Configurar permissões para conector Mac e orbital de endpoint seguro com MDM: acesso total ao disco, extensões do sistema

Contents

Introduction

Este documento descreve as alterações e etapas recentes para que os administradores implantem o conector Mac 1.14 e mais recente.

Perfis MDM

É altamente recomendável implantar o conector Mac com um perfil MDM que conceda as aprovações necessárias. Os perfis MDM devem ser instalados antes da instalação, atualização ou remoção do conector Mac para garantir que as permissões necessárias sejam reconhecidas. Consulte a seção Problemas conhecidos posteriormente neste documento se o MDM não puder ser usado.

Avisos

A versão 1.14 do conector Mac introduziu alterações que exigem atenção:

- Aprovação completa de acesso ao disco
- Aprovação de extensão do sistema

O conector Mac 1.14 ou mais recente é necessário para garantir a proteção do endpoint no macOS 11 e posterior. Conectores Mac mais antigos não funcionam nessas versões do MacOS.

A versão 1.16 do conector Mac introduziu o suporte para o Cisco Orbital em hardware Intel. O Orbital pode ser habilitado de acordo com a política com o Advantage ou Premier Tier e é instalado automaticamente quando habilitado e instalado em uma versão de SO e hardware compatíveis. A versão 1.20 do conector Mac introduz a prontidão de suporte para o Cisco Orbital no hardware de silício da Apple, planejado para ser lançado com o Orbital Node 1.21. Consulte as seções Cisco Orbital deste documento para obter detalhes sobre como conceder as permissões adicionais de acesso total ao disco necessárias para Orbital.

Requisitos mínimos do SO

O conector Mac 1.14.0 do Cisco Secure Endpoint oferece suporte às versões do macOS:

- macOS 11, com extensões de sistema macOS.
- macOS 10.15.5 e posterior, com extensões de sistema macOS.
- macOS 10.15.0 a macOS 10.15.4, com extensões de kernel macOS.
- macOS 10.14, com extensões de kernel macOS.

O conector Mac 1.14.1 do Cisco Secure Endpoint oferece suporte às versões do macOS:

- macOS 11, com extensões de sistema macOS.
- macOS 10.15 com extensões de kernel macOS.
- macOS 10.14, com extensões de kernel macOS.

O suporte para Cisco Orbital em hardware Intel foi introduzido na versão 1.16.0 do conector Secure Endpoint Mac. O suporte para Cisco Orbital em hardware de silício da Apple foi introduzido no conector Secure Endpoint Mac versão 1.20.0.

Consulte a Tabela de Compatibilidade de SO para obter informações sobre a compatibilidade atual do conector Mac.

Alterações importantes

O conector Mac 1.14 introduziu alterações importantes em três áreas:

1. Aprovação das extensões macOS usadas pelo conector
2. Acesso total ao disco
3. Nova Estrutura de Diretório

O MacOS 12 introduziu uma opção MDM para permitir a remoção das extensões macOS do conector sem solicitar senhas de usuário.

Aprovação das extensões Mac Connector macOS

O conector Mac usa as extensões do sistema ou as extensões do kernel herdadas para monitorar as atividades do sistema, conforme necessário para a versão macOS. No macOS 11, as Extensões de Sistema substituem as Extensões de Kernel legadas que não são suportadas no macOS 11 e posterior. É necessária a aprovação

do usuário em todas as versões do macOS antes que qualquer tipo de extensão possa ser executado. Sem aprovação, certas funções de conector, como varredura de arquivos ao acessar e monitor de acesso à rede, não estão disponíveis.

O conector Mac 1.14 introduz duas novas extensões de sistema macOS:

1. Uma extensão do Endpoint Security, chamada Secure Endpoint File Monitor (anteriormente AMP Security Extension), para monitorar eventos do sistema
2. Uma extensão do Network Content Filter, chamada Cisco Secure Endpoint Filter (anteriormente AMP Network Extension), para monitorar o acesso à rede

As duas extensões de kernel legadas, `ampfileop.kext` e `ampnetworkflow.kext`, estão incluídas para compatibilidade com versões anteriores do macOS que não suportam as novas extensões de sistema do macOS.

As aprovações necessárias para o macOS 11** e posterior:

- Aprovar Monitor de Arquivo de Ponto de Extremidade Seguro para carregar
- Aprovar Filtro de Ponto de Extremidade Seguro da Cisco para carregar
- Permitir que o Filtro de Ponto de Extremidade Seguro da Cisco filtre o conteúdo da rede

** conector Mac versão 1.14.0 também exigia essas aprovações no macOS 10.15. Essas aprovações não são mais necessárias no macOS 10.15 para o conector Mac 1.14.1 ou mais recente.

