Configurazione delle autorizzazioni per il connettore Mac dell'endpoint protetto e orbitale con MDM: Accesso completo al disco, Estensioni di sistema

Sommario

Introduzione

In questo documento vengono descritte le modifiche recenti e i passaggi per distribuire il connettore Mac 1.14 e versioni successive.

Profili MDM

Si consiglia vivamente di distribuire il connettore Mac con un profilo MDM che conceda le approvazioni necessarie. I profili MDM devono essere installati prima dell'installazione, dell'aggiornamento o della rimozione del connettore Mac per garantire il riconoscimento delle autorizzazioni necessarie. Se non è possibile utilizzare MDM, consultare la sezione Problemi noti più avanti in questo documento.

Consulenze

Mac Connector versione 1.14 ha introdotto modifiche che richiedono attenzione:

- Approvazione completa dell'accesso al disco
- Approvazione estensione di sistema

Per garantire la protezione dell'endpoint su macOS 11 e versioni successive, è necessario il connettore Mac versione 1.14 o successive. I connettori Mac meno recenti non funzionano su queste versioni di macOS.

Il connettore Mac versione 1.16 ha introdotto il supporto per Cisco Orbital su hardware Intel. Orbital può essere abilitato nei criteri con Advantage o Premier Tier e viene installato automaticamente quando abilitato e installato su una versione del sistema operativo e su un hardware supportato. Il connettore Mac versione 1.20 introduce la disponibilità del supporto per Cisco Orbital su hardware in silicio Apple, il cui rilascio è previsto con Orbital Node 1.21. Fare riferimento alle sezioni Cisco Orbital di questo documento per i dettagli su come concedere le ulteriori autorizzazioni di accesso completo al disco necessarie per Orbital.

Requisiti minimi del sistema operativo

Il connettore Cisco Secure Endpoint Mac 1.14.0 supporta le versioni macOS:

- macOS 11, con estensioni macOS.
- macOS 10.15.5 e versioni successive, con estensioni di sistema macOS.
- da macOS 10.15.0 a macOS 10.15.4, con estensioni del kernel macOS.
- macOS 10.14, con estensioni del kernel macOS.

Il connettore Cisco Secure Endpoint Mac 1.14.1 supporta le versioni macOS:

- macOS 11, con estensioni macOS.
- macOS 10.15 con estensioni del kernel macOS.
- macOS 10.14, con estensioni del kernel macOS.

Il supporto per Cisco Orbital su hardware Intel è stato introdotto nel connettore Secure Endpoint per Mac versione 1.16.0. Il supporto per Cisco Orbital su hardware in silicio Apple è stato introdotto nel connettore Secure Endpoint Mac versione 1.20.0.

Consultare la Tabella di compatibilità del sistema operativo per l'attuale compatibilità dei connettori Mac.

Modifiche importanti

Il connettore Mac 1.14 ha introdotto importanti cambiamenti in tre aree:

1. Approvazione delle estensioni macOS utilizzate dal connettore
2. Accesso completo al disco
3. Nuova struttura di directory

MacOS 12 ha introdotto un'opzione MDM per consentire la rimozione delle estensioni macOS del connettore senza richiedere le password utente.

Approvazione delle estensioni di Mac Connector macOS

Il connettore Mac utilizza le estensioni di sistema o le estensioni del kernel legacy per monitorare le attività del sistema, come richiesto dalla versione macOS. In macOS 11, le estensioni di sistema sostituiscono le estensioni del kernel legacy non supportate in macOS 11 e versioni successive. L'approvazione dell'utente è necessaria per tutte le versioni di macOS prima che sia consentita l'esecuzione di entrambi i tipi di estensione. Senza l'approvazione, alcune funzioni dei connettori come la scansione dei file all'accesso e il monitoraggio dell'accesso alla rete non sono disponibili.

Il connettore Mac 1.14 introduce due nuove estensioni di sistema macOS:

1. Un'estensione Endpoint Security, denominata Secure Endpoint File Monitor (in precedenza AMP Security Extension), per monitorare gli eventi di sistema
2. Un'estensione Network Content Filter, denominata Cisco Secure Endpoint Filter (in precedenza AMP Network Extension), per monitorare l'accesso alla rete

Le due estensioni del kernel legacy, `ampfileop.kext` e `ampnetworkflow.kext`, sono incluse per la compatibilità con le versioni precedenti di macOS che non supportano le nuove estensioni di sistema di macOS.

Approvazioni richieste per macOS 11** e versioni successive:

- Approva il caricamento di Secure Endpoint File Monitor
- Approva Cisco Secure Endpoint Filter da caricare
- Consenti a Cisco Secure Endpoint Filter di filtrare il contenuto della rete

** Il connettore Mac versione 1.14.0 richiedeva anche queste approvazioni su macOS 10.15. Queste approvazioni non sono più richieste su macOS 10.15 per il connettore Mac 1.14.1 o versioni successive.

