Implante CSC no macOS usando JAMF com o módulo Umbrella

Contents

Introdução

Este documento descreve como implantar o Cisco Secure Client com o módulo Umbrella em dispositivos macOS gerenciados usando JAMF.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

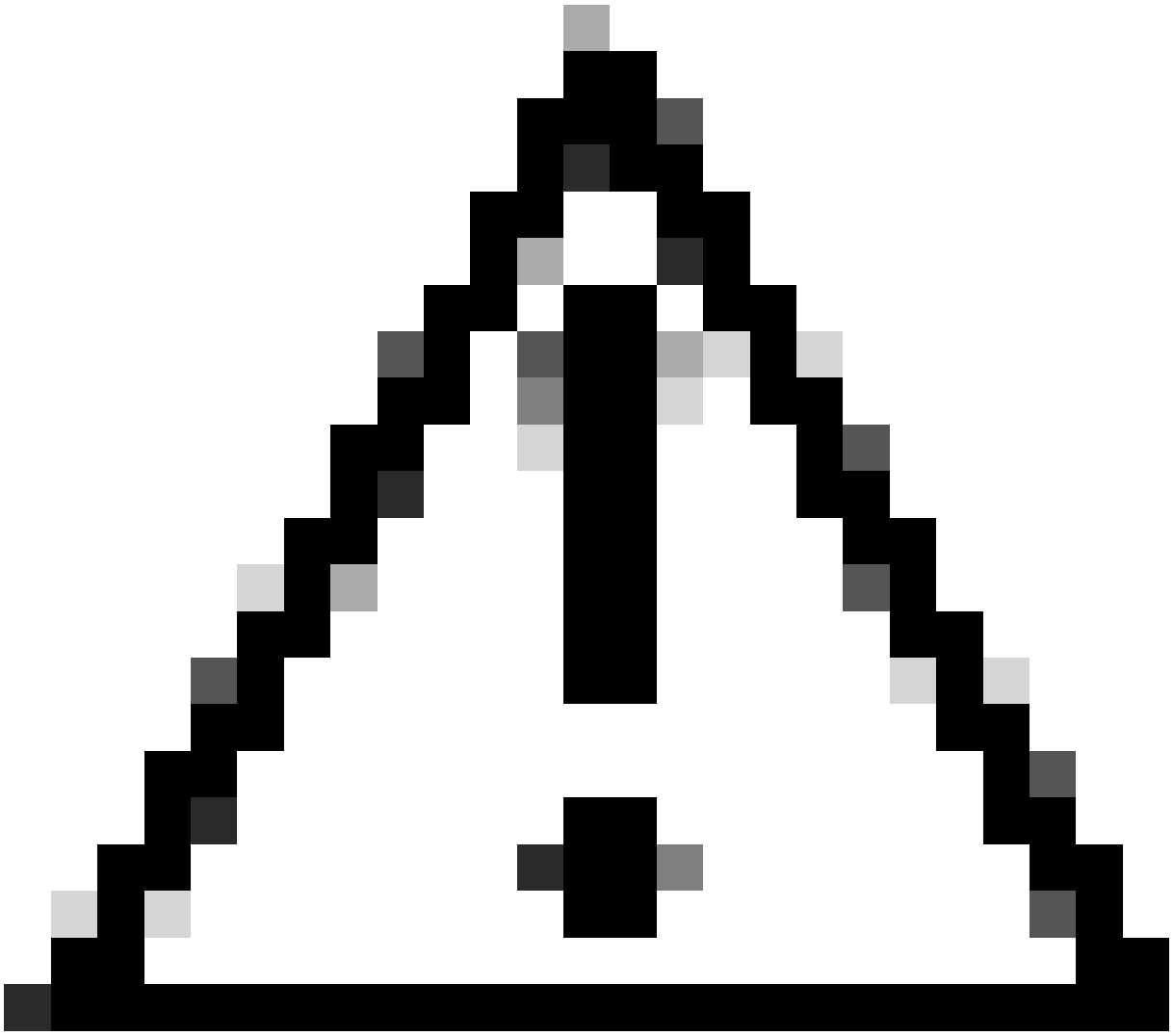
- os dispositivos macOS devem ser gerenciados pelo JAMF.
- Para obter instruções de inscrição de MDM para macOS, consulte a documentação JAMF.

Componentes Utilizados

As informações neste documento são baseadas no Cisco Secure Client.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma

configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.



Caution: Este artigo é fornecido como está a partir de 1º de fevereiro de 2025. O Cisco Umbrella Support não garante que essas instruções sejam válidas após essa data e estejam sujeitas a alterações com base nas atualizações da JAMF e da Apple.

