使用带有Umbrella模块的JAMF将CSC部署到macOS

目录

简介

本文档介绍如何使用JAMF将带有Umbrella模块的Cisco安全客户端部署到托管macOS设备。

先决条件

要求

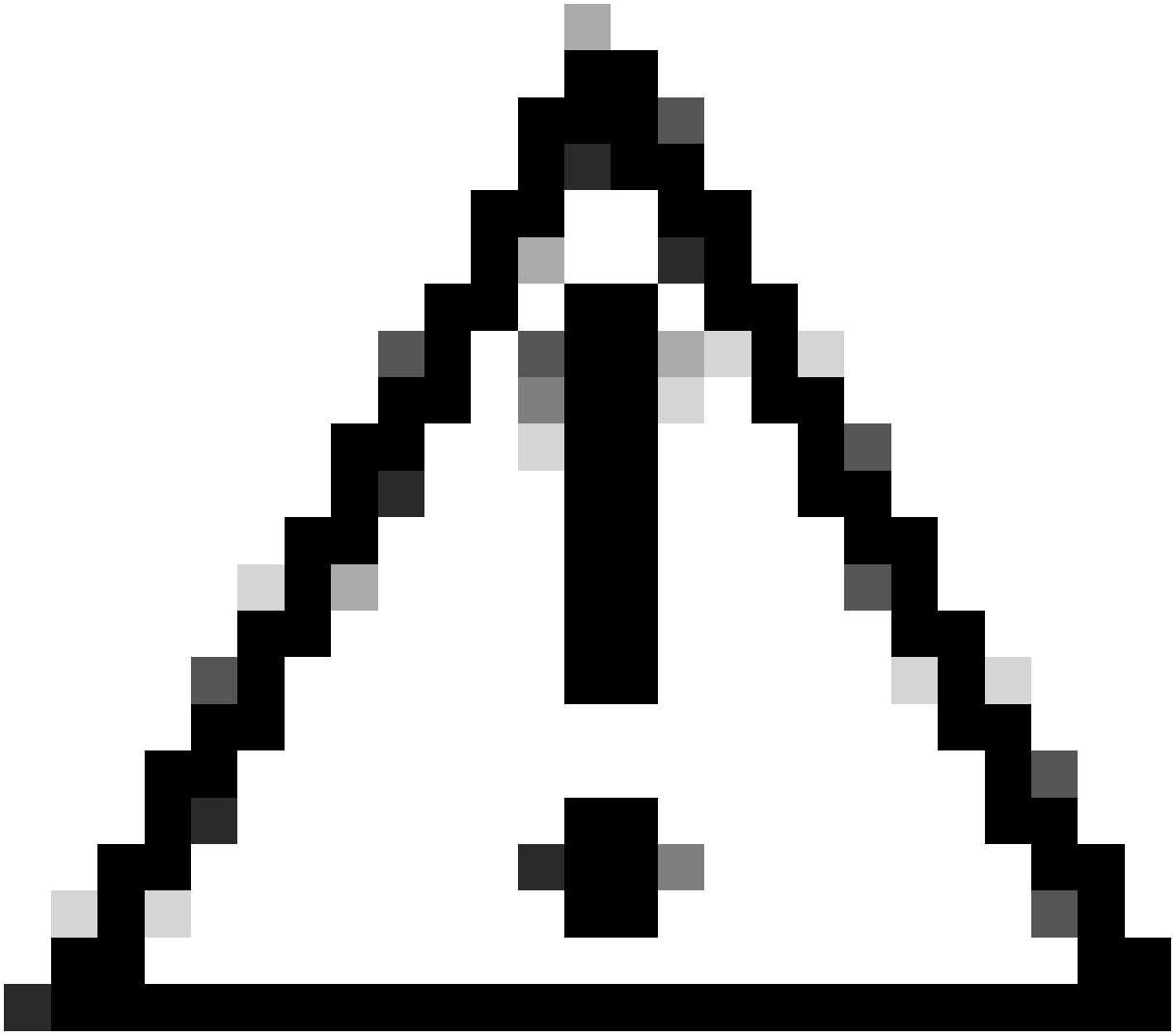
Cisco 建议您了解以下主题：

- macOS设备必须由JAMF管理。
- 有关macOS的MDM注册说明，请参阅JAMF文档。

使用的组件

本文档中的信息基于Cisco安全客户端。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。



警告：本文自2025年2月1日起提供。Cisco Umbrella支持不保证这些说明在此日期之后有效，并且可能会根据JAMF和Apple的更新进行更改。

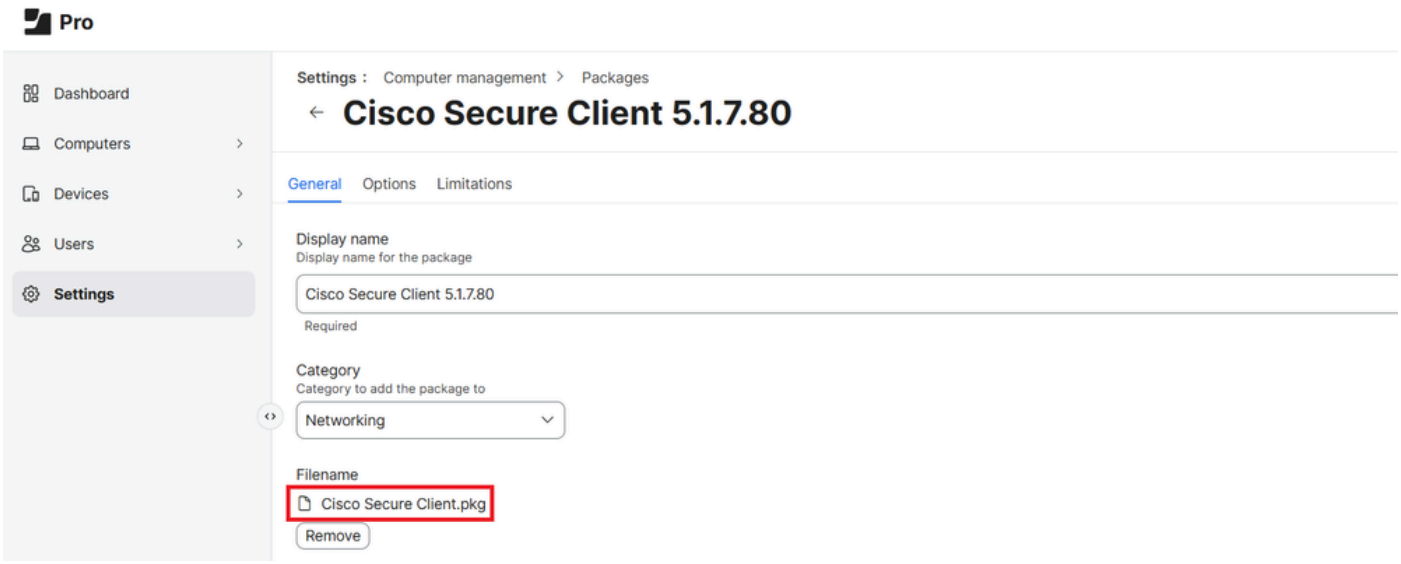
上传安装包(PKG)

1.从Umbrella控制面板的Deployments > Roaming Computers > Roaming Client > Pre-Deployment Package > macOS下载Cisco Secure Client DMG。