Approvazioni richieste per macOS 10.14 e macOS 10.15:

- Approva estensioni del kernel del connettore da caricare

Queste approvazioni possono essere concesse nelle preferenze di sicurezza e privacy di macOS sull'endpoint o tramite i profili MDM (Mobile Device Management).

Approvazione delle estensioni macOS del connettore Mac sull'endpoint

Le estensioni del sistema e del kernel possono essere approvate manualmente dal riquadro delle preferenze di sicurezza e privacy di macOS.

Approvazione delle estensioni macOS del connettore Mac con MDM

NOTA: le estensioni macOS non possono essere approvate retroattivamente tramite MDM. Se il profilo MDM non viene distribuito prima dell'installazione del connettore, le approvazioni non vengono concesse ed è necessario un ulteriore intervento in uno dei due modi seguenti:

1. Approvazione manuale delle estensioni macOS sugli endpoint con il profilo di gestione distribuito retroattivamente.

2. Aggiornare il connettore Mac a una versione più recente di quella attualmente distribuita. Gli endpoint con il profilo di gestione distribuito in modo retroattivo riconoscono il profilo di gestione dopo un aggiornamento e ottengono l'approvazione una volta completato l'aggiornamento.

Le estensioni degli endpoint sicuri possono essere approvate con un profilo di gestione con i seguenti payload e proprietà:

Payload	Proprietà	Valore
Estensioni di sistema	.AllowedSystemExtensions	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension
	TipiEstensioneSistemaConsentiti	EstensioneSicurezzaEndpoint, EstensioneRete
	IdentificatoriTeamConsentiti	DE8Y96K9QP
EstensioniKernelCriteriSistema	EstensioniKernelConsentite	com.cisco.amp.fileop, com.cisco.amp.nke
	IdentificatoriTeamConsentiti	TDNYQP7VRK
FiltroContenutoWeb	Filtro automatico abilitato	falso
	IdentificatoreBundleProviderDatiFiltro	com.cisco.endpoint.svc.networkextension
	.FiltroDatiProviderDesignatiRequisito	l'identificatore generico e "com.cisco.endpoint.svc.networkextension e (certificato leaf[campo.1.2.840.113635.100.6.1.9] /* esiste */ o il certificato 1[campo.1.2.840.113635.100.6.2.6] /* esiste */ e il certificato leaf[campo.1.2.840.113635.10 6.1.13] /* esiste */ e certificato foglia[subject.OU] = DE8Y96K9QP)
	.LivelloFiltro	firewall
	FiltraBrowser	falso
	FiltraPacchetti	falso
	FiltraSocket	vero
	IDPacchettoPlugin	cisco.endpoint.svc
	NomeDefinitoUtente	Cisco Secure Endpoint Filter (AMP Network Extension se la versione del connettore è precedente alla 1.18.0)

Rimozione delle estensioni macOS del connettore Mac con MDM

MacOS 12 e versioni successive consentono di contrassegnare le estensioni di macOS come rimovibili con la proprietà RemovableSystemExtensions come descritto di seguito.
NOTA: quando è consentita l'autorizzazione rimovibile dell'estensione macOS, qualsiasi utente o processo con privilegi root può rimuovere l'estensione senza richiedere la password utente. Pertanto, la proprietà RemovableSystemExtensions deve essere utilizzata solo quando l'amministratore desidera automatizzare la disinstallazione del connettore.
NOTA: le estensioni macOS non possono essere rimosse retroattivamente tramite MDM. Se il profilo MDM non viene distribuito prima della disinstallazione del connettore, l'approvazione della rimozione delle estensioni macOS non viene concessa e all'utente viene richiesto di immettere manualmente una password sull'endpoint durante il processo di disinstallazione del connettore per rimuovere le estensioni macOS.

Le estensioni dell'endpoint sicuro possono essere rimosse come parte della disinstallazione del connettore quando viene installato un profilo di gestione con la proprietà RemovableSystemExtensions aggiunta al payload SystemExtensions. La proprietà RemovableSystemExtensions deve contenere gli identificatori di bundle di entrambe le estensioni Secure Endpoint:

Payload	Proprietà	Valore
Estensioni di sistema	EstensioniSistemaRimovibili	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Accesso completo al disco

MacOS 10.14 e versioni successive richiedono l'approvazione prima che un'applicazione possa accedere a parti del file system che contengono dati utente personali (ad esempio, Contatti, Foto, Calendario e altre applicazioni). Alcune funzioni dei connettori, ad esempio la scansione dei file all'accesso, non sono in grado di analizzare questi file per rilevare eventuali minacce senza approvazione.