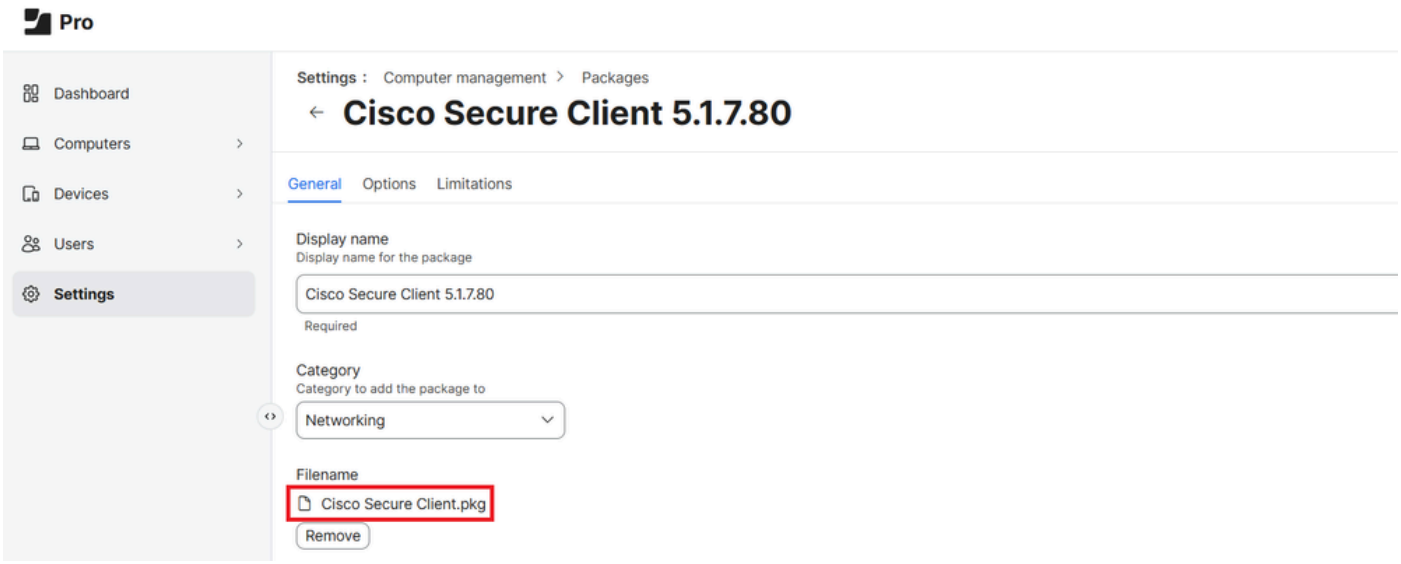
Carregar o pacote de instalação (PKG)

1. Baixe o Cisco Secure Client DMG no painel Umbrella em Implantações > Computadores em Roaming > Cliente em Roaming > Pacote Pré-implantação > macOS.

