使用MDM配置安全终端Mac连接器和轨道的权限：全磁盘访问，系统扩展

目录

简介

MDM配置文件

Advisories

最低操作系统要求

重要更改

批准Mac连接器macOS扩展

- 在终端上批准Mac Connector macOS扩展
- 使用MDM批准Mac连接器macOS扩展

删除带有MDM的Mac连接器macOS扩展

使用MDM阻止系统扩展禁用

全磁盘访问

- 批准终端上早于1.18.0的连接器版本的全磁盘访问
- 批准终端的Cisco Orbital全磁盘访问
- 在终端上批准思科安全终端连接器1.18.0及更高版本的全磁盘访问
- 通过MDM批准连接器的全磁盘访问
- 批准使用MDM对Cisco Orbital进行全磁盘访问

MDM配置配置文件示例

- MacOS 10.15或更早版本的MDM配置示例

新建目录结构

- 版本1.14.0到1.16.2
- 版本1.18.0及更高版本

MacOS 11.0和Mac Connector 1.14.1的已知问题。

MacOS 10.15/11.0和Mac Connector 1.14.0的已知问题。

卸载系统扩展时的已知问题

Intune部署安装脚本

重新命名的Mac连接器（版本1.18.0及更高版本）

修订历史纪录

简介

本文档介绍管理员部署Mac连接器1.14及更高版本的最新更改和步骤。

MDM配置文件

强烈建议使用授予所需批准权限的MDM配置文件来部署Mac连接器。在安装、升级或删除Mac连接器之前，必须安装MDM配置文件，以确保识别所需的权限。如果MDM不可用，请参阅本文档后面的“已知问题”部分。

Advisories

Mac连接器版本1.14引入了一些需要注意的更改：

- 全磁盘访问批准
- 系统延期审批

需要Mac connector 1.14或更高版本才能确保macOS 11及更高版本上的终端保护。较旧的Mac连接器在这些版本的macOS上不起作用。

Mac连接器版本1.16引入了对Intel硬件上Cisco Orbital的支持。Orbital可以在策略中通过优势或高级层启用，并在启用后自动安装，并安装在支持的操作系统版本和支持的硬件上。Mac连接器版本1.20介绍了对Apple硅硬件上的Cisco Orbital（计划与Orbital Node 1.21一起发布）的支持就绪性。有关如何授予Orbital所需的额外全磁盘访问权限的详细信息，请参阅本文档的Cisco Orbital部分。

最低操作系统要求

思科安全终端Mac连接器1.14.0支持macOS版本：

- macOS 11，带macOS系统扩展。
- macOS 10.15.5及更高版本，带macOS系统扩展。
- macOS 10.15.0至macOS 10.15.4，带macOS内核扩展。
- macOS 10.14，带macOS内核扩展。

思科安全终端Mac连接器1.14.1支持macOS版本：

- macOS 11，带macOS系统扩展。
- 带macOS内核扩展的macOS 10.15。
- macOS 10.14，带macOS内核扩展。

安全终端Mac连接器版本1.16.0中引入了对英特尔硬件上的Cisco Orbital的支持。安全终端Mac连接器版本1.20.0中引入了对苹果硅硬件上Cisco Orbital的支持。

有关当前Mac连接器兼容性，请参阅操作系统兼容性表。

重要更改

Mac连接器1.14在以下三个方面引入了重要更改：

1.批准连接器使用的macOS扩展

2.全磁盘访问

3.新的目录结构

macOS 12引入了MDM选项，以允许删除连接器的macOS扩展而不提示输入用户密码。

批准Mac连接器macOS扩展

Mac连接器使用System Extensions或legacy Kernel Extensions来监控macOS版本所需的系统活动。在macOS 11上，System Extensions将替换macOS 11及更高版本中不受支持的旧版内核扩展。所有macOS版本都需要用户批准，才能允许任一类型的扩展运行。未经批准，某些连接器功能（例如访问时文件扫描和网络访问监控器）不可用。

Mac连接器1.14引入了两个新的macOS系统扩展：

1. 名为Secure Endpoint File Monitor（以前称为AMP Security Extension）的Endpoint Security扩展名，用于监控系统事件
2. 名为Cisco Secure Endpoint Filter（以前称为AMP Network Extension）的网络内容过滤器扩展，用于监控网络访问