Le versioni precedenti dei connettori Mac richiedevano all'utente di concedere l'accesso completo al disco al programma `ampdaemon`. Il connettore Mac 1.14 richiede l'accesso completo al disco per:

- "AMP for Endpoints Service"
- "AMP Security Extension"

Il connettore Mac 1.16.0 e versioni successive richiedono l'accesso completo al disco aggiuntivo per:

- "Cisco Orbital" se abilitato in policy, disponibile con accesso Advantage e Premier

Il connettore Mac 1.18 e versioni successive richiedono l'accesso completo al disco per:

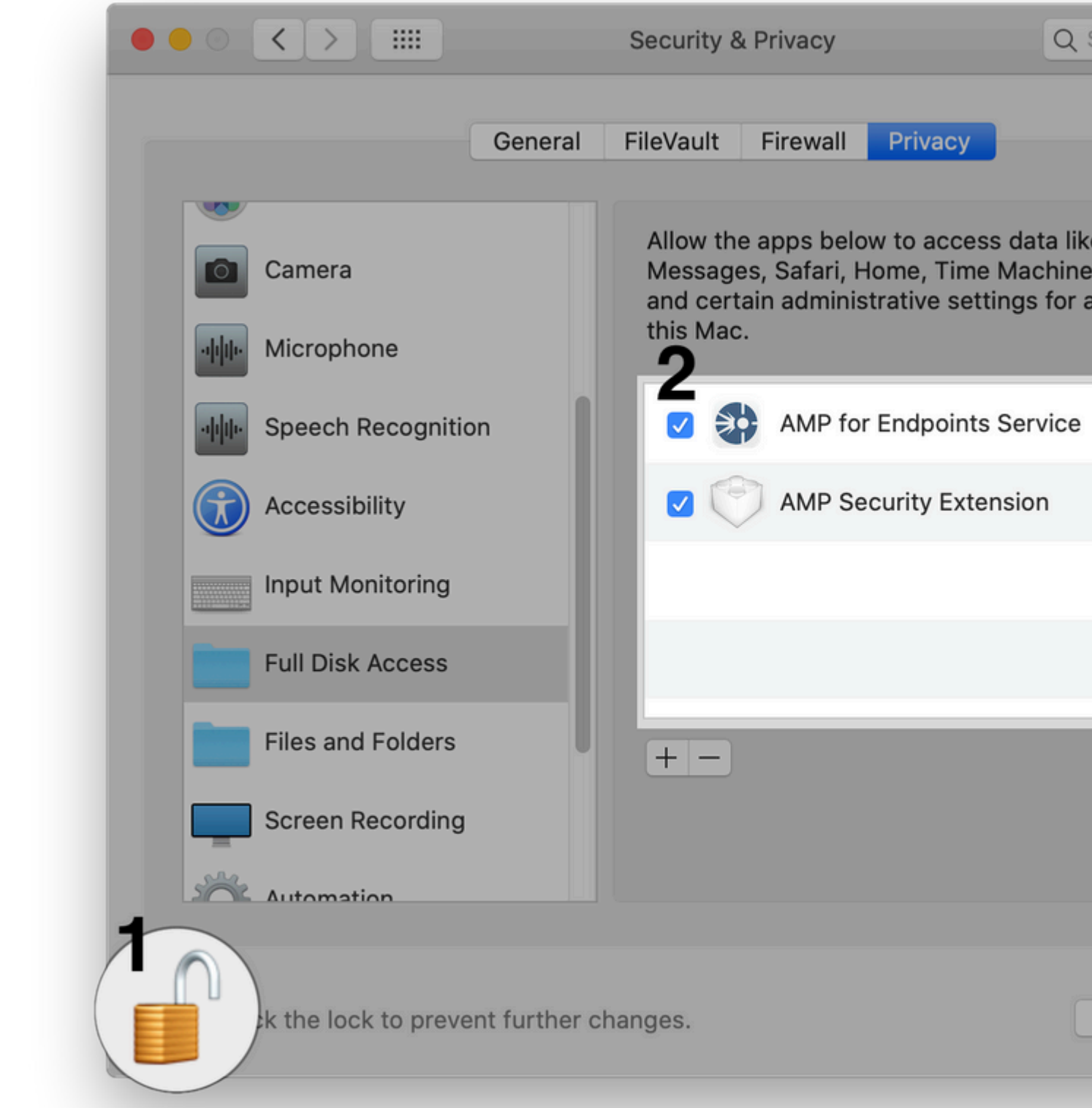
- "Secure Endpoint Service"
- "Secure Endpoint System Monitor"
- "Cisco Orbital" quando Orbital è abilitato nella policy (disponibile con i livelli Advantage e Premier)

Il programma `ampdaemon` non richiede più l'accesso completo al disco con il connettore Mac versione 1.14 e successive.