2. Inicie sessão na sua instância de nuvem do JAMF Pro.

3. Navegue até Configurações > Gerenciamento do Computador > Pacotes > Novo.

4. Carregue o PKG extraído do pacote DMG baixado do painel do Umbrella.

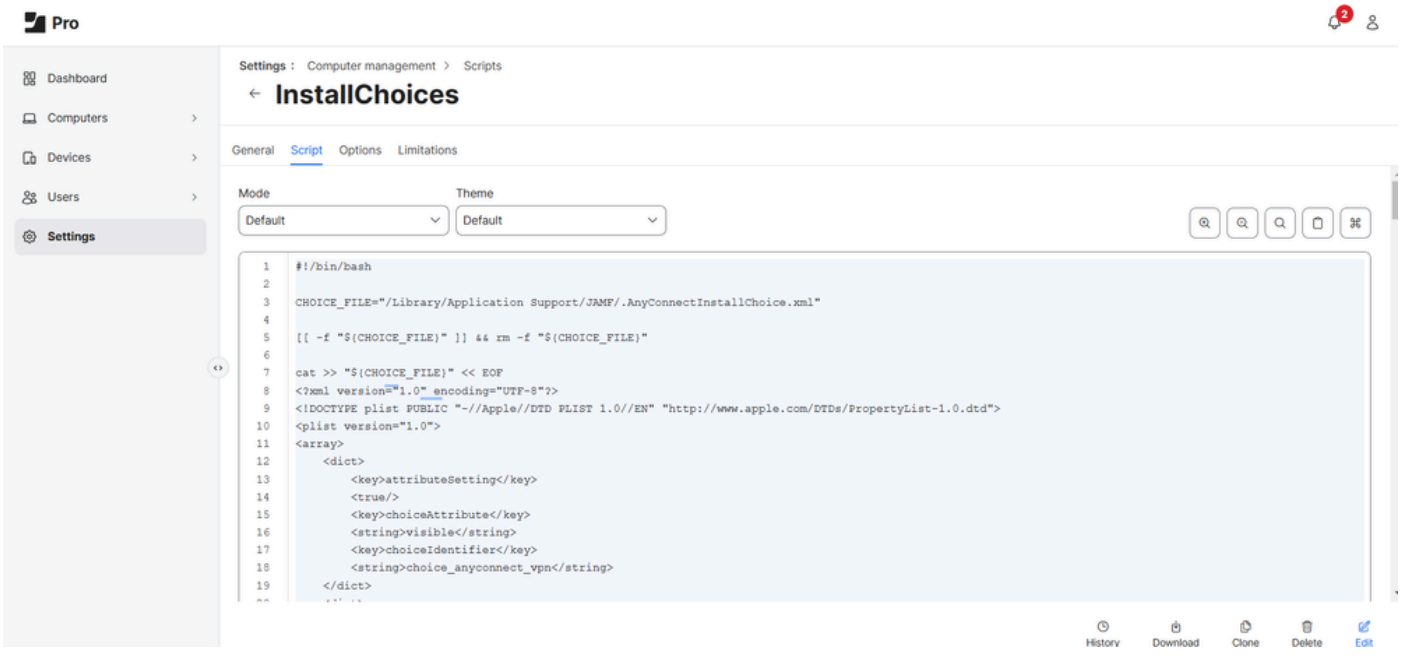


Adicionar configuração e scripts de seleção de módulo

1. Vá para Configurações > Gerenciamento do Computador > Scripts e adicione este script para controlar quais módulos são instalados durante a implantação.

2. Você pode controlar a instalação dos módulos do Secure Client definindo um módulo como 0 para ignorá-lo ou 1 para instalá-lo, pois o PKG está configurado para instalar todos os módulos por padrão.

- Você pode obter o arquivo XML de exemplo na documentação do Umbrella: Personalizar a instalação do macOS do Cisco Secure Client
- A Umbrella também adicionou o script "installchoice" a este link do github. Neste exemplo, os módulos Core VPN, Umbrella e DART são definidos como 1 e podem ser incluídos na instalação do Secure Client.



3. Navegue até Settings > Computer management > Scripts e adicione este script para criar um arquivo de configuração `Orginfo.json` que é exigido pelo Cisco Secure Client.

- Baixe o perfil do módulo diretamente do painel do Umbrella e adicione a ID da organização, Impressão digital e ID de usuário ao script:

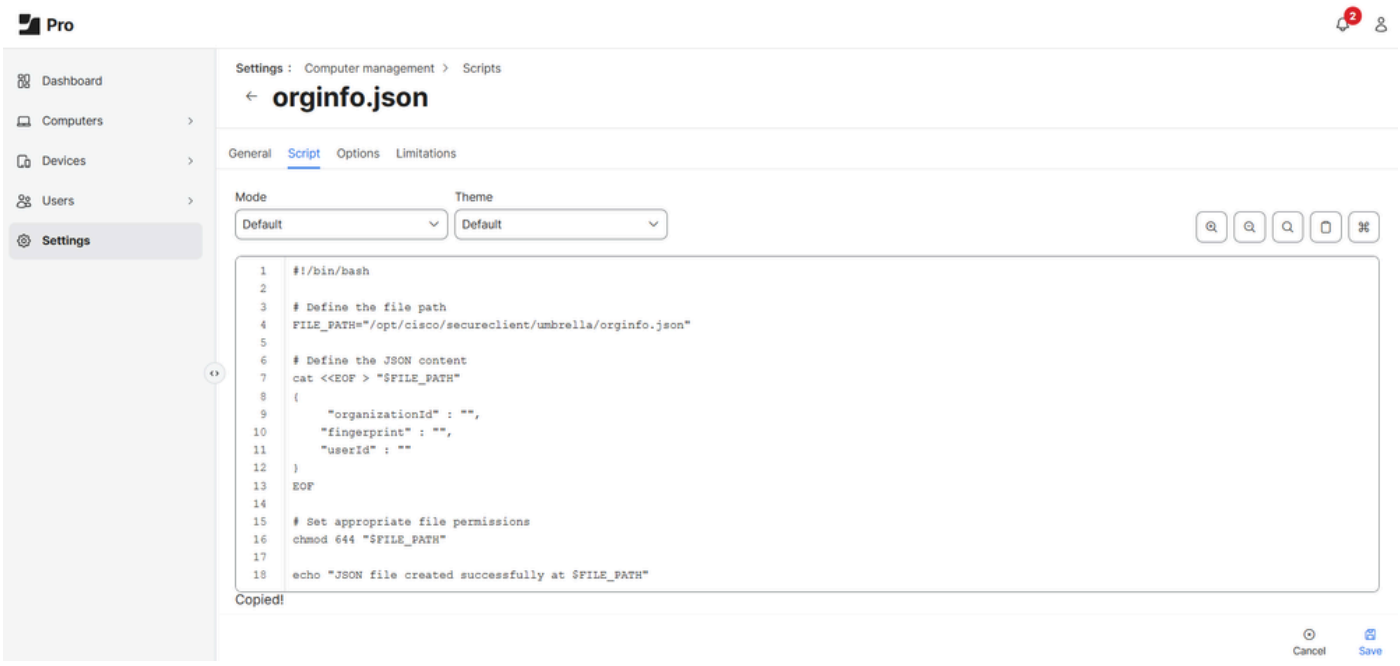
```
#!/bin/bash

# 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

Criar a política JAMF

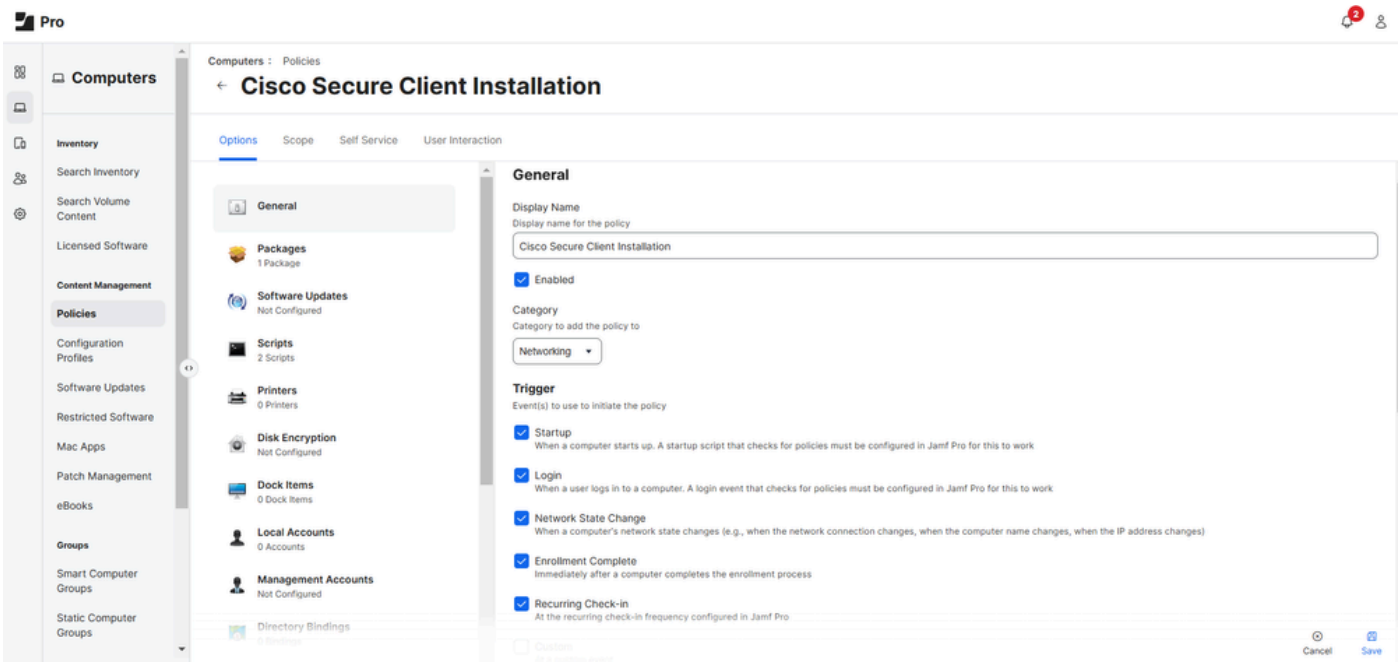
A Política JAMF é usada para determinar como e quando o Cisco Secure Client com módulo Umbrella é retirado.

1. Navegue até Computadores > Gerenciamento de conteúdo > Políticas > Novo.

2. Atribua um nome exclusivo à política e selecione os eventos Category e Trigger desejados (por exemplo, quando essa política for executada).