As aprovações necessárias para macOS 10.14 e macOS 10.15:

- Aprovar Extensões de Kernel do conector a serem carregadas

Essas aprovações podem ser concedidas nas Preferências de segurança e privacidade do macOS no endpoint ou por meio de perfis de gerenciamento de dispositivos móveis (MDM).

Aprovação das extensões Mac Connector macOS no endpoint

As extensões de sistema e kernel podem ser aprovadas manualmente no painel Preferências de segurança e privacidade do macOS.

Aprovação das extensões Mac Connector macOS com MDM

OBSERVAÇÃO: As extensões macOS **não podem** ser aprovadas retroativamente via MDM. Se o perfil MDM não for implantado antes da instalação do conector, as aprovações não serão concedidas e será necessária uma intervenção adicional em uma destas duas formas:

1. Aprovação manual das extensões macOS em endpoints com o perfil de gerenciamento implantado retroativamente.

2. Atualize o conector Mac para uma versão mais recente do que a atualmente implantada. Os endpoints com o perfil de gerenciamento implantado de forma retroativa reconhecem o perfil de gerenciamento após uma atualização e obtêm aprovação após a conclusão da atualização.

As extensões do Secure Endpoint podem ser aprovadas com um perfil de gerenciamento com estas cargas e propriedades:

Carga útil	Propriedade	Valor
Extensões doSistema	AllowedSystemExtensions	com.cisco.endpoint.svc.securitye com.cisco.endpoint.svc.network
	TiposDeExtensãoDoSistemaPermitidos	ExtensãoDeSegurançaDoPontoF ExtensãoDeRede
	IdentificadoresEquipePermitidos	DE8Y96K9QP
ExtensõesKernelDaPolíticaDoSistema	ExtensõesKernelPermitidas	com.cisco.amp.fileop, com.cisco
	IdentificadoresEquipePermitidos	TDNYQP7VRK
FiltroDeConteúdoDaWeb	AutoFiltroHabilitado	falso
	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.network
	FilterDataProviderDesignatedRequirement	genérico e identificador de apple "com.cisco.endpoint.svc.networl e (certificate leaf[field.1.2.840.113635.100.6. exists */ ou certificate 1[field.1.2.840.113635.100.6.2.6 */ e certificate leaf[field.1.2.840.113635.100.6. exists */ e certificate leaf[subject DE8Y96K9QP)
	FiltrarGrau	firewall
	FiltrarNavegadores	falso
	FiltrarPacotes	falso
	FiltrarSoquetes	verdadeiro
	IDdoPacotePlug-in	com.cisco.endpoint.svc
	Nomedefinido pelo usuário	Cisco Secure Endpoint Filter (ex rede AMP se a versão do conecto anterior à 1.18.0)

Remoção das extensões Mac Connector macOS com MDM

O MacOS 12 e posterior permite que as extensões macOS sejam marcadas como removíveis com a propriedade RemovableSystemExtensions, conforme descrito abaixo.
OBSERVAÇÃO: quando a permissão removível do macOS Extension é permitida, qualquer usuário ou processo com privilégios de raiz tem a capacidade de remover o ramal sem solicitar a senha do usuário. Assim, a propriedade RemovableSystemExtensions só deve ser usada quando o administrador deseja automatizar a desinstalação do conector.
OBSERVAÇÃO: As extensões macOS **não podem** ser removidas retroativamente via MDM. Se o perfil MDM não for implantado antes da desinstalação do conector, a aprovação de remoção das extensões macOS não será concedida e o usuário precisará inserir manualmente uma senha no endpoint durante o processo de desinstalação do conector para remover as extensões macOS.

As extensões de Ponto de Extremidade Seguro podem ser removidas como parte da desinstalação do conector quando um perfil de gerenciamento com a propriedade RemovableSystemExtensions adicionada à carga de SystemExtensions for instalado. A propriedade RemovableSystemExtensions deve conter os identificadores de pacote das duas extensões de Ponto de Extremidade Seguro:

Carga útil	Propriedade	Valor
Extensões doSistema	ExtensõesDeSistemaRemovíveis	com.cisco.endpoint.svc.securityextension, com.cisco.endpoint.svc.networkextension

Acesso total ao disco

O MacOS 10.14 e posterior requer aprovação antes que um aplicativo possa acessar partes do sistema de arquivos que contenham dados pessoais do usuário (por exemplo, Contatos, Fotos, Calendário e outros aplicativos). Determinadas funções do conector, como varredura de arquivos ao acessar, não podem examinar esses arquivos em busca de ameaças sem aprovação.