2.登录您的JAMF Pro云实例。

3.导航到“设置”>“计算机管理”>“包”>“新建”。

4.上传从您从Umbrella控制面板下载的DMG包中提取的PKG。

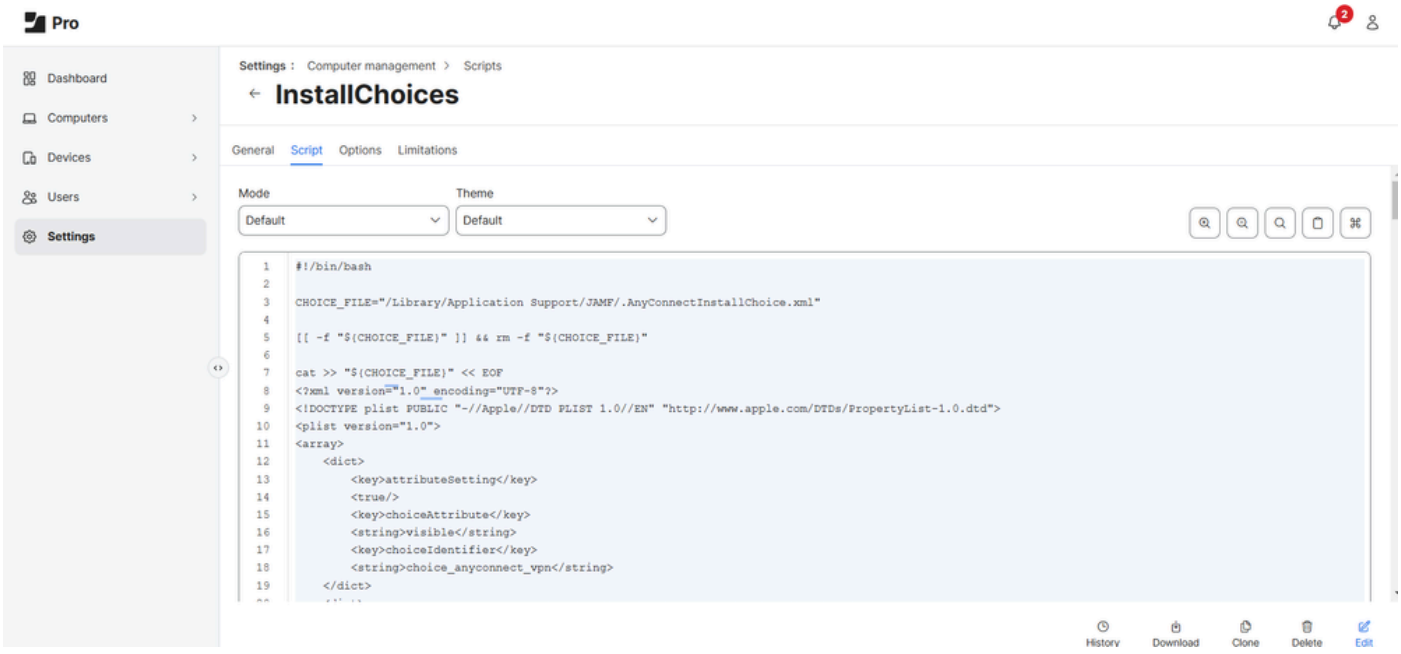


添加配置和模块选择脚本

1.转到设置>计算机管理>脚本，然后添加此脚本以控制部署过程中安装哪些模块。

2.您可以控制安全客户端模块的安装，方法是将模块设置为0以跳过该模块，或设置为1，以在PKG配置为默认安装所有模块时安装该模块。

- 您可以从Umbrella文档获取示例XML文件：自定义Cisco安全客户端的macOS安装
- Umbrella还将“installchoices”脚本添加到此github链接中。在本示例中，核心VPN、Umbrella和DART模块设置为1，可以包括在安全客户端安装中。



3.导航到设置>计算机管理>脚本，然后添加此脚本，以便它创建Cisco Secure Client所需的配置文件Orginfo.json。

- 直接从Umbrella控制面板下载模块配置文件，然后将Organization ID、Fingerprint和User

ID添加到脚本：

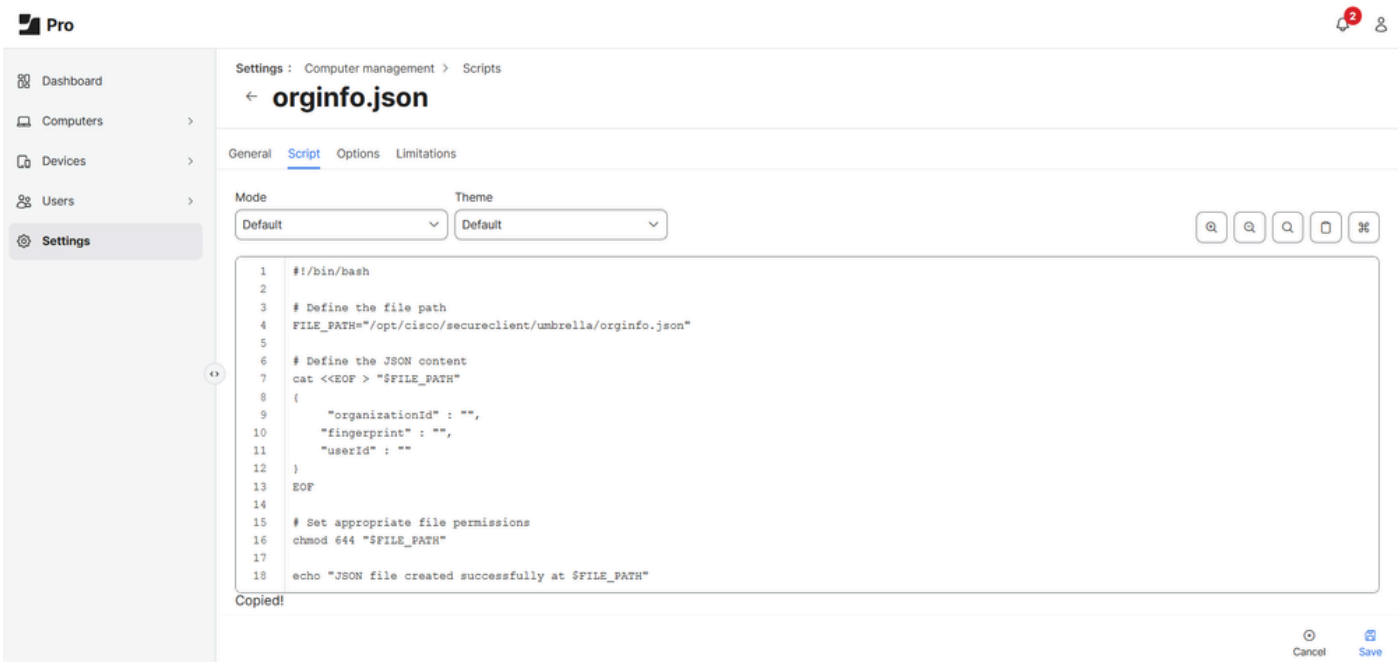
```
#!/bin/bash

# Define the file path
FILE_PATH="/opt/cisco/secureclient/umbrella/orginfo.json"

# Define the JSON content
cat <<EOF > "$FILE_PATH"
{
"organizationId" : "OrgID",
"fingerprint" : "Fingerprint",
"userId" : "UserID"
}
EOF

# Set appropriate file permissions
chmod 644 "$FILE_PATH"

echo "JSON file created successfully at $FILE_PATH"
```