Le approvazioni di accesso completo al disco possono essere concesse nelle preferenze di sicurezza e privacy di macOS sull'endpoint o tramite i profili MDM (Mobile Device Management).

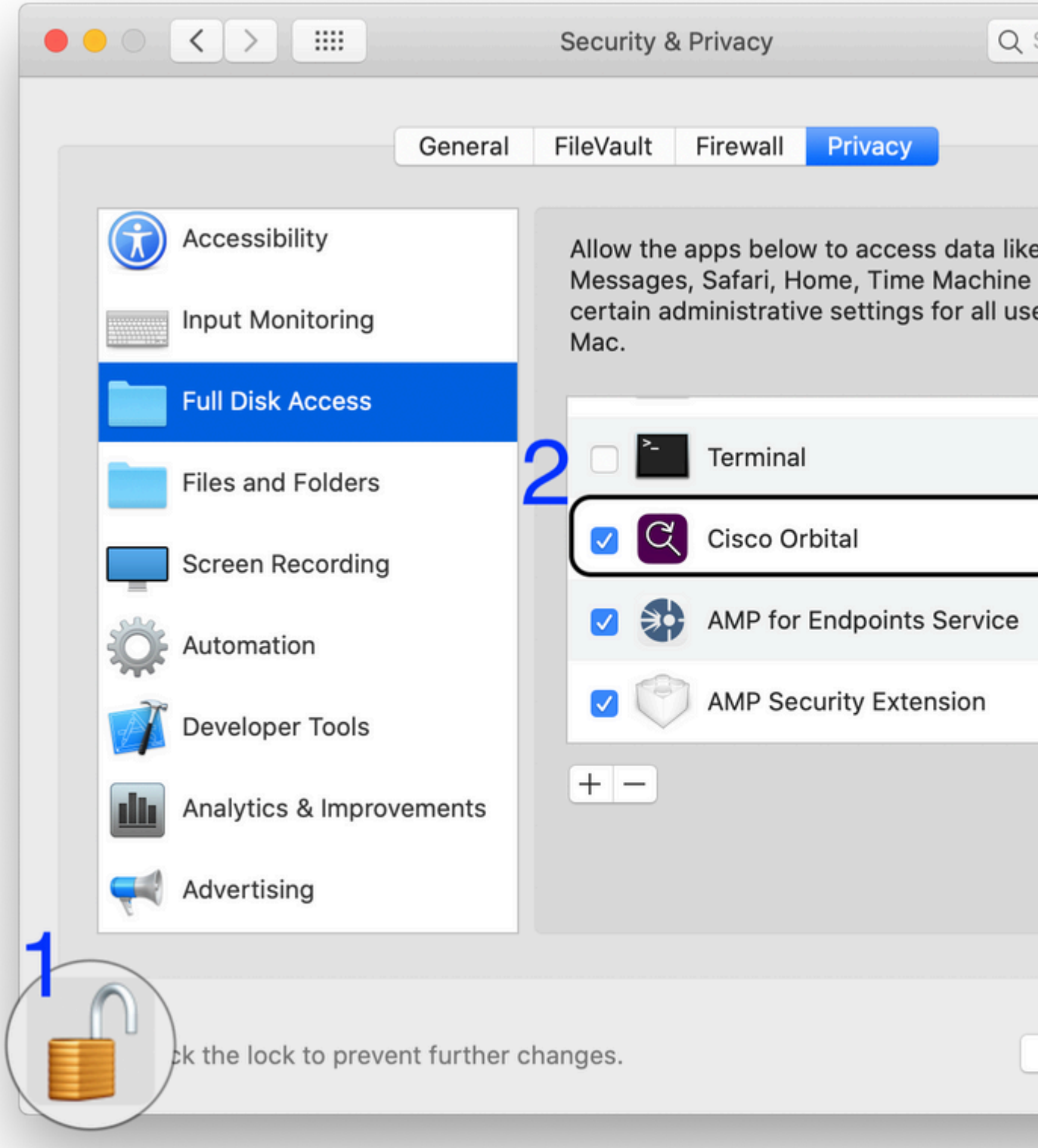
Approvazione dell'accesso completo al disco per le versioni dei connettori precedenti alla 1.18.0 sull'endpoint

Accesso completo al disco può essere approvato manualmente dal riquadro delle preferenze di sicurezza e privacy di macOS.