包括两个传统内核扩展ampfileop.kext和ampnetworkflow.kext，以便在不支持新macOS系统扩展的旧macOS版本上进行向后兼容。

MacOS 11G及更高版本**需审批：

- 批准加载安全终端文件监视器
- 批准加载思科安全终端过滤器
- 允许思科安全终端过滤器过滤网络内容

** Mac连接器1.14.0版在macOS 10.15上也要求这些批准。对于Mac连接器1.14.1或更高版本，MacOS 10.15不再需要这些批准。

MacOS 10.14和MacOS 10.15所需的批准：

- 批准加载连接器内核扩展

这些批准在终端的macOS安全和隐私首选项中或通过移动设备管理(MDM)简档授予。

在终端上批准Mac Connector macOS扩展

系统和内核扩展从macOS安全和隐私首选项窗格中手动批准。



使用MDM批准Mac连接器macOS扩展

注意：macOS扩展不能通过MDM进行追溯性批准。如果在安装连接器之前未部署MDM配置

文件，则不会获得批准，并且需要通过以下方式之一进行额外干预：

1. 在已追溯部署管理配置文件的终端上手动批准macOS扩展。
2.将Mac连接器升级到比当前部署的连接器更新的版本。已追溯部署管理配置文件的终端在升级后识别管理配置文件，并在升级完成后获得批准。

安全终端扩展可以通过具有以下有效负载和属性的管理配置文件进行审批：

有效载荷	属性	价值
SystemExtensions	AllowedSystemExtensions	com.cisco.endpoint.svc.securityextension， com.cisco.endpoint.svc.networkextension
SystemExtensions	AllowedSystemExtensionType	EndpointSecurityExtension、NetworkExtension
SystemExtensions	AllowedTeamIdentifiers	DE8Y96K9QP

有效载荷	属性	价值
SystemPolicyKernelExtensions	AllowedKernelExtensions	com.cisco.amp.fileop、 com.cisco.amp.nke
SystemPolicyKernelExtensions	AllowedTeamIdentifiers	TDNYQP7VRK

有效载荷	属性	价值
WebContentFilter	AutoFilterEnabled	假
WebContentFilter	FilterDataProviderBundleIdentifier	com.cisco.endpoint.svc.networkextension
WebContentFilter	FilterDataProviderDesignatedRequirement	锚apple通用和标识符“com.cisco.endpoint.svc.networkextension”和（certificate leaf[field.1.2.840.113635.100.6.1.9] /*存在*/或certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.1.13] /*存在*/和certificate leaf[subject.OU] = DE96Y9QP）
WebContentFilter	FilterGrade	防火墙
WebContentFilter	过滤器浏览器	假
WebContentFilter	FilterPackets	假
WebContentFilter	FilterSockets	true
WebContentFilter	插件捆绑包ID	com.cisco.endpoint.svc
WebContentFilter	UserDefinedName	思科安全终端过滤器（如果连接器版本早于1.18.0，则为AMP网络扩展）

删除带有MDM的Mac连接器macOS扩展

macOS 12及更高版本允许使用RemovableSystemExtensions属性将macOS扩展标记为可移除，如

下所述。

⚠ 警告：当允许macOS扩展删除权限时，任何具有root权限的用户或进程都能够删除扩展，而无需提示输入用户密码。因此，仅当管理员要自动卸载连接器时，才必须使用RemovableSystemExtensions属性。

注意：无法通过MDM回溯删除macOS扩展。如果在卸载连接器之前未部署MDM配置文件，则不会授予macOS扩展删除批准，用户需要在连接器卸载过程中手动在终端上输入密码以删除macOS扩展。

安装具有RemovableSystemExtensions属性的管理配置文件时，可以在连接器卸载过程中删除安全终端扩展。RemovableSystemExtensions属性必须包含两个安全终端扩展的捆绑标识符：

有效载荷	属性	价值
SystemExtensions	RemovableSystemExtensions	com.cisco.endpoint.svc.securityextension， com.cisco.endpoint.svc.networkextension

使用MDM阻止系统扩展禁用

macOS 15及更高版本允许macOS扩展：

- 无法使用NonRemovableSystemExtensions属性移除。
- 无法使用NonRemovableFromUISystemExtensions属性在“系统设置”中禁用