34452906673812

创建JAMF策略

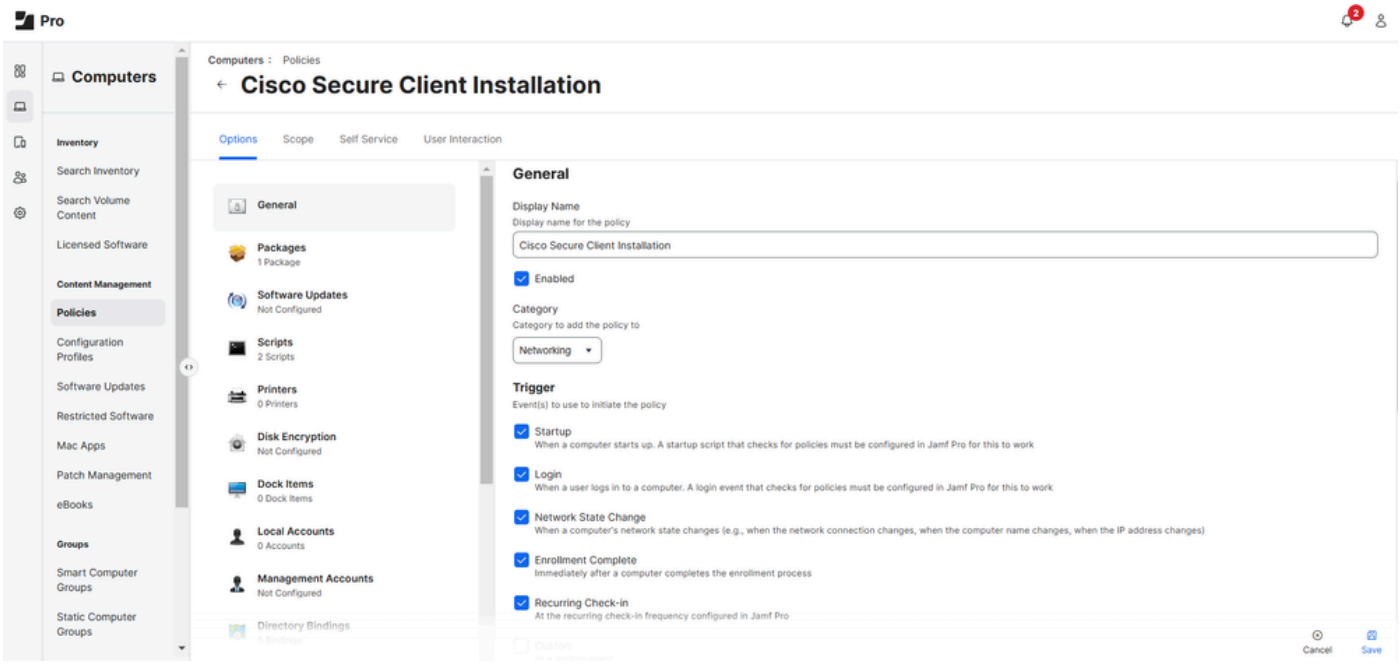
JAMF策略用于确定如何和何时推出带有Umbrella模块的思科安全客户端。

1.导航到计算机>内容管理>策略>新建。

2.为策略分配唯一的名称，并选择所需的Category和Trigger事件（例如，执行此策略时）。

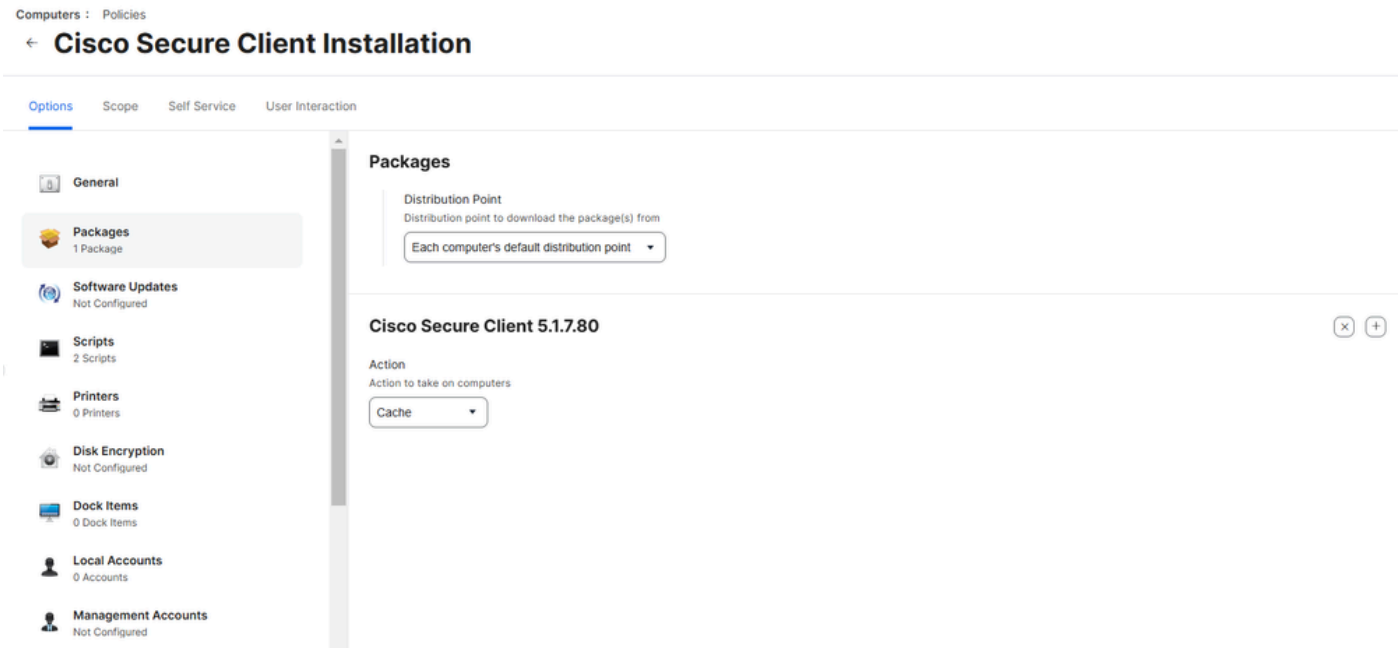
3.（可选）您还可以配置可在“自定义”下执行的自定义命令。用于执行和运行此策略的命令如下所示：

```
sudo jamf policy -event <custom_command>
```