Approvazione dell'accesso completo al disco per Cisco Orbital sull'endpoint

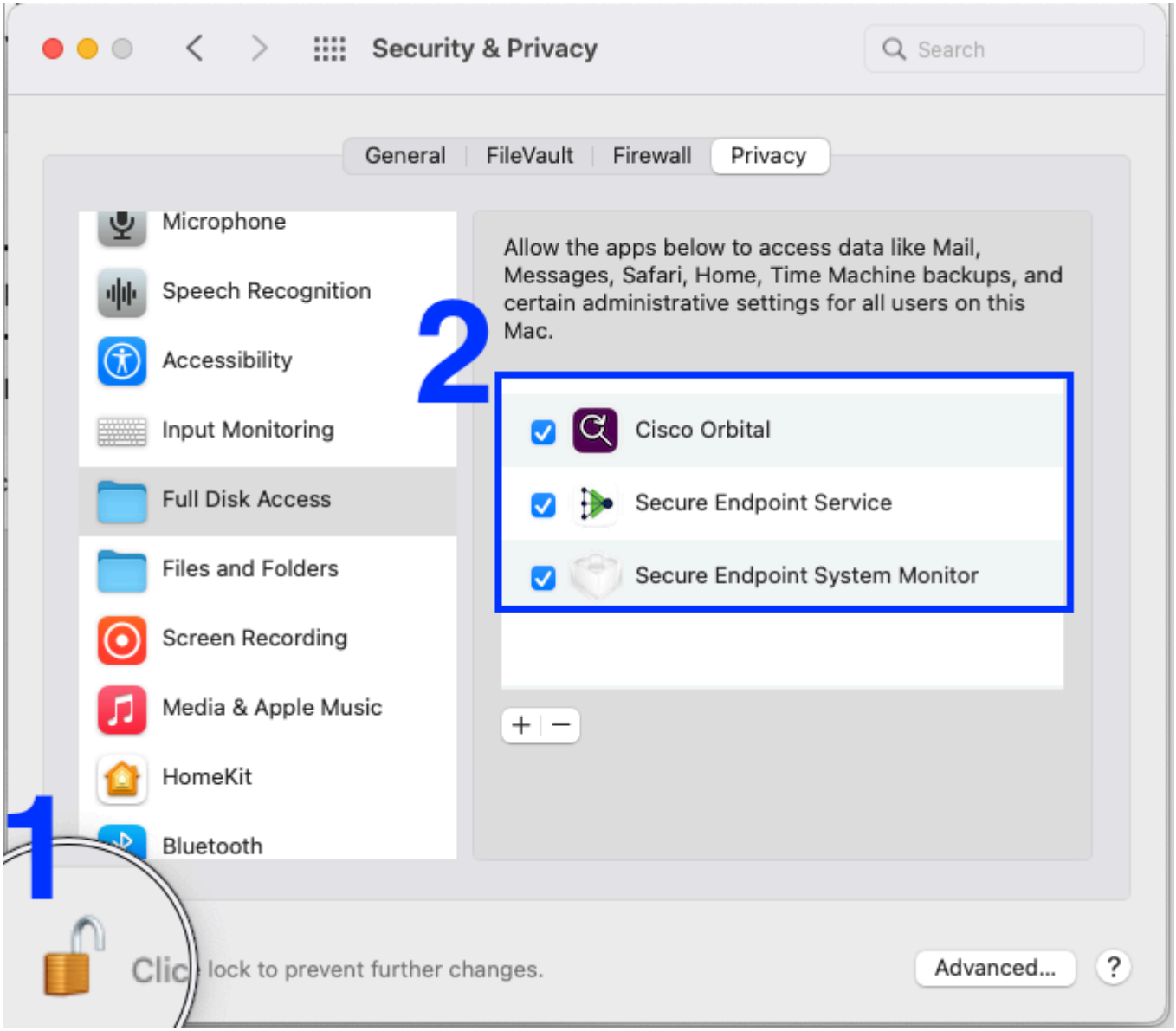
Accesso completo al disco può essere approvato manualmente dal riquadro delle preferenze di sicurezza e privacy di macOS.



Approvazione dell'accesso completo al disco per Cisco Secure Endpoint Connector 1.18.0 e versioni successive sull'endpoint

Accesso completo al disco può essere approvato manualmente dal riquadro delle preferenze di sicurezza e

privacy di macOS.



Approvazione dell'accesso completo al disco per il connettore con MDM

NOTA: le estensioni macOS non possono essere approvate retroattivamente tramite MDM. Se il profilo MDM non viene distribuito prima dell'installazione del connettore, le approvazioni non vengono concesse ed è necessario un ulteriore intervento in uno dei due modi seguenti:

1. Approvazione manuale delle estensioni macOS sugli endpoint con il profilo di gestione distribuito retroattivamente.
2. Aggiornare il connettore Mac a una versione più recente di quella attualmente distribuita. Gli endpoint con il profilo di gestione distribuito in modo retroattivo riconoscono il profilo di gestione dopo l'aggiornamento e ottengono l'approvazione al termine dell'aggiornamento.