Versões anteriores do conector Mac exigiam que o usuário concedesse acesso total ao disco para o programa `ampdaemon`. O conector Mac 1.14 requer acesso total ao disco para:

- "Serviço AMP para endpoints"
- "Extensão de segurança da AMP"

O conector Mac 1.16.0 e mais recente requer acesso total ao disco adicional para:

- "Cisco Orbital" quando habilitado na política, disponível com acesso Advantage e Premier

O conector Mac 1.18 e mais recente requer acesso total ao disco para:

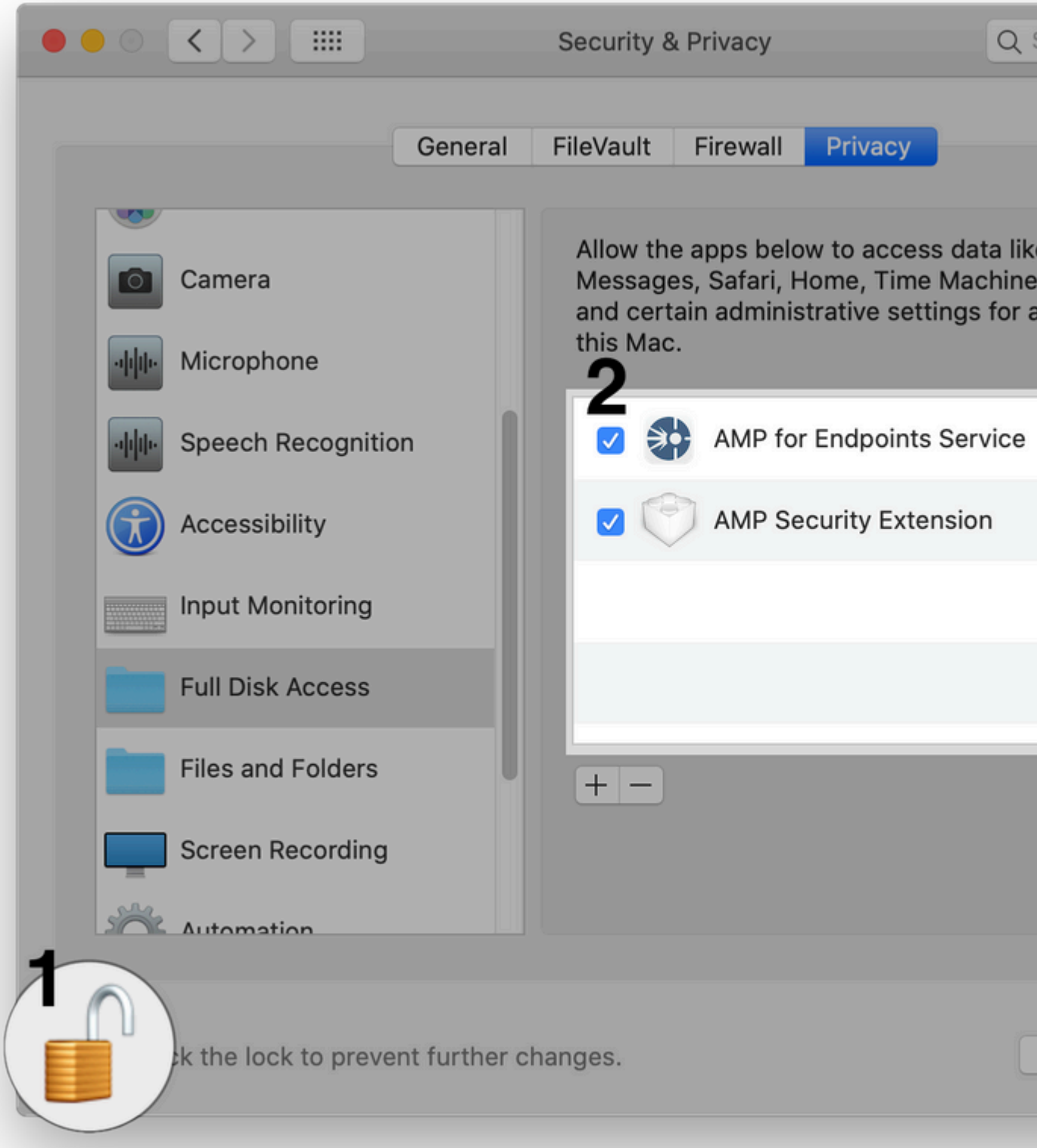
- "Secure Endpoint Service"
- "Monitor de sistema de endpoint seguro"
- "Cisco Orbital" quando a Orbital está habilitada na política (disponível com as camadas Advantage e Premier)

O programa `ampdaemon` não requer mais Full Disk Access com conector Mac versão 1.14 e mais recente.