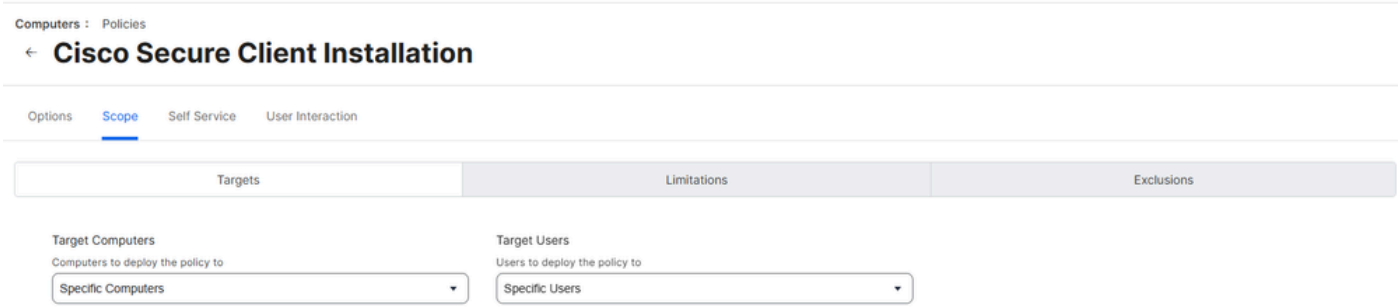


4.选择Packages > Configure，然后选择Cisco Secure Client软件包旁边的Add。

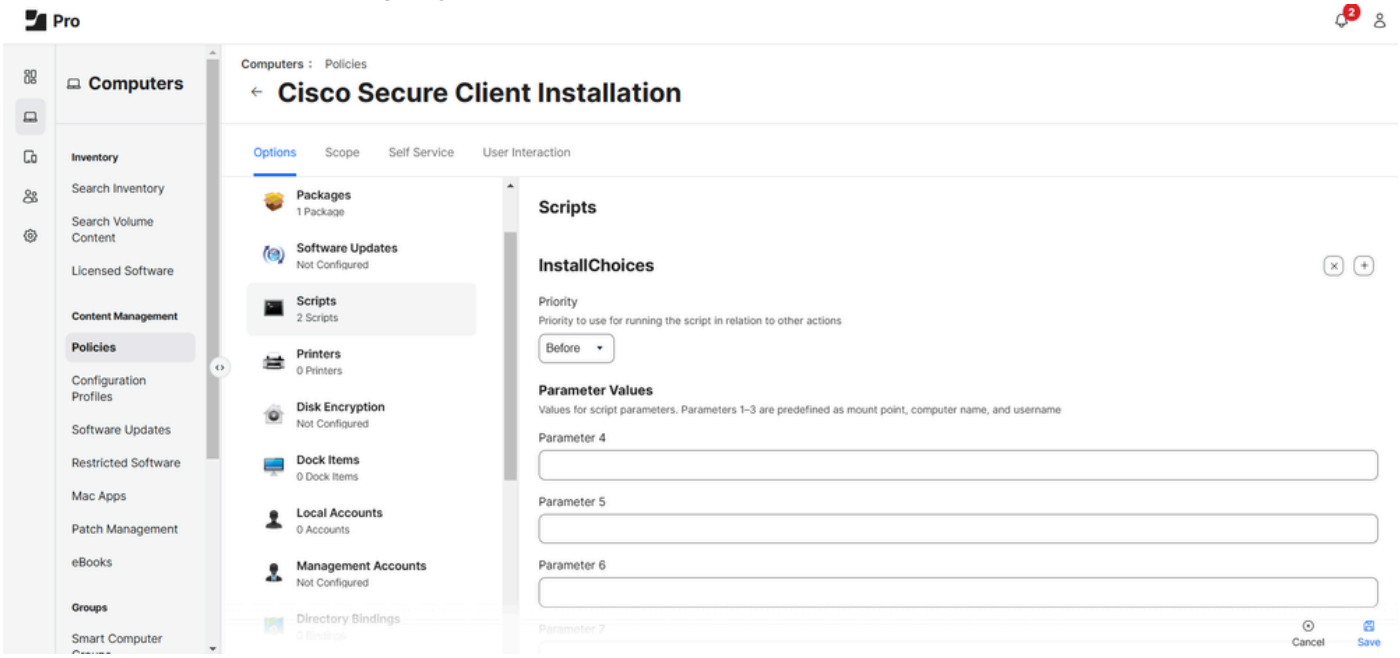
- 在分发点下，选择每台计算机的默认分发点。
- 在操作下，选择缓存。

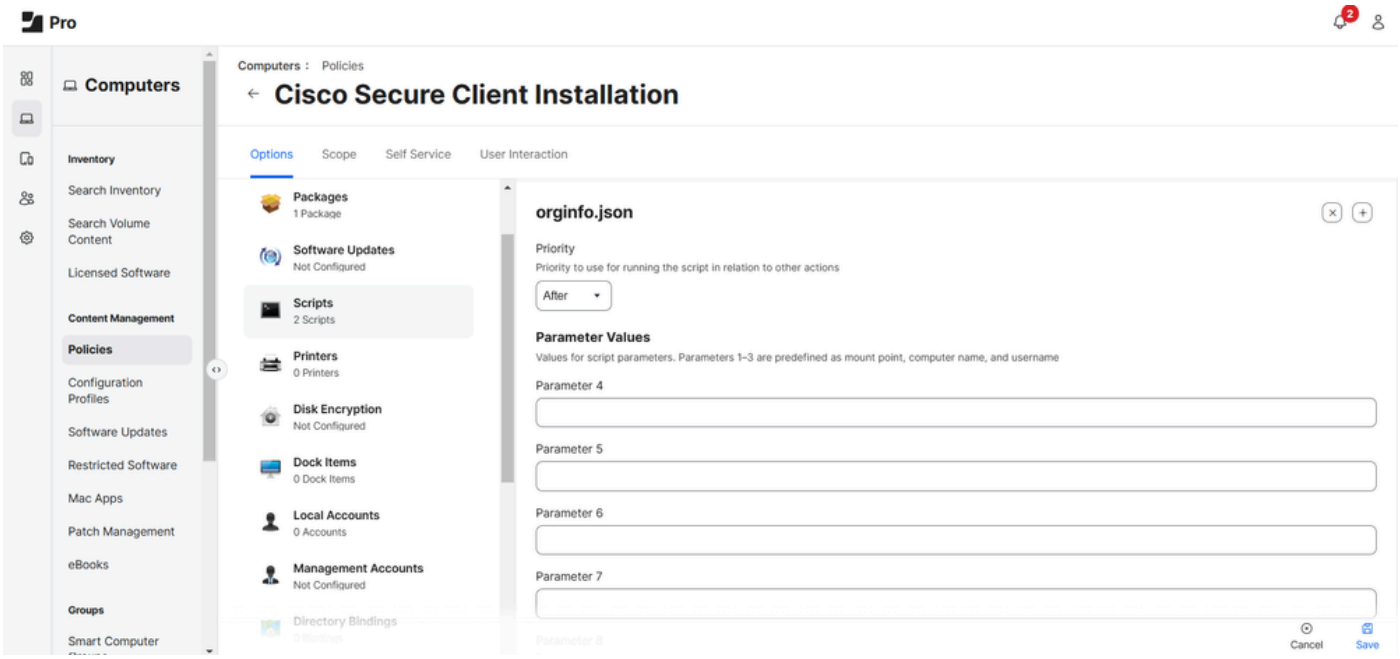


5.定义要部署的设备或用户的范围，然后选择保存。



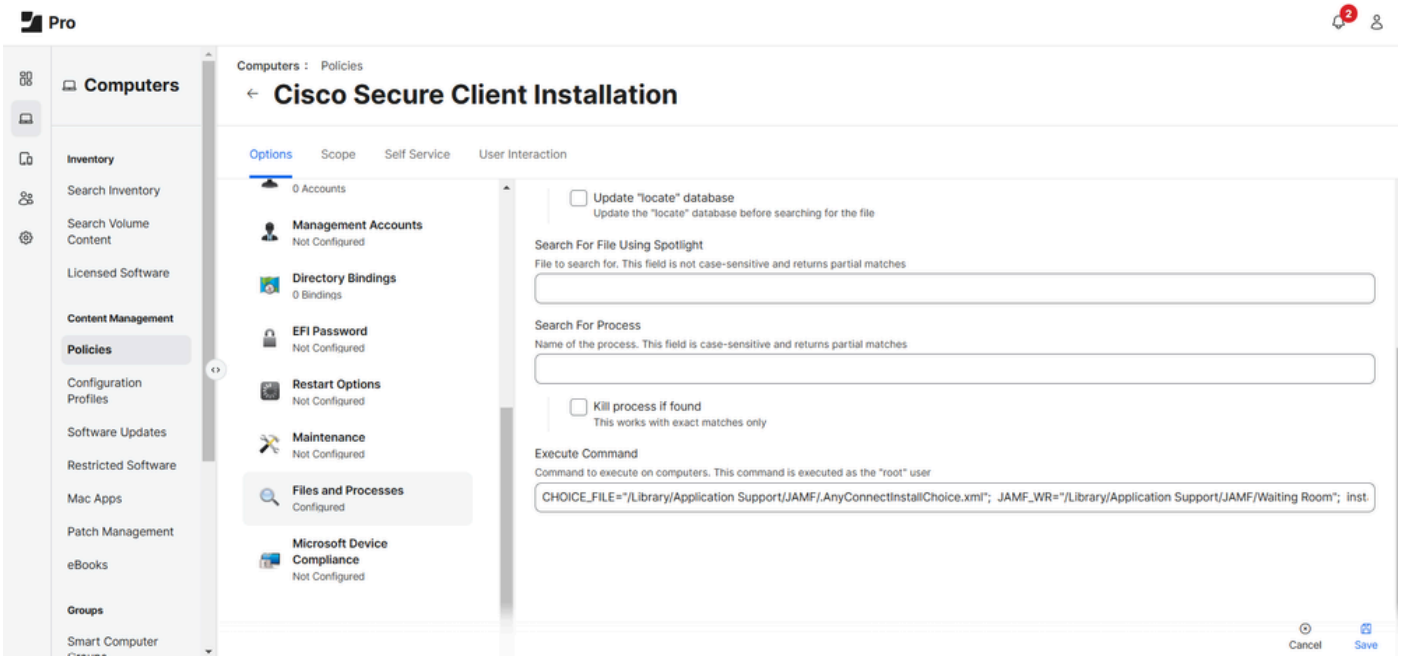
6.添加和脚InstallChoices本，**orginfo.json** 并为它们指定相对于其他操作运行脚本的优先级。





7.执行以下命令在设备上安装带有选定模块的Cisco安全客户端软件包：

```
CHOICE_FILE="/Library/Application Support/JAMF/.AnyConnectInstallChoice.xml"; JAMF_WR="/Library/Applica
```