L'accesso completo al disco può essere approvato da un profilo di gestione payload del controllo delle preferenze di privacy con una proprietà SystemPolicyAllFiles con due voci, una per il `servizio Secure Endpoint (AMP for Endpoints Service per le versioni di connettore precedenti alla 1.18.0)` e una per `Secure Endpoint System Monitor (AMP Security Extension per le versioni di connettore precedenti alla 1.18.0)`:

Descrizione	Proprietà	Valore
Secure Endpoint Service (AMP for Endpoints Service)	ALLOWED	vero
	RequisitoCodice	l'identificatore generico e "com.cisco.endpoint.svc" e (certificate leaf[field.1.2.840.113635.100.6.1.9] /* esiste */ o il certificato 1[field.1.2.840.113635.100.6.2.6] /* esiste */ e il certificato leaf[field.1.2.840.113635.100.6.1 13] /* esiste */ e foglia certificato[subject.OU] = DE8Y96K9QP)
	Identificativo	cisco.endpoint.svc
	TipoIdentificatore	ID pacchetto
Secure Endpoint System Monitor (estensione di sicurezza AMP)	ALLOWED	vero
	RequisitoCodice	anchor apple generic and identifier "com.cisco.endpoint.svc.securityextension" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* esiste */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* esiste */ and certificate leaf[field.1.2.840.113635.10 0.6.1.13] /* esiste */ e certificato foglia[subject.OU] = DE8Y96K9QP)
	Identificativo	estensione com.cisco.endpoint.svc.securityextension
	TipoIdentificatore	ID pacchetto

Se la distribuzione include computer con connettore versione 1.12.7 o precedente installato, questa voce aggiuntiva è ancora necessaria per concedere l'accesso completo al disco a `ampdaemon` per tali computer:

Descrizione	Proprietà	Valore
ampdaemon	ALLOWED	vero
	RequisitoCodice	l'identificatore ampdaemon and anchor apple generic e il certificato 1[field.1.2.840.113635.100.6.2.6] /* esiste */ e il certificato leaf[field.1.2.840.113635.100.6.1.13] /* esiste */ e il certificato leaf[subject.OU] = TDNYQP7VRK
	Identificativo	/opt/cisco/amp/ampdaemon
	TipoIdentificatore	percorso

Approvazione dell'accesso completo al disco per Cisco Orbital con MDM

Se la distribuzione include computer con connettore Cisco Secure Endpoint Mac versione 1.16.0 o successive, in computer con macOS 10.15 o successiva e Orbital è abilitato nei criteri, questa voce aggiuntiva è comunque necessaria per concedere l'accesso completo al disco Orbital per tali computer:

Descrizione	Proprietà	Valore
Cisco Orbital	ALLOWED	vero
	RequisitoCodice	anchor apple generic and identifier "com.cisco.endpoint.orbital.app" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* esiste */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* esiste */ and certificate leaf[field.1.2.840.113635.100.6.1 1.13] /* esiste */ e foglia certificato[subject.OU] = DE8Y96K9QP)
	Identificativo	com.cisco.endpoint.orbitale.app
	TipoIdentificatore	ID pacchetto

Esempio di profilo di configurazione MDM

Questo esempio di profilo di configurazione MDM può essere utilizzato come riferimento.

- Approvazione delle estensioni di sistema per il connettore Secure Endpoint Mac.
- Concede l'accesso completo al disco per il connettore Secure Endpoint Mac e Orbital.
- Consente la disinstallazione invisibile all'utente delle estensioni di sistema quando il connettore viene disinstallato.
  NOTA: quando l'autorizzazione RemovableSystemExtensions è consentita, qualsiasi utente o processo con privilegi di primo livello può rimuovere l'estensione di sistema senza richiedere la password utente. Pertanto, la proprietà RemovableSystemExtensions deve essere utilizzata solo quando l'amministratore desidera automatizzare la disinstallazione del connettore.

```
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

Esempio di configurazione MDM per macOS 10.15 o versione precedente

- Approvazione delle estensioni del kernel e concessione dell'accesso completo al disco per i connettori.
  - NOTA: M1 e i prodotti Apple più recenti non possono utilizzare profili che contengono questa configurazione

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

Nuova struttura di directory

Versioni da 1.14.0 a 1.16.2

Il connettore Mac 1.14 introduce due modifiche alla struttura della directory:

1. La directory Applications è stata rinominata da `Cisco AMP` a `Cisco AMP for Endpoints`.
2. L'utilità della riga di comando `ampcli` è stata spostata da `/opt/cisco/amp` a `/Applications/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS`. La directory `/opt/cisco/amp` contiene un collegamento simmetrico al programma `ampcli` nella nuova posizione.

Di seguito è riportata la struttura di directory completa per le versioni del connettore Mac da 1.14.0 a 1.16.2:

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

Versioni 1.18.0 e successive

Il connettore Mac 1.18 introduce una modifica alla struttura di directory delle applicazioni:

1. La directory Applications è stata rinominata da `Cisco AMP for Endpoints` a `Cisco Secure Endpoint`.

Di seguito è riportata la struttura di directory completa per il connettore Mac versione 1.18.0 e successive:

```
â”œâ”€â”€ Applications
|   â””â”€â”€ Cisco Secure Endpoint
|       â””â”€â”€Secure Endpoint Connector.app
|       |    â””â”€â”€ Contents
|       |        â””â”€â”€ MacOS
|       |
|       â””â”€â”€ Secure Endpoint Service.app
|       |   â””â”€â”€ Contents
|       |       â””â”€â”€ MacOS
|       |           â””â”€â”€ ampcli
|       |           â””â”€â”€ ampdaemon
|       |           â””â”€â”€ ampscansvc
|       |           â””â”€â”€ ampcreport
|       |           â””â”€â”€ ampupdater
|       |           â””â”€â”€ SupportTool
|       |
|       â””â”€â”€ Support Tool.app
```

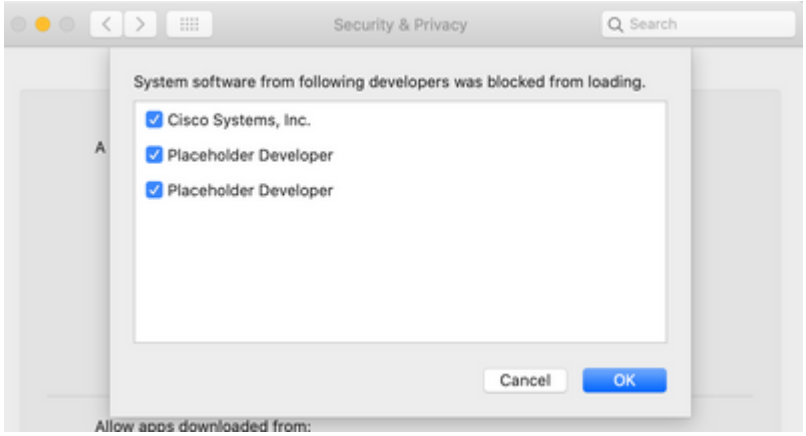
Problemi noti con macOS 11.0 e Mac Connector 1.14.1.

- Le istruzioni per l'errore 10, "Riavvio necessario per caricare il modulo del kernel o l'estensione del sistema", possono essere errate se sul computer sono installati quattro o più filtri dei contenuti di rete. Per ulteriori informazioni, consultare l'articolo Cisco Secure Endpoint Mac Connector Faults.

Problemi noti con macOS 10.15/11.0 e Mac Connector 1.14.0.

- Alcuni errori generati dal connettore Mac possono essere generati in modo imprevisto. Per ulteriori informazioni, consultare l'articolo Cisco Secure Endpoint Mac Connector Faults.
  - Errore 13. Troppe estensioni di sistema di Filtro contenuto di rete possono essere generate dopo un aggiornamento. Il riavvio del computer risolve il problema in questa situazione.
  - Errore 15. L'estensione del sistema richiede l'accesso completo al disco. Può essere generato dopo il riavvio a causa di un bug in macOS 11.0.0. Questo problema è risolto in macOS 11.0.1. Per risolvere il problema, è possibile concedere nuovamente l'accesso completo al disco nel riquadro Protezione e privacy in Preferenze di sistema macOS.

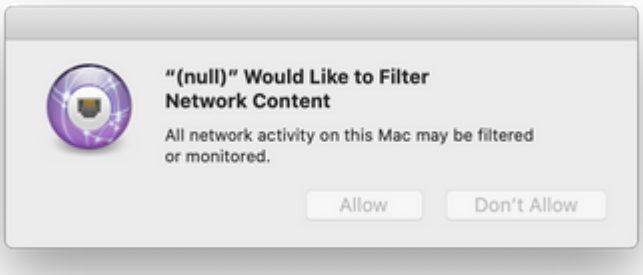
- Durante l'installazione, il riquadro Protezione e privacy può visualizzare "Placeholder Developer" come nome dell'applicazione quando macOS chiede l'autorizzazione per l'esecuzione delle estensioni di sistema del connettore Mac. Ciò è dovuto a un bug in macOS 10.15. Selezionare le caselle accanto a "Placeholder Developer" per consentire al connettore Mac di proteggere il computer.



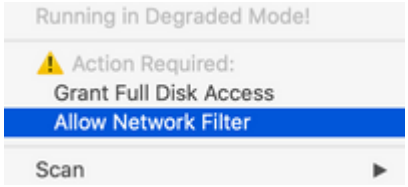
  - È possibile utilizzare il comando `systemextensionsctl` listcommand per determinare le

estensioni di sistema da approvare. Estensioni di sistema con stato `[activated wait for user]` in questo output vengono visualizzati come "Placeholder Developer" nella pagina delle preferenze macOS mostrata in precedenza. Se nella pagina delle preferenze sono visualizzate più di due voci "Placeholder Developer", disinstallare tutto il software che utilizza le estensioni di sistema (compreso il connettore Mac) in modo che nessuna estensione di sistema richieda l'approvazione, quindi reinstallare il connettore Mac.
Le estensioni del sistema di connettori per Mac sono identificate come segue:
    - L'estensione di rete viene visualizzata come `com.cisco.endpoint.svc.networkextension`.
    - Viene visualizzata l'estensione Sicurezza endpoint con `com.cisco.endpoint.svc.securityextension`.