As aprovações completas de acesso ao disco podem ser concedidas nas preferências de segurança e privacidade do macOS no endpoint ou através de perfis de gerenciamento de dispositivos móveis (MDM).

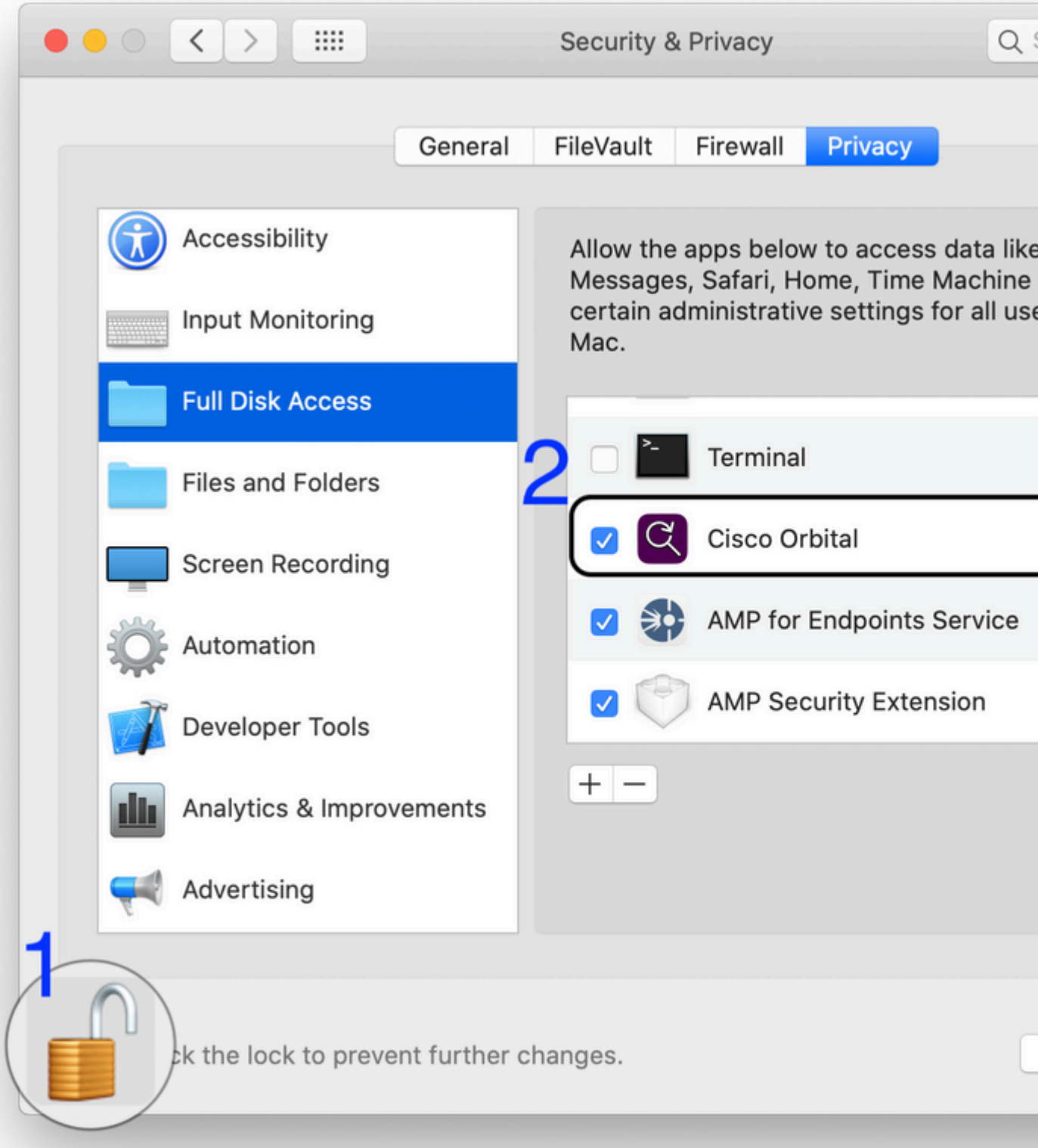
Aprovação de Acesso Total ao Disco para versões de conector anteriores à 1.18.0 no Endpoint

O acesso total ao disco pode ser aprovado manualmente no painel Preferências de segurança e privacidade do macOS.



