y, a continuación, vuelva a instalar el conector Mac.
    Las extensiones del sistema del conector Mac se identifican de la siguiente manera:
    - La extensión de red se muestra como `com.cisco.endpoint.svc.networkextension`.
    - La extensión de Seguridad de terminal se muestra con `com.cisco.endpoint.svc.securityextension`.

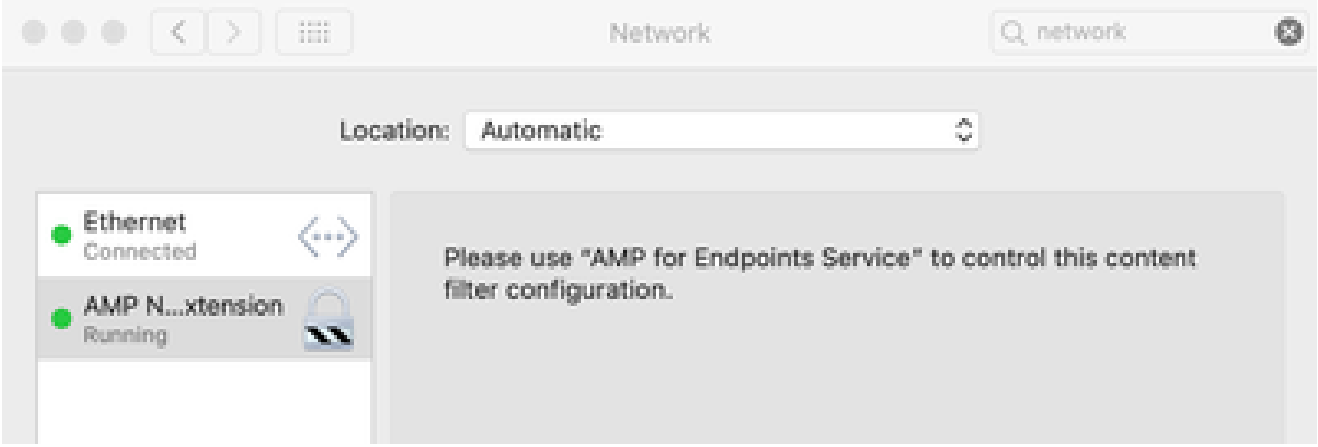
- Durante la instalación, el mensaje para permitir que el filtro de contenido supervise el tráfico de red puede mostrar "(null)" como el nombre de la aplicación. Esto es causado por un bug en macOS 10.15. El usuario debe seleccionar "Permitir" para garantizar la protección del equipo.



- Si se ha descartado el mensaje porque se ha seleccionado "No permitir", seleccione  "Permitir filtro de red" en el menú desplegable del icono Agente en la barra de menús para volver a abrir el mensaje.



- Una vez activado, el filtro Extensión de red de terminal seguro aparece en la página Preferencias de red.



- En macOS 11, cuando se realiza una actualización del conector Mac 1.12 al conector Mac 1.14, Fault 4, System Extension Failed to Load, puede ser elevado temporalmente mientras el conector pasa de las extensiones del núcleo a las nuevas extensiones del sistema.

Problemas conocidos durante la desinstalación de extensiones del sistema

- Antes de macOS 12, o cuando no se utiliza MDM, cuando se realiza una desinstalación del conector Mac, se le pide al usuario que introduzca su contraseña dos veces para que se puedan desinstalar las extensiones del sistema. Esta es una limitación de macOS y se ha mejorado un poco en macOS 12 con la adición de la clave de perfil MDM RemovableSystemExtensions descrita en este documento.

Script de instalación de Intune Deployment

- Una secuencia de comandos que ayudará a instalar Secure Endpoint Connector en macOS mantenido por Microsoft se aloja aquí:

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

Conector Mac rebautizado (versiones 1.18.0 y posteriores)

NOTA: Las configuraciones de MDM existentes para las versiones de conector anteriores a la 1.18.0 funcionan sin intervención para las actualizaciones a las versiones de conector 1.18.0 y posteriores. Consulte Secure Endpoint Mac Rebrand para obtener más información.

Historial de revisión

1 de dic de 2020

- El conector Mac 1.14.1 ya no usa extensiones del sistema en macOS 10.15.
- Guía adicional sobre la verificación de terminal que "Placeholder Developer" Extensiones del sistema necesitan aprobación con el conector Mac 1.14.0.

9 de nov de 2020

- ID de paquete corregido en el código de acceso al disco completoRequisito de carga de MDM.

3 de nov de 2020

- La fecha de lanzamiento del conector 1.14.0 para Mac es noviembre de 2020.
- El conector Mac 1.14.0 utiliza Extensiones del sistema con macOS 10.15.5 y versiones posteriores. Anteriormente era 10.15.6.
- Se ha agregado la sección Problemas conocidos.
- Esquema actualizado de la estructura de directorios.

3 de junio de 2021

- Se han añadido instrucciones para conceder acceso completo al disco para Cisco Orbital.

13 de oct de 2021

- Se ha agregado la sección Eliminación de Mac Connector macOS Extensions con MDM.
- Se agregaron problemas conocidos para la sección Desinstalación de extensiones del sistema.

25 de feb de 2022

- Renombrar

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).