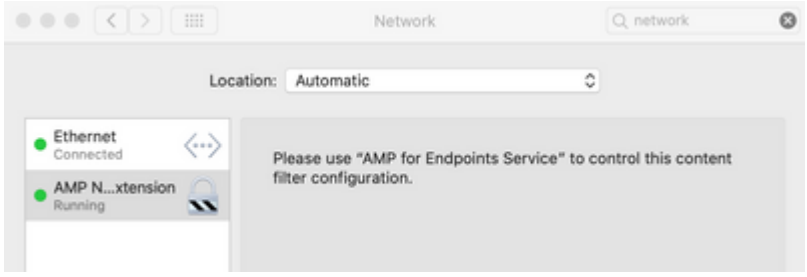
- Durante l'installazione, la richiesta di consentire al filtro contenuti di monitorare il traffico di rete può visualizzare "(null)" come nome dell'applicazione. Ciò è causato da un bug in macOS 10.15. L'utente deve selezionare "Consenti" per garantire la protezione del computer.



- Se la richiesta è stata ignorata perché è stato selezionato "Non consentire", selezionare "Consenti filtro di rete" dal menu a discesa nell'icona dell'agente  nella barra dei menu per aprire di nuovo il prompt.



- Una volta abilitato, il filtro Estensione rete endpoint sicuro viene elencato nella pagina Preferenze di rete.



- Su macOS 11, quando viene eseguito un aggiornamento dal connettore Mac 1.12 al connettore Mac 1.14, Fault 4, System Extension Failed to Load, può essere sollevato temporaneamente mentre il connettore passa dalle estensioni del kernel alle nuove estensioni del sistema.

Problemi noti durante la disinstallazione delle estensioni di sistema

- Prima di macOS 12, o quando MDM non viene utilizzato, quando viene eseguita una disinstallazione

del connettore Mac all'utente viene richiesto di immettere la password due volte in modo che le estensioni di sistema possano essere disinstallate. Si tratta di una limitazione di macOS ed è stata in qualche modo migliorata in macOS 12 con l'aggiunta della chiave di profilo MDM RemovableSystemExtensions descritta in questo documento.

Script di installazione della distribuzione di Intune

- Uno script che consentirà di installare il connettore Secure Endpoint su macOS gestito da Microsoft è ospitato qui:

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

Connettore Mac rebranded (versioni 1.18.0 e successive)

NOTA: le configurazioni MDM esistenti per le versioni dei connettori precedenti alla 1.18.0 funzionano senza interventi per gli aggiornamenti alle versioni dei connettori 1.18.0 e successive. Per ulteriori informazioni, vedere Secure Endpoint Mac Rebrand.

Cronologia delle revisioni

01 dic 2020

- Il connettore Mac 1.14.1 non utilizza più le estensioni di sistema su macOS 10.15.
- Ulteriori informazioni sul controllo terminale quali estensioni di sistema "Placeholder Developer" richiedono approvazione con il connettore Mac 1.14.0.

09 nov 2020

- ID bundle corretto nel payload MDM del requisito del codice di accesso completo al disco.

03 nov 2020

- La data di rilascio per il connettore Mac 1.14.0 è novembre 2020.
- Il connettore Mac 1.14.0 utilizza le estensioni di sistema con macOS 10.15.5 e versioni successive. In precedenza era 10.15.6.
- È stata aggiunta la sezione Problemi noti.
- Struttura della directory aggiornata.

03 giugno 2021

- Sono state aggiunte le istruzioni per concedere l'accesso completo al disco per Cisco Orbital.

13 ott 2021

- Aggiunta rimozione delle estensioni macOS del connettore Mac con la sezione MDM.
- Sono stati aggiunti i problemi noti relativi alla sezione Disinstallazione delle estensioni di sistema.

25 feb 2022

- Rebrand

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).