Aprovação de acesso total ao disco para Cisco Orbital no endpoint

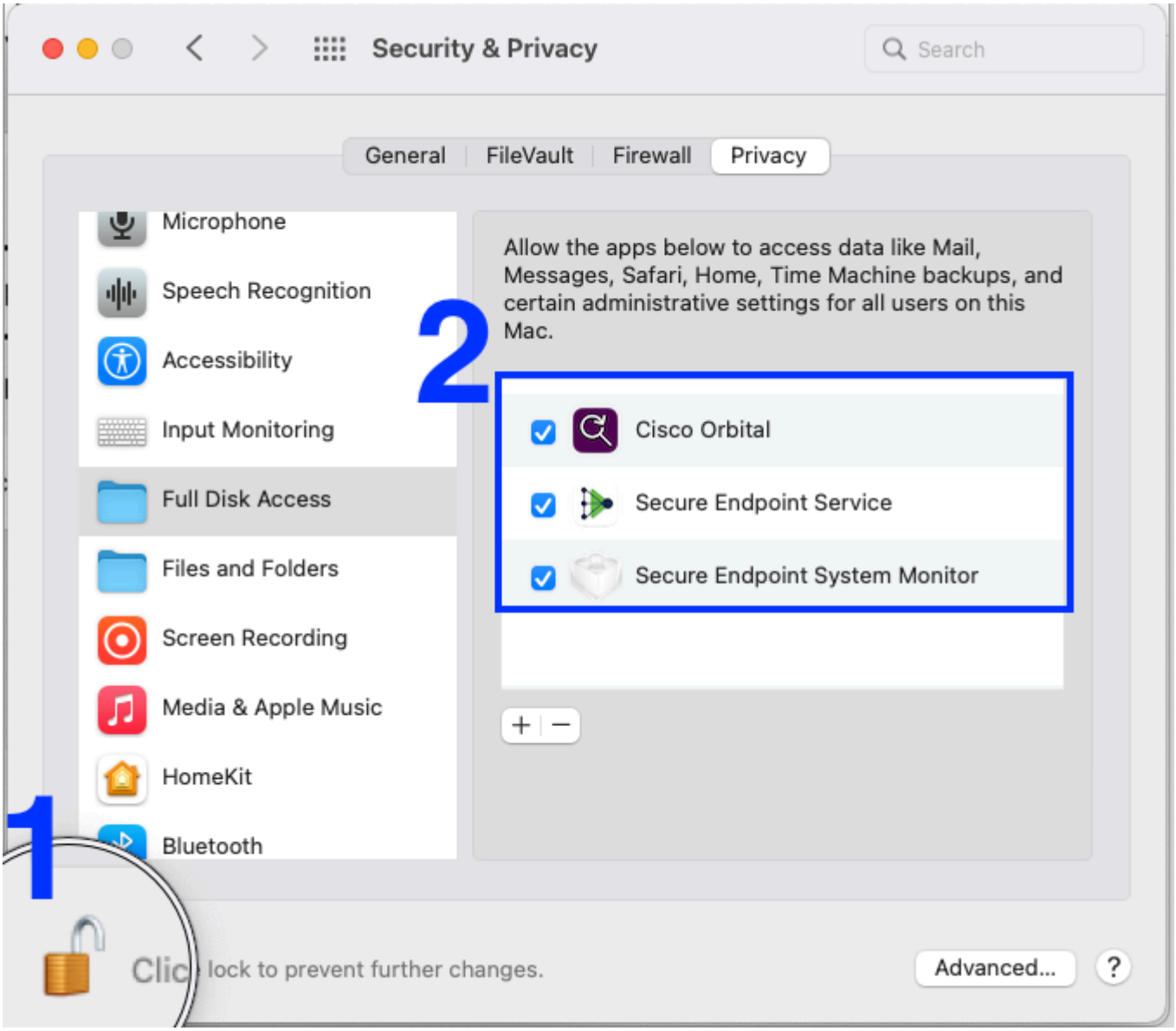
O acesso total ao disco pode ser aprovado manualmente no painel Preferências de segurança e privacidade do macOS.



Aprovação de acesso total ao disco para conector 1.18.0 do Cisco Secure Endpoint e mais recente no endpoint

O acesso total ao disco pode ser aprovado manualmente no painel Preferências de segurança e privacidade

do macOS.