注意：不可移除的密钥只能应用于macOS Sequoia 15设备。从旧版本的macOS更新到macOS Sequoia 15时，不应用此管理设置。

注意：NonRemovableSystemExtensions键不能与RemovableSystemExtensions键一起使用；配置文件安装失败。

注意：NonRemovableFromUISystemExtensions键可以与RemovableSystemExtensions键一起使用。

不可移除属性必须包含两个安全终端扩展的捆绑标识符：

有效载荷	属性	价值
SystemExtensions	NonRemovableFromUISystemExtensions	com.cisco.endpoint.svc.securityextension， com.cisco.endpoint.svc.networkextension

有效载荷	属性	价值
	NonRemovableSystemExtensions	com.cisco.endpoint.svc.securityextension， com.cisco.endpoint.svc.networkextension

全磁盘访问

macOS 10.14及更高版本需要经过批准，应用程序才能访问包含个人用户数据的文件系统部分（例如，联系人、照片、日历和其他应用程序）。 某些连接器功能（例如访问时文件扫描）未经批准无法扫描这些文件的威胁。

以前的Mac连接器版本要求用户授予对ampdaemon程序的全磁盘访问权限。Mac连接器1.14需要完全磁盘访问：

- 面向终端的AMP服务
- AMP安全扩展

Mac连接器1.16.0及更高版本需要额外的全磁盘访问：

- Cisco Orbital（在策略中启用），提供优势和Premier访问

Mac连接器1.18及更高版本要求完全磁盘访问：

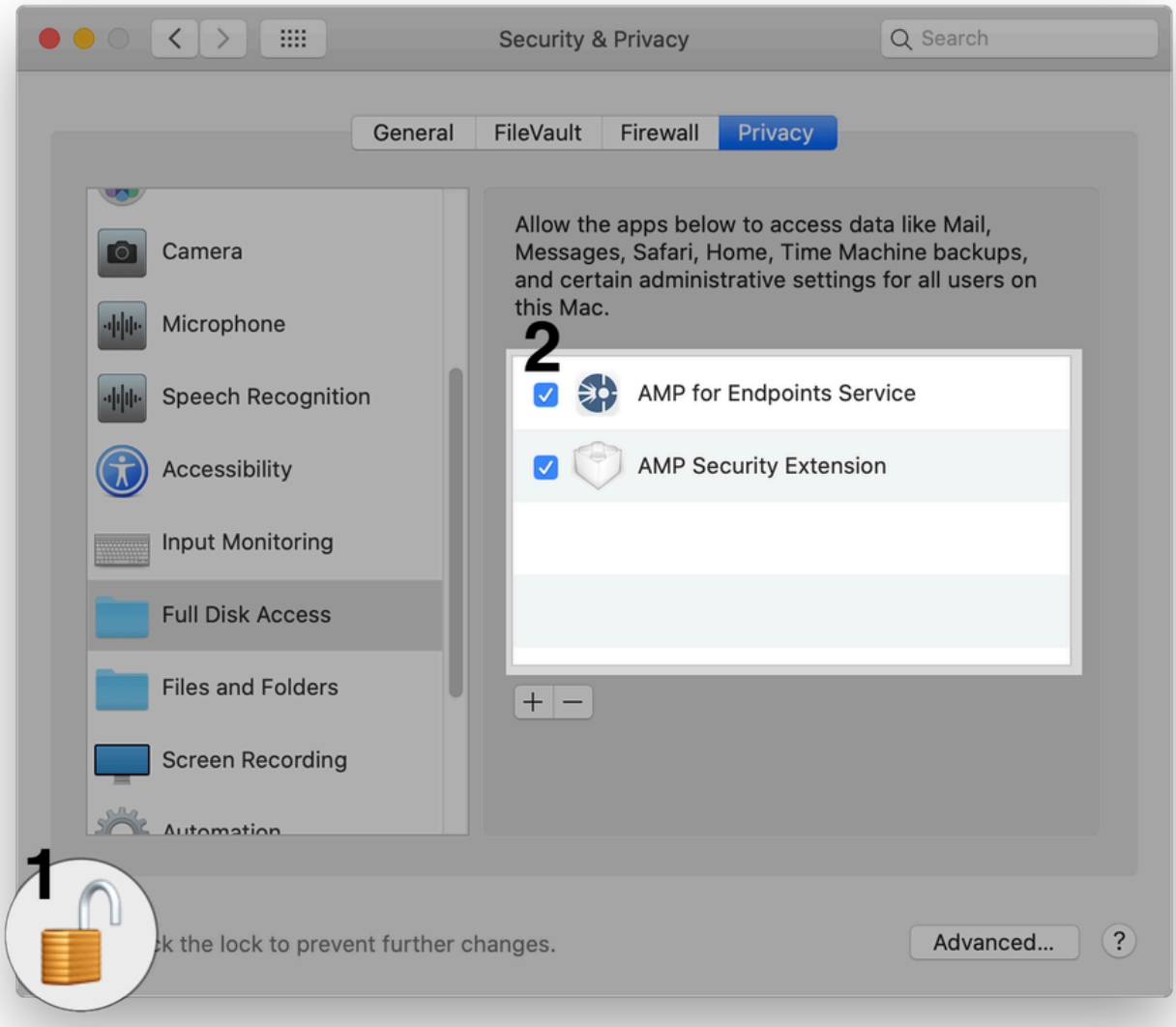
- 安全终端服务
- 安全终端系统监控器
- Cisco Orbital（在策略中启用Orbital）（提供优势和首要级别）