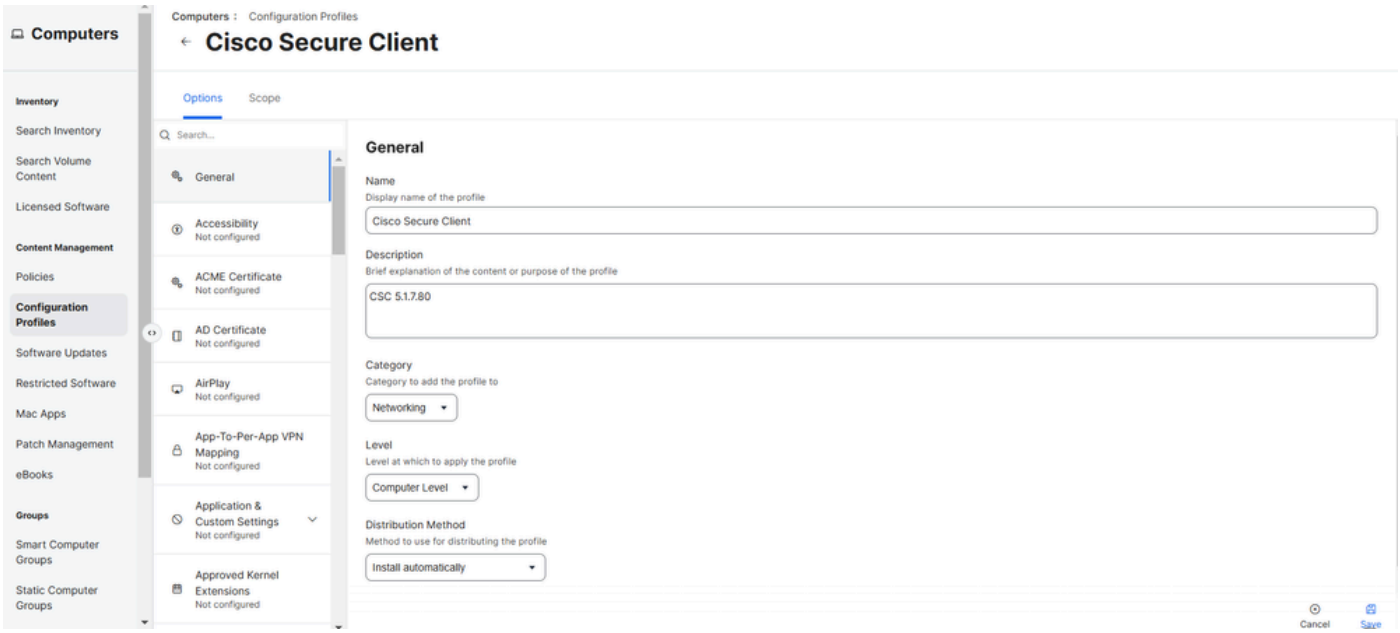
配置系统扩展的无提示安装

接下来，使用JAMF配置并允许Cisco安全客户端所需的系统扩展，以便带Umbrella模块的Cisco安全客户端能够正常运行而无需用户交互。

1.转到计算机>内容管理>配置文件>新建。

2.为配置文件指定唯一的名称，然后选择Category 和Distribution Method。

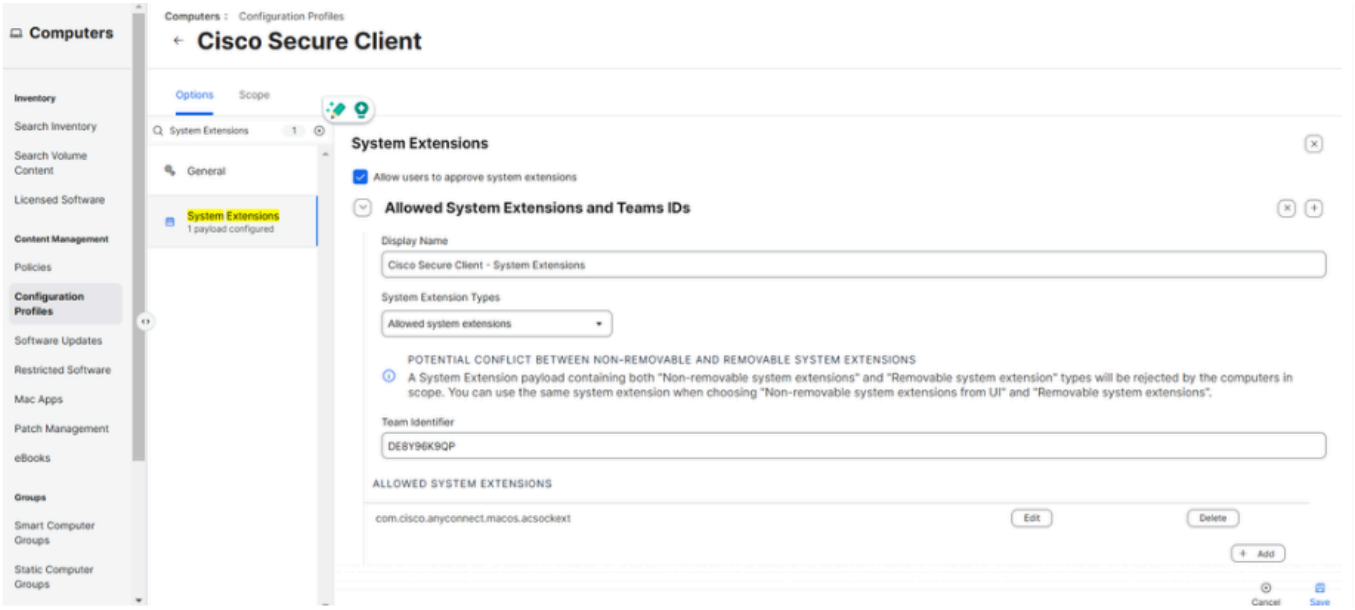
3.将EnsureLevel设置为Computer Level。



4.搜索System Extensions > Configure。输入以下值：

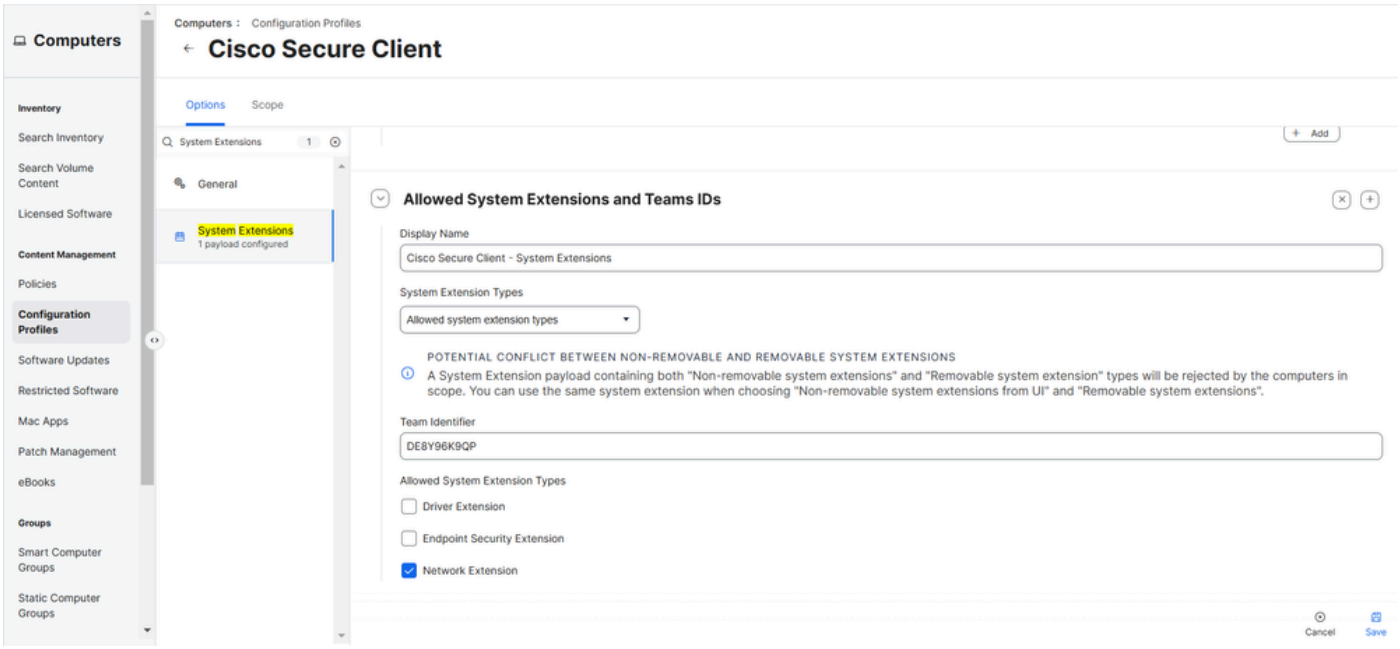
- 显示姓名：思科安全客户端 — 系统扩展

- 系统扩展类型：允许的系统扩展
- 组标识符：DE8Y96K9QP
- 允许的系统扩展：com.cisco.anyconnect.macos.acsockext，然后选择Save。