Aprovação de Acesso Total ao Disco para o Conector com MDM

OBSERVAÇÃO: As extensões macOS **não podem** ser aprovadas retroativamente via MDM. Se o perfil MDM não for implantado antes da instalação do conector, as aprovações não serão concedidas e será necessária uma intervenção adicional em uma destas duas formas:

1. Aprovação manual das extensões macOS em endpoints com o perfil de gerenciamento implantado retroativamente.
2. Atualize o conector Mac para uma versão mais recente do que a atualmente implantada. Os endpoints que tiveram o perfil de gerenciamento implantado reconhecem retroativamente o perfil de gerenciamento após a atualização e obtêm aprovação quando a atualização é concluída.

O acesso total ao disco pode ser aprovado por um perfil de gerenciamento Privacy Preferences Policy Control com uma propriedade SystemPolicyAllFiles com duas entradas, uma para o `Secure Endpoint Service (AMP para Endpoints Service para versões do conector anteriores a 1.18.0)` e outra para o Secure Endpoint System Monitor (AMP Security Extension para versões do conector anteriores a 1.18.0):

Descrição	Propriedade	Valor
Secure Endpoint	Permitido	verdadeiro

Descrição	Propriedade	Valor
Service (Serviço AMP para Endpoints)	CodeRequirement	genérico e identificador de apple de âncora "com.cisco.endpoint.svc" e (certificado leaf[field.1.2.840.113635.100.6.1.9] /* exists */ ou certificado 1[field.1.2.840.113635.100.6.2.6] /* exists */ e certificado leaf[field.1.2.840.113635.100.6.1.13] /* exists */ e certificado leaf[subject.OU] = DE8Y 96 K9QP)
	Identifier	com.cisco.endpoint.svc
	Tipo deidentificador	ID do pacote
Monitor de sistema de endpoint seguro (extensão de segurança AMP)	Permitido	verdadeiro
	CodeRequirement	genérico e identificador de apple de âncora "com.cisco.endpoint.svc.securityextension" e (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ ou certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ e certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ e certificate leaf[subject.OU] = DE8Y96K9QP)
	Identifier	com.cisco.endpoint.svc.securityextension
	Tipo deidentificador	ID do pacote

Se a distribuição incluir computadores com a versão de conector 1 12 7 ou mais antiga instalada, esta entrada adicional ainda será necessária para conceder acesso total ao disco para `ampdaemon` para esses computadores:

Descrição	Propriedade	Valor
ampdaemon	Permitido	verdadeiro
	CodeRequirement	identificador ampdaemon e âncora apple genérico e certificado 1[campo.1.2.840.113635.100.6.2.6] /* existe */ e certificado leaf[campo.1.2.840.113635.100.6.1.13] /* existe */ e certificado leaf[subject.OU] = TDNYQP7VRK
	Identifier	/opt/cisco/amp/ampdaemon
	Tipo deidentificador	caminho

Aprovação de acesso total ao disco para Cisco Orbital com MDM

Se a sua implementação incluir computadores com o conector Cisco Secure Endpoint Mac versões 1.16.0 ou mais recente, em computadores com o MacOS 10.15 ou mais recente, e o Orbital estiver habilitado na política, esta entrada adicional ainda será necessária para conceder acesso total ao disco para esses computadores:

Descrição	Propriedade	Valor
Cisco Orbital	Permitido	verdadeiro
	CodeRequirement	genérico e identificador da anchor apple "com.cisco.endpoint.orbital.app" e (certificado leaf[field.1.2.840.113635.100.6.1.9] /* exists */ ou certificado 1[field.1.2.840.113635.100.6.2.6] /* exists */ e certificado leaf[field.1.2.840.113635.100.6.1.13] /* exists */ e certificado leaf[subject.OU] = DE Y96K9QP)

Descrição	Propriedade	Valor
	Identifier	com.cisco.endpoint.orbital.app
	Tipo deidentificador	ID do pacote

Exemplo de perfil de configuração MDM

Este exemplo de perfil de configuração MDM pode ser usado como referência.

- Aprovação de extensões de sistema para conector Mac de Ponto de Extremidade Seguro.
- Concede acesso total ao disco para o conector Mac e o Orbital do Secure Endpoint.
- Permite a desinstalação silenciosa das extensões de sistema quando o conector é desinstalado. OBSERVAÇÃO: quando a permissão RemovableSystemExtensions é permitida, qualquer usuário ou processo com privilégios de raiz pode remover a Extensão do Sistema sem solicitar a senha do usuário. Assim, a propriedade RemovableSystemExtensions só deve ser usada quando o administrador deseja automatizar a desinstalação do 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

1

Exemplo de configuração MDM para macOS 10.15 ou anterior

- A aprovação de extensões de kernel concede acesso total ao disco para conectores.
    - OBSERVAÇÃO: os produtos M1 e mais recentes da Apple não podem usar perfis que contenham essa configuração

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

Nova Estrutura de Diretório

Versões 1.14.0 a 1.16.2

O conector Mac 1.14 introduz duas alterações na estrutura de diretórios:

1. O diretório de aplicativos foi renomeado de `Cisco AMP` para `Cisco AMP para endpoints`.
2. O utilitário de linha de comando `ampcli` foi movido de `/opt/cisco/amp` para `/Applications/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS`. O diretório `/opt/cisco/amp` contém um link simbólico para o programa `ampcli` em seu novo local.