ampdaemon程序不再需要使用Mac连接器1.14版及更高版本进行全磁盘访问。

在终端的macOS安全和隐私首选项中或通过移动设备管理(MDM)配置文件授予全磁盘访问批准。

批准终端上早于1.18.0的连接器版本的全磁盘访问

可以从macOS安全和隐私首选项窗格手动批准全磁盘访问。



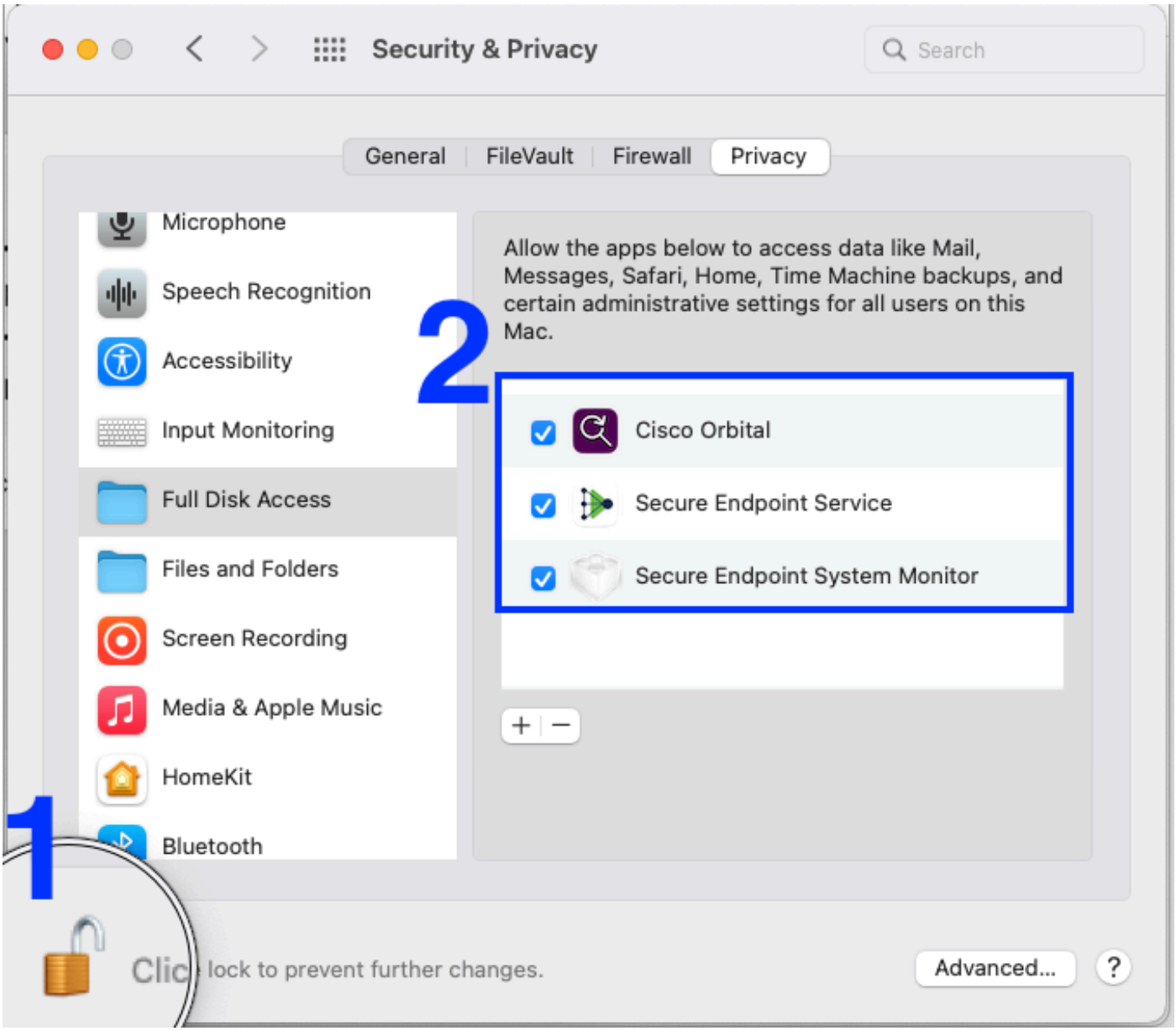
批准终端的Cisco Orbital全磁盘访问

可以从macOS安全和隐私首选项窗格手动批准全磁盘访问。



在终端上批准思科安全终端连接器1.18.0及更高版本的全磁盘访问

可以从macOS安全和隐私首选项窗格手动批准全磁盘访问。



通过MDM批准连接器的全磁盘访问

注意：macOS扩展不能通过MDM进行追溯性批准。如果在安装连接器之前未部署MDM配置文件，则不会获得批准，并且需要以下两种形式之一进行额外干预:

1. 在已追溯部署管理配置文件的终端上手动批准macOS扩展。
2.将Mac连接器升级到比当前部署的连接器更新的版本。已追溯部署管理配置文件的终端在升级后识别管理配置文件，并在升级完成后获得批准。

全磁盘访问由管理配置文件隐私首选项策略控制负载批准，该负载具有SystemPolicyAllFiles属性，该属性包含两个条目，一个用于安全终端服务（适用于终端的AMP服务适用于版本早于1.18.0的连接器），另一个用于安全终端系统监视器（适用于版本早于1.18.0的连接器的AMP安全扩展）：

有效载荷	属性	价值
隐私首选项策略控制：安全终端服务（面向终端的AMP服务）	允许	true
隐私首选项策略控制：安全终端服务（面向终端的AMP服务）	CodeRequirement	锚apple通用和标识符“com.cisco.endpoint.svc”和（certificate leaf[field.1.2.840.113635.100.6.1.9] /*存在*/或certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.13] /*存在*/和certificate leaf[subject.OU] = DE8Y96K9QP）
隐私首选项策略控制：安全终端服务（面向终端的AMP服务）	标识符	com.cisco.endpoint.svc
隐私首选项策略控制：安全终端服务（面向终端的AMP服务）	IdentifierType	捆绑包ID
隐私首选项策略控制：安全终端系统监控（AMP安全扩展）	允许	true