5.选择允许组ID和系统扩展旁边的+图标以添加另一个系统扩展。然后，输入以下值：

- 显示姓名：思科安全客户端 — 系统扩展
- 系统扩展类型：允许系统扩展类型
- 组标识符：DE8Y96K9QP
- 允许系统扩展类型：网络扩展



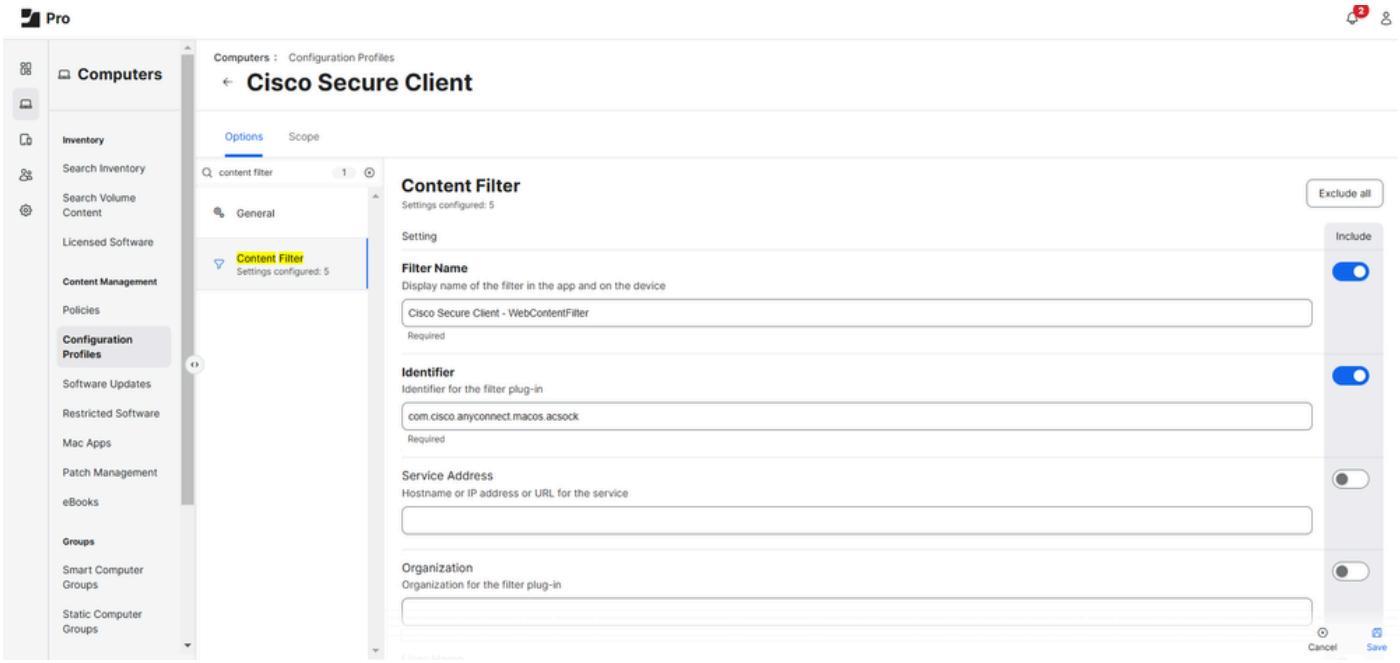
为内容过滤器配置静默安装

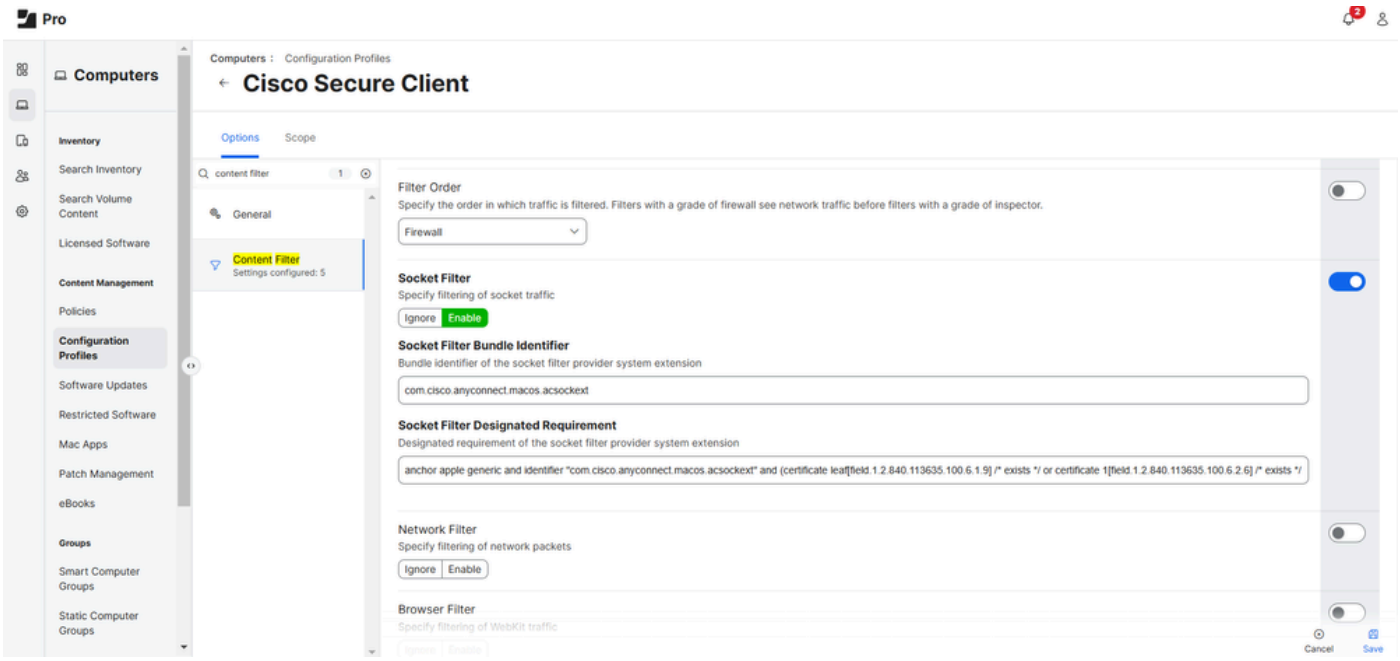
接下来，为内容过滤器配置静默安装，该安装将思科安全客户端与Umbrella模块的Socket Filter相关联：

1.搜索内容过滤器。启用这些字段并填写其各自的值：

- 过滤器名称:思科安全客户端 — WebContentFilter
- 标识符:com.cisco.anyconnect.macos.acsock
- 套接字过滤器：启用
- 套接字过滤器捆绑包标识符：com.cisco.anyconnect.macos.acsockext
- 套接字过滤器指定要求：

  anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext"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)





2.在自定义数据下，选择添加五次，然后输入以下值：

密钥	价值

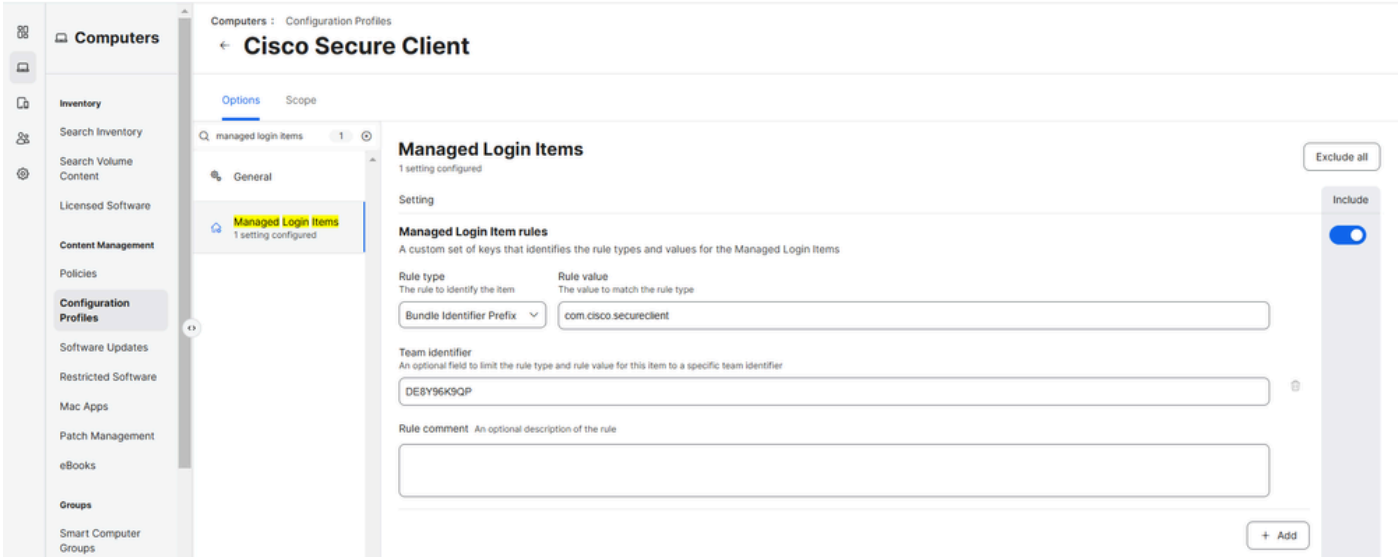
AutoFilterEnabled	假
过滤器浏览器	假
FilterSockets	true
FilterPackets	假
FilterGrade	防火墙

配置托管登录项目

为带有Umbrella模块的Cisco安全客户端配置托管登录项目可确保Cisco安全客户端在设备启动时启动。

要配置，请搜索Managed Login Items，并使用以下值配置字段：

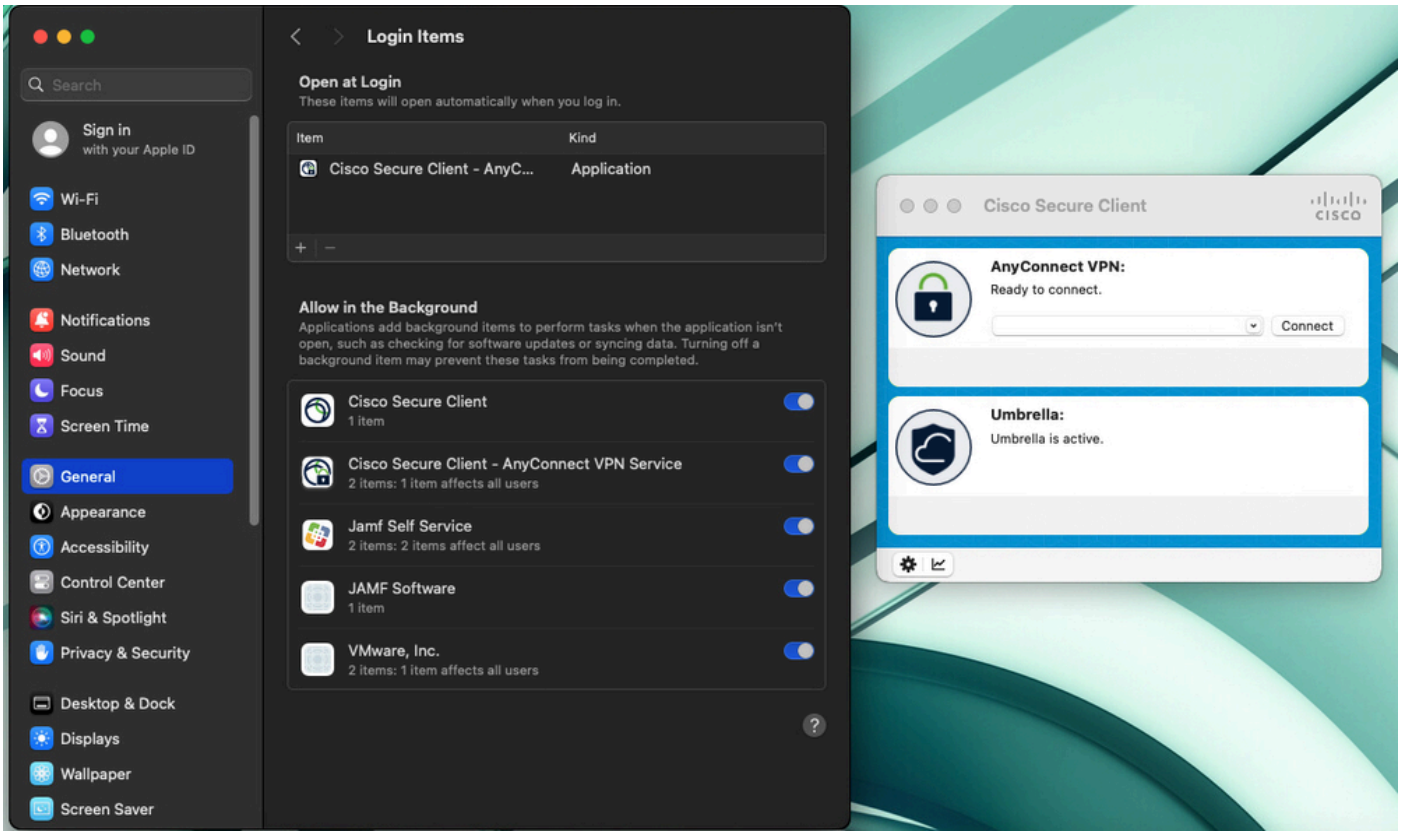
- 规则类型:捆绑包标识符前缀
- 规则值：com.cisco.secureclient
- 组标识符：DE8Y96K9QP