A estrutura completa de diretórios para o conector Mac versões 1.14.0 a 1.16.2 é a seguinte:

```
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
```

Versões 1.18.0 e Mais Recentes

O conector Mac 1.18 introduz uma mudança na estrutura do diretório de aplicativos:

1. O diretório Applications foi renomeado de `Cisco AMP for Endpoints` para `Cisco Secure Endpoint`.

A estrutura completa de diretórios para as versões 1.18.0 e mais recentes do conector Mac é a seguinte:

```
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
```

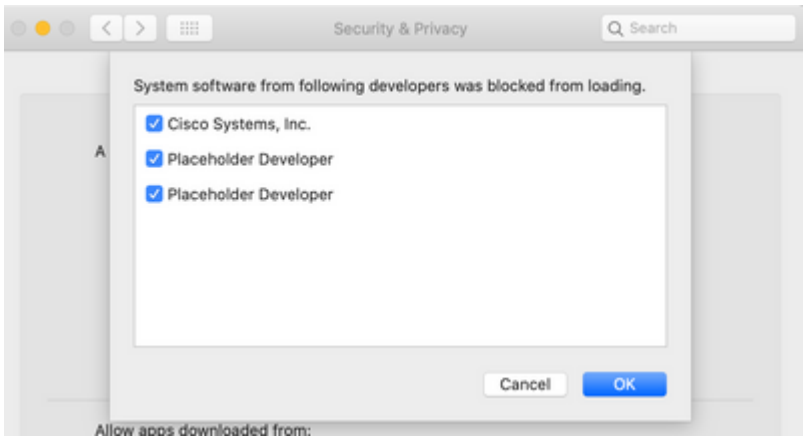
Problemas conhecidos do macOS 11.0 e do Mac Connector 1.14.1.

- A orientação para a falha 10, "Reinicialização necessária para carregar o módulo do kernel ou a extensão do sistema", pode estar incorreta se quatro ou mais Filtros de Conteúdo de Rede estiverem instalados no computador. Consulte o artigo Falhas do Conector Mac do Cisco Secure Endpoint para obter mais detalhes.

Problemas conhecidos com o MacOS 10.15/11.0 e o Mac Connector 1.14.0.

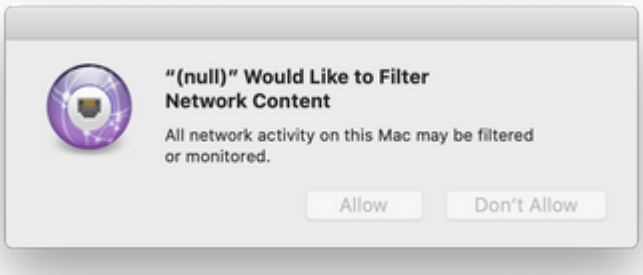
- Algumas falhas levantadas pelo conector Mac podem ser levantadas inesperadamente. Consulte o artigo Falhas do Conector Mac do Cisco Secure Endpoint para obter mais detalhes.
    - A falha 13, Excesso de extensões do sistema Network Content Filter, pode ser gerada após uma atualização. Uma reinicialização do computador resolve a falha nessa situação.
    - Falha 15, Extensão do Sistema requer Acesso Total ao Disco, pode ser levantada após a reinicialização devido a um bug no macOS 11.0.0. Esse problema é corrigido no macOS 11.0.1. A falha pode ser resolvida por uma nova concessão de acesso total ao disco no painel Segurança e privacidade nas preferências do sistema do macOS.

- Durante a instalação, o painel Segurança e privacidade pode exibir "Desenvolvedor de espaço reservado" como o nome do aplicativo quando o macOS pede permissão para que as extensões de sistema do conector Mac sejam executadas. Isso ocorre devido a um bug no macOS 10.15. Marque as caixas ao lado de "Placeholder Developer" para permitir que o conector Mac proteja o computador.