隐私首选项策略控制：安全终端系统监控（AMP安全扩展）	CodeRequirement	锚apple通用和标识符“com.cisco.endpoint.svc.securityextension”和（certificate leaf[field.1.2.840.113635.100.6.1.9] /*存在*/或certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.1.13] /*存在*/和certificate leaf[subject.OU] = DE96Y9QP）
隐私首选项策略控制：安全终端系统监控（AMP安全扩展）	标识符	com.cisco.endpoint.svc.securityextension
隐私首选项策略控制：安全终端系统监控（AMP安全扩展）	IdentifierType	捆绑包ID

对于包含已安装连接器版本1.12.7或更早版本的计算机的部署，需要以下附加条目才能授予对ampdaemon的完全磁盘访问:

描述	属性	价值
ampdaemon	允许	true
	CodeRequirement	标识符ampdaemon和anchor apple generic和certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.1.13] /*存在*/和certificate leaf[subject.OU] = TDNYQP7VRK
	标识符	/opt/cisco/amp/ampdaemon
	IdentifierType	路径

批准使用MDM对Cisco Orbital进行全磁盘访问

如果您的部署包括使用Cisco安全终端Mac连接器版本1.16.0或更高版本的计算机，在macOS 10.15或更高版本的计算机上，并且策略中启用了Orbital，则仍需要以下附加条目来授予这些计算机对Orbital的完全磁盘访问权限：

有效载荷	属性	价值
隐私首选项策略控制：Cisco Orbital	允许	true
隐私首选项策略控制：Cisco Orbital	CodeRequirement	锚apple通用和标识符“com.cisco.endpoint.orbital.app”和（certificate leaf[field.1.2.840.113635.100.6.1.9] /*存在*/或certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.1.13] /*存在*/和certificate leaf[subject.OU] = DE8Y96K9QP）
隐私首选项策略控制：Cisco Orbital	标识符	com.cisco.endpoint.orbal.app
隐私首选项策略控制：Cisco Orbital	IdentifierType	捆绑包ID