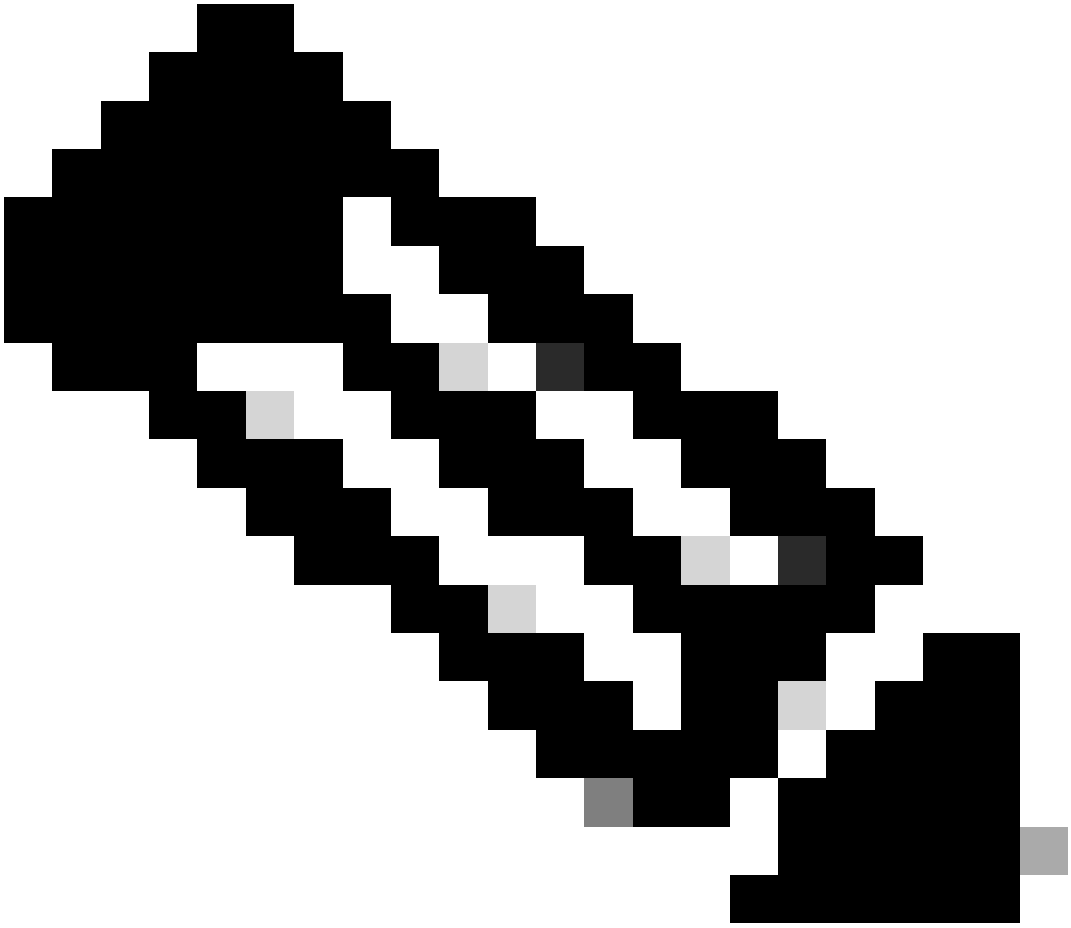


分配范围和推送部署

1.定位至范围，然后定义设备或用户的范围。

2.激活您在创建JAMF策略第2步中配置的一个触发器时，可以将Cisco Secure Client with Umbrella模块推出到所需的macOS设备。或者，您可以通过JAMF的自助服务门户推送此内容。


Search
Sign in
with your Apple ID
Wi-Fi
Bluetooth
Network
Notifications
Sound
Focus
Screen Time
General
Appearance
Accessibility
Control Center
Siri & Spotlight
Privacy & Security
Desktop & Dock
Displays
Wallpaper
Screen Saver
Login Items
Open at Login
These items will open automatically when you log in.
Item
Kind
Cisco Secure Client - AnyC...
Application
Allow in the Background
Applications add background items to perform tasks when the application isn't open, such as checking for software updates or syncing data. Turning off a background item may prevent these tasks from being completed.
Cisco Secure Client
1 item
Cisco Secure Client - AnyConnect VPN Service
2 items: 1 item affects all users
Jamf Self Service
2 items: 2 items affect all users
JAMF Software
1 item
VMware, Inc.
2 items: 1 item affects all users
Cisco Secure Client
AnyConnect VPN:
Ready to connect.
Connect
Umbrella:
Umbrella is active.



注意：即使用户尝试在系统设置(网络(Network)>过滤器(Filter))中禁用DNS代理或透明代理，默认情况下，它会自动重新启用，因为内容过滤器通过JAMF启用，如本文所述，且无法禁用。

配置macOS防火墙例外

如果macOS防火墙设置为Block all incoming connections，还必须将Cisco Secure Client及其组件添加到其例外列表中：

1.导航到计算机>内容管理>配置文件。

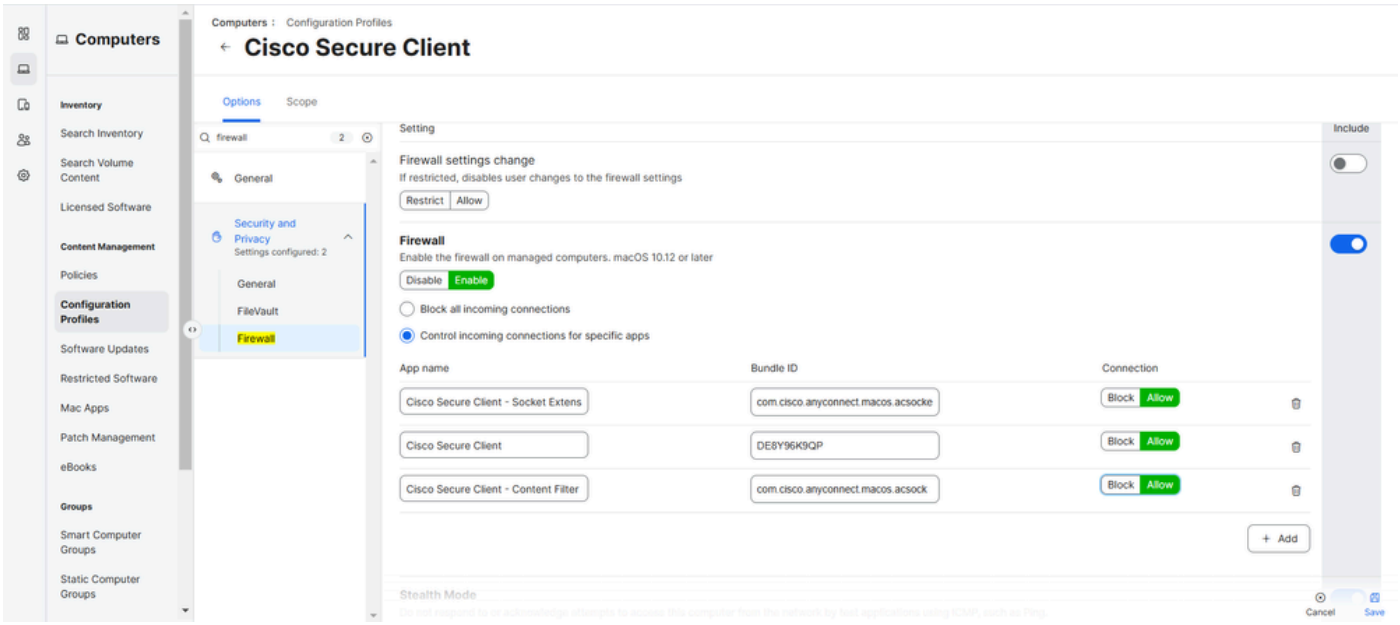
2.选择您的Cisco Secure Client配置文件并找到Security and Privacy。