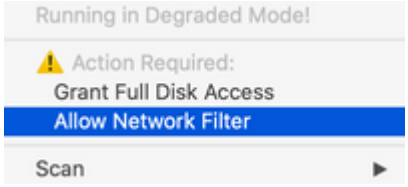


- O comando `systemextensionsctl list` pode ser usado para determinar quais extensões do sistema precisam de aprovação. Extensões do sistema com o estado `[ativado aguardando usuário]`nesta saída são exibidos como "Placeholder Developer" na página de preferências do macOS mostrada anteriormente. Se mais de duas entradas de "Placeholder Developer" forem mostradas na página de preferências, desinstale todos os softwares que usam extensões de sistema (incluindo o conector Mac) para que nenhuma extensão de sistema precise de aprovação e, em seguida, reinstale o conector Mac.
  As extensões de sistema do conector Mac são identificadas da seguinte forma:
  - A extensão de rede é mostrada como `com.cisco.endpoint.svc.networkextension`.
  - A extensão de segurança de endpoint mostrada tem `com.cisco.endpoint.svc.securityextension`.

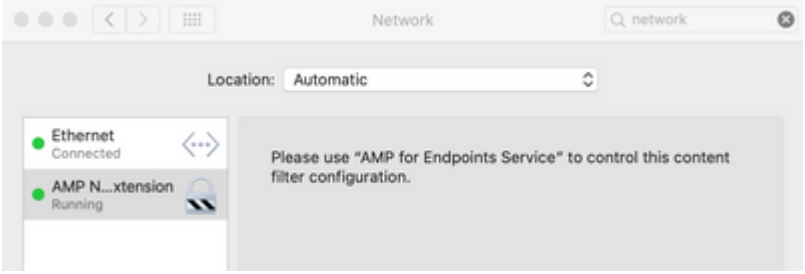
- Durante a instalação, o prompt para permitir que o Filtro de Conteúdo monitore o tráfego de rede pode exibir "(null)" como o nome do aplicativo. Isso é causado por um bug no macOS 10.15. O usuário precisa selecionar "Permitir" para garantir a proteção do computador.



- Se o aviso foi ignorado porque "Não permitir" foi escolhido, selecione "Permitir filtro de rede" no menu suspenso no ícone Agente  na barra de menus para abrir o prompt novamente.



- Depois de habilitado, o filtro Secure Endpoint Network Extension é listado na página Preferências da rede.



- No macOS 11, quando uma atualização do conector Mac 1.12 para o conector Mac 1.14 é realizada, a falha 4, System Extension Failed to Load, pode ser aumentada temporariamente enquanto o conector faz a transição das extensões do kernel para as novas extensões do sistema.

Problemas conhecidos durante a desinstalação de extensões do sistema

- Antes do macOS 12, ou quando o MDM não é usado, quando uma desinstalação do conector Mac é executada, o usuário é solicitado a inserir sua senha duas vezes para que as extensões do sistema possam ser desinstaladas. Esta é uma limitação do macOS e foi melhorada um pouco no macOS 12 com a adição da chave de perfil do MDM RemovableSystemExtensions descrita neste documento.

Script de Instalação de Implantação do Intune

- Um script que ajudará a instalar o conector Secure Endpoint no macOS mantido pela Microsoft está hospedado aqui:

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

Conector Mac renomeado (versões 1.18.0 e mais recentes)

OBSERVAÇÃO: as configurações MDM existentes para versões de conector mais antigas que 1.18.0 funcionam sem intervenção para atualizações para versões de conector 1.18.0 e mais recentes. Consulte Secure Endpoint Mac Rebrand para obter mais informações.

Histórico das revisões

1 de dezembro de 2020

- O conector Mac 1.14.1 não usa mais extensões de sistema no macOS 10.15.
- Orientações adicionais sobre verificação de terminal quais extensões de sistema do "Placeholder Developer" precisam de aprovação com o conector Mac 1.14.0.

9 Nov 2020

- ID do pacote corrigida na carga MDM CodeRequirement de acesso total ao disco.

3 Nov 2020

- A data de lançamento do conector Mac 1.14.0 é novembro de 2020.
- O conector Mac 1.14.0 usa as extensões de sistema com macOS 10.15.5 e posterior. Anteriormente, era 10.15.6.
- Adicionada a seção Problemas conhecidos.
- Estrutura de tópicos de diretório atualizada.

3 de junho de 2021

- Instruções adicionais para conceder acesso total ao disco para o Cisco Orbital.

13 de outubro de 2021

- Remoção adicionada de Mac Connector macOS Extensions com seção MDM.
- Adicionados problemas conhecidos para a seção Desinstalação de extensões do sistema.

25 de fevereiro de 2022

- Renomear marca

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.