MDM配置配置文件示例

此MDM配置配置文件示例用作参考。

- 批准安全终端Mac连接器的系统扩展。
- 授予安全终端Mac连接器和轨道设备的全磁盘访问权限。
- 在卸载连接器时允许无提示卸载系统扩展。

⚠ 警告：当允许RemovableSystemExtensions权限时，任何具有root权限的用户或进程都能够删除系统扩展，而无需提示输入用户密码。因此，仅当管理员要自动卸载连接器时，才必须使用RemovableSystemExtensions属性。

```
<?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>F63OE2F3-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>F63OE2F3-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>
```

MacOS 10.15或更早版本的MDM配置示例

- 批准内核扩展并授予连接器全磁盘访问权限。
    - NOTE:M1和较新的Apple产品不能使用包含此配置的配置文件

```
<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>
```

新建目录结构

版本1.14.0到1.16.2

Mac连接器1.14对目录结构进行了两项更改：

1. 应用目录已从思科AMP重命名为面向终端的思科AMP。
2. 命令行界面(CLI)实用程序ampcli已从/opt/cisco/amp移至/Applications/Cisco AMP for Endpoints/AMP for Endpoints Connector.app/Contents/MacOS。目录/opt/cisco/amp包含指向新位置的ampcli程序的符号链接。

Mac连接器版本1.14.0到1.16.2的完整目录结构如下：

```
├── 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
```

版本1.18.0及更高版本

Mac连接器1.18引入了应用程序目录结构的更改：

1. 应用目录已从面向终端的思科AMP重命名为思科安全终端。

Mac连接器版本1.18.0及更高版本的完整目录结构如下：

```
├── 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
```

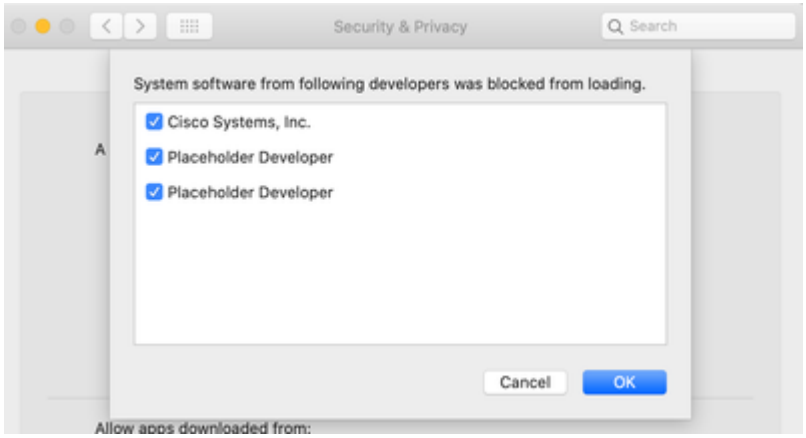
MacOS 11.0和Mac Connector 1.14.1的已知问题。

- 如果计算机上安装了四个或更多个网络内容过滤器，则故障10（加载内核模块或系统扩展时需要重启）的指导可能不正确。有关更多详细信息，请参阅Cisco安全终端Mac连接器故障文章。

MacOS 10.15/11.0和Mac Connector 1.14.0的已知问题。

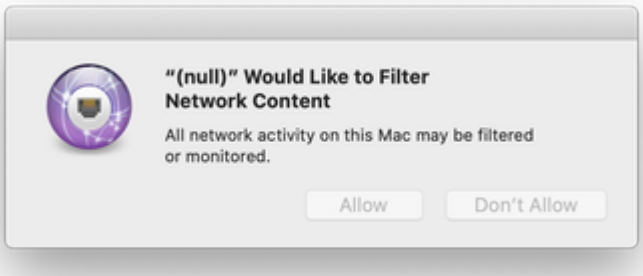
- Mac连接器引发的一些故障可能会意外发生。有关详细信息，请参阅Cisco安全终端Mac连接器故障文章。
  - 故障13（网络内容过滤器系统扩展过多）可能会在升级后出现。重新启动计算机可解决此情况下的故障。
  - 故障15（系统扩展需要全磁盘访问），在重新启动后由于macOS 11.0.0中的错误而可能发生。此问题在macOS 11.0.1中已解决。可以通过在macOS系统首选项的“安全和隐私”窗格中重新授予全磁盘访问权来解决故障。