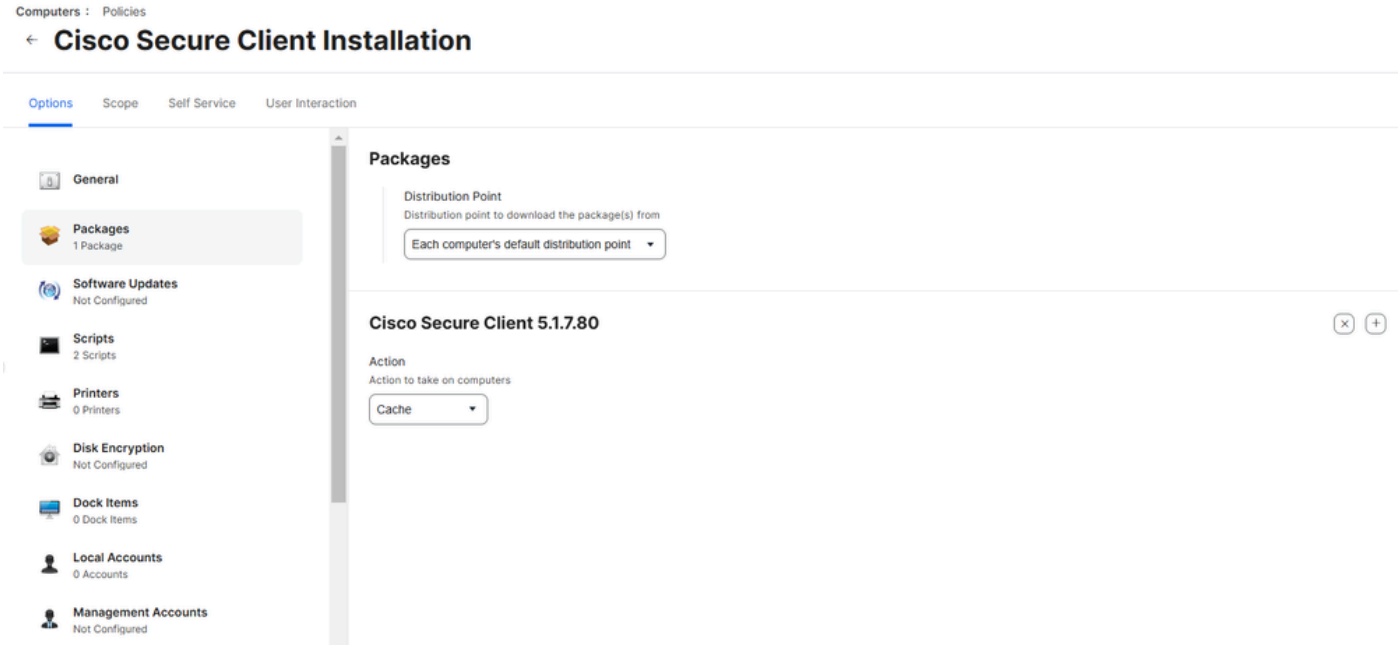
3. Opcionalmente, você também pode configurar um comando personalizado que pode ser executado em Personalizado. O comando para executar e executar essa política seria semelhante a:

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

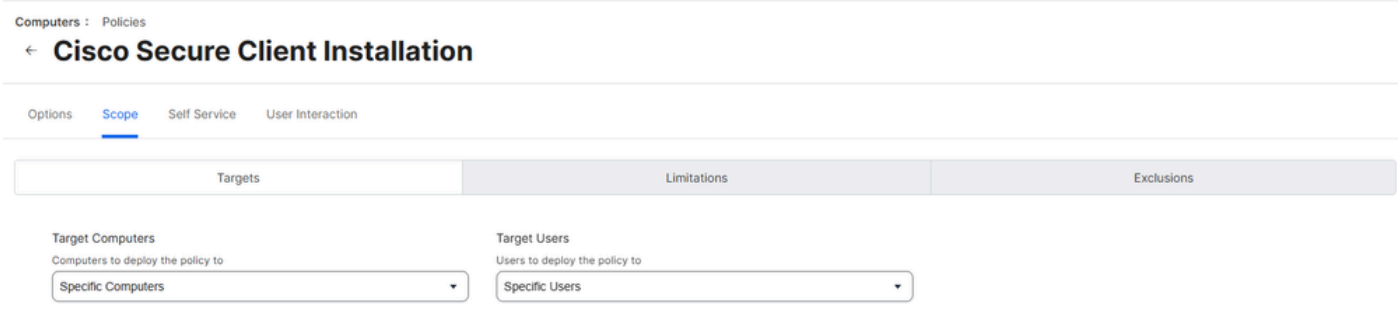


4. Selecione Packages > Configure e selecione Add ao lado do pacote do Cisco Secure Client.