3.使用以下设置进行配置：

- 防火墙：启用 — 控制特定应用的传入连接

应用名称	捆绑包ID

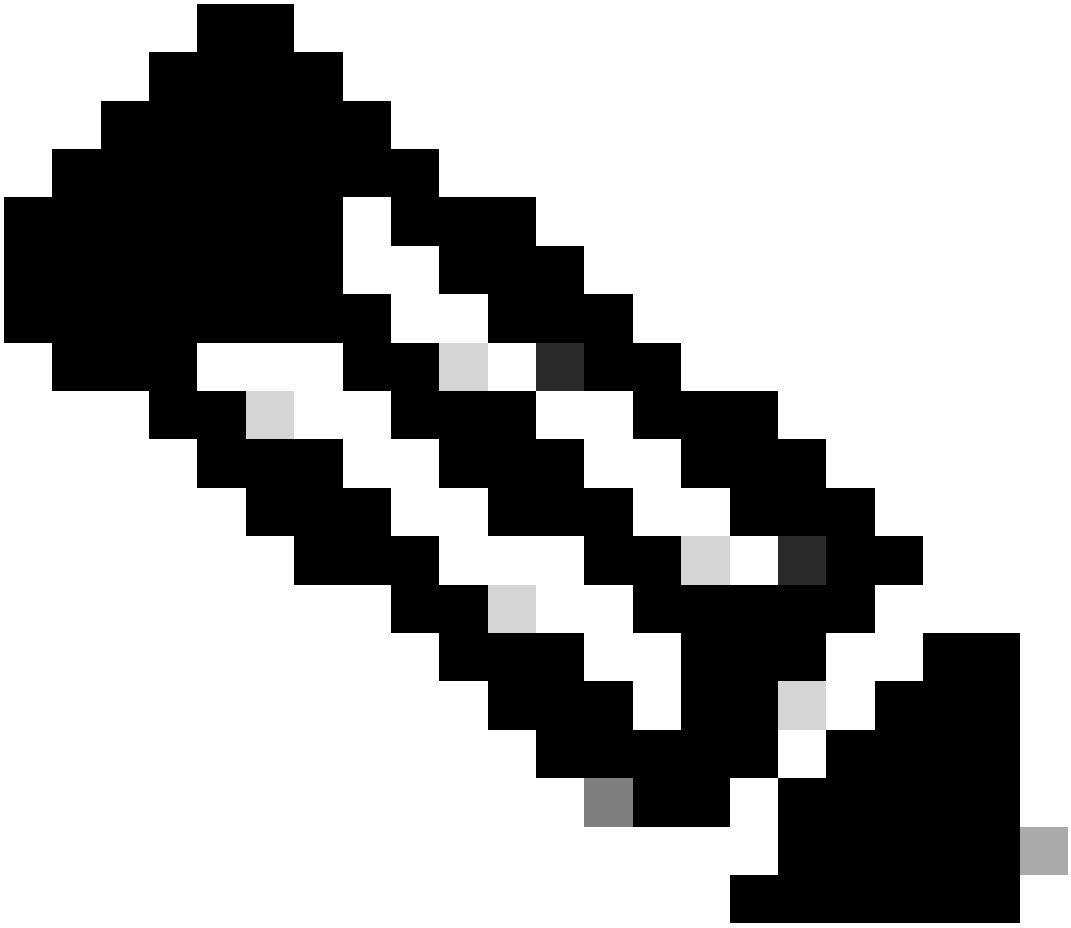
思科安全客户端 — 套接字扩展	com.cisco.anyconnect.macos.acsockext
思科安全客户端	DE8Y96K9QP
思科安全客户端 — 内容过滤器	com.cisco.anyconnect.macos.acsock



4.选择保存。

5.如果系统提示重分发选项，请选择分发到所有，立即将更改推送到所需的macOS设备。

部署Cisco Umbrella根证书



注意：此步骤仅适用于新部署的思科安全客户端或以前未部署Cisco Umbrella根证书的设备。如果您从Umbrella漫游客户端或Cisco AnyConnect 4.10客户端进行迁移，并且/或者以前已部署了Cisco Umbrella根证书，则可以跳过此部分。

从Umbrella控制面板中的Policies > Root Certificates下载Cisco Umbrella Root Certificate。

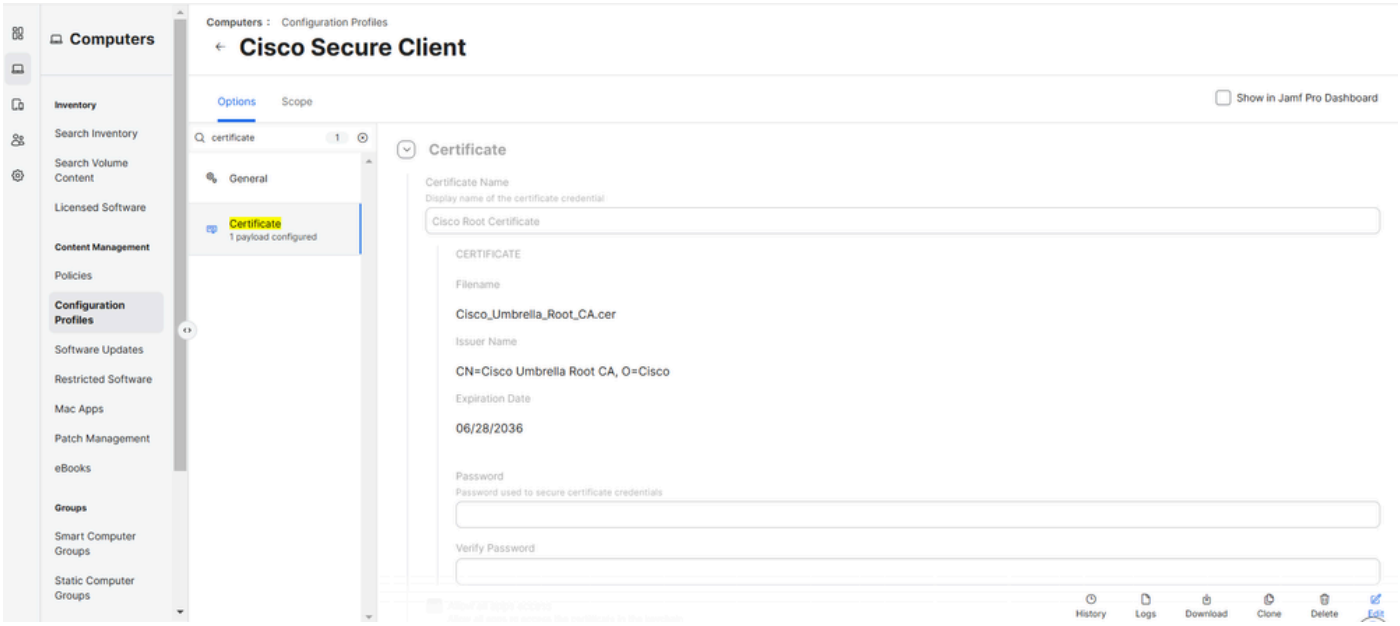
1.在Policies > Root Certificate下的Umbrella控制面板中，下载Cisco Umbrella Root Certificate。

2.在JAMF中，导航到计算机>配置文件> Cisco安全客户端>编辑。

3.搜索证书>配置。为其指定唯一名称。

4.在Select Certificate Option下，选择Upload并上传您之前在第1步中下载的Cisco Umbrella根证书。

5.确保您不在此处配置密码，然后选择保存。



6.如果系统提示重分发选项，请选择分发到所有，立即将更改推送到所需的macOS设备。

确认

要验证带Umbrella模块的Cisco安全客户端是否正常工作，请浏览到https://policy-debug.checkumbrella.com或运行此命令：

```
dig txt debug.opendns.com
```

任一输出都必须包含与Umbrella组织相关的独特信息，例如您的OrgID。

MacOS 14.3的解决方法

对于使用Cisco安全客户端5.1.x的macOS 14.3（或更高版本），如果遇到“VPN客户端代理无法创建进程间通信仓库”：

1.在JAMF中，导航到设置>计算机管理>脚本>新建。

2.为其指定唯一的名称并定义类别。

3.定位至脚本选项卡，然后添加以下内容：

```
#!/bin/bash

# Create variables with the folder path and Cisco Secure Client app services

app_name="Cisco Secure Client - AnyConnect VPN Service.app"
app_path="/opt/cisco/secureclient/bin/$app_name"
```

```
# Checks if the Cisco Secure Client services is already running

app_process=$(pgrep -fl "$app_name")

# If not, launch the Cisco Secure Client app services via "open -a" command

if [ -z "$app_process" ]; then
    open -a "$app_path"
else
    exit 0
fi
```

4.在Options下，确保Priority设置为After。此bash脚本通过从`pgrep -fl`返回进程ID的预期输出来检查Cisco安全客户端 — AnyConnect VPN service.app是否正在运行。

- 如果返回空输出，则可以确认`Cisco Secure Client - AnyConnect VPN service.app`未运行，并且脚本将执行以启动Cisco Secure Client核心服务，这是使Umbrella模块正确运行所必需的。

自动更新

思科已决定从Umbrella控制面板中扩展自动更新支持，以包含从安全客户端5.1.6.103(MR6)开始的安全客户端。 今后，如果已在Umbrella控制面板中配置了自动更新，已升级到至少思科安全客户端5.1.6 MR6的客户可以自动更新到较新的版本。

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）。