- 在安装期间，当macOS请求允许运行Mac连接器系统扩展时，“安全和隐私”窗格可以将占位符开发程序显示为应用程序名称。这是由macOS 10.15中的漏洞引起的。选中“占位符开发程序”旁边的复选框，以允许Mac连接器保护计算机。

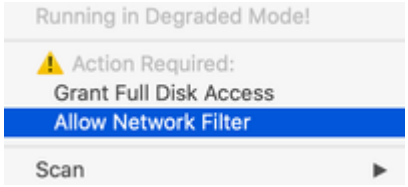


  - systemextensionsctl list命令可用于确定需要批准哪些系统扩展。此输出中状态为[激活等待用户]的系统扩展在前面显示的macOS首选项页面中显示为“占位符开发者”。如果首选项页面中显示两个以上的Placeholder Developer项，请卸载所有使用系统扩展名的软件（包括Mac连接器），以便不需要批准任何系统扩展，然后重新安装Mac连接器。Mac连接器系统扩展标识如下：
    - 网络扩展显示为com.cisco.endpoint.svc.networkextension。
    - 所示的终端安全扩展有com.cisco.endpoint.svc.securityextension。

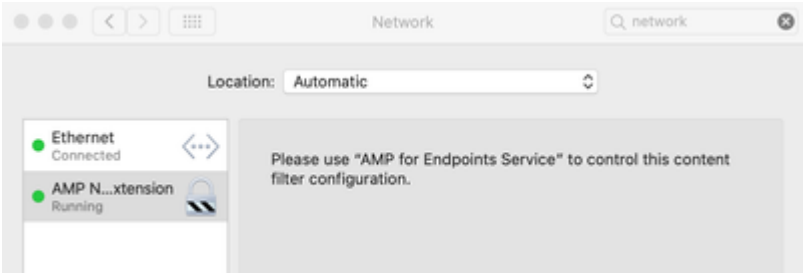
- 在安装期间，允许内容过滤器监视网络流量的提示可以作为应用程序名称显示(null)。这是由macOS 10.15中的漏洞引起的。用户需要选择允许以确保对计算机的保护。



- 如果由于选择Don't Allow而取消提示，则从“座席”图标的下拉菜单中选择“允许网络过滤器”

以再次打开提示。


- 启用后，安全终端网络扩展过滤器会列在Network Preferences页面上。



- 在macOS 11上，当执行从Mac连接器1.12到Mac连接器1.14的升级时，当连接器从内核扩展转换为新的系统扩展时，可以暂时引发故障4（系统扩展无法加载）。

卸载系统扩展时的已知问题

- 在macOS 12之前，或者未使用MDM时，当执行Mac连接器的卸载时，系统会提示用户输入其密码两次，以便可以卸载系统扩展。这是macOS的一个限制，通过添加本文档中描述的RemovableSystemExtensions MDM配置文件密钥，在macOS 12中进行了一些改进。

Intune部署安装脚本

- Microsoft维护的macOS上安装安全终端连接器的脚本托管在以下位置：

面向终端的思科AMP Mac连接器安装脚本

重新命名的Mac连接器（版本1.18.0及更高版本）

注意：对于低于1.18.0的连接器版本，现有MDM配置无需干预即可升级到连接器版本1.18.0及更高版本。有关详细信息，请参阅安全终端Mac重新换品牌。

修订历史纪录

2020年12月1日

- Mac连接器1.14.1不再使用macOS 10.15上的系统扩展。
- 有关终端检查哪些系统扩展需要Mac连接器1.14.0审批的附加指南。

2020年11月9日

- 已更正全磁盘访问代码要求MDM负载中的捆绑包ID。

2020年11月3日

- 1.14.0 Mac连接器的发布日期为2020年11月。
- 1.14.0 Mac连接器使用System Extensions with macOS 10.15.5及更高版本。以前是10.15.6。
- 添加了已知问题部分。
- 更新的目录结构大纲。

2021年6月3日

- 添加了向Cisco Orbital授予全磁盘访问权限的说明。

2021年10月13日

- 添加删除带有MDM的Mac连接器macOS扩展部分。
- 为“卸载系统扩展”部分添加了“已知问题”。

2022年2月25日

- 重新命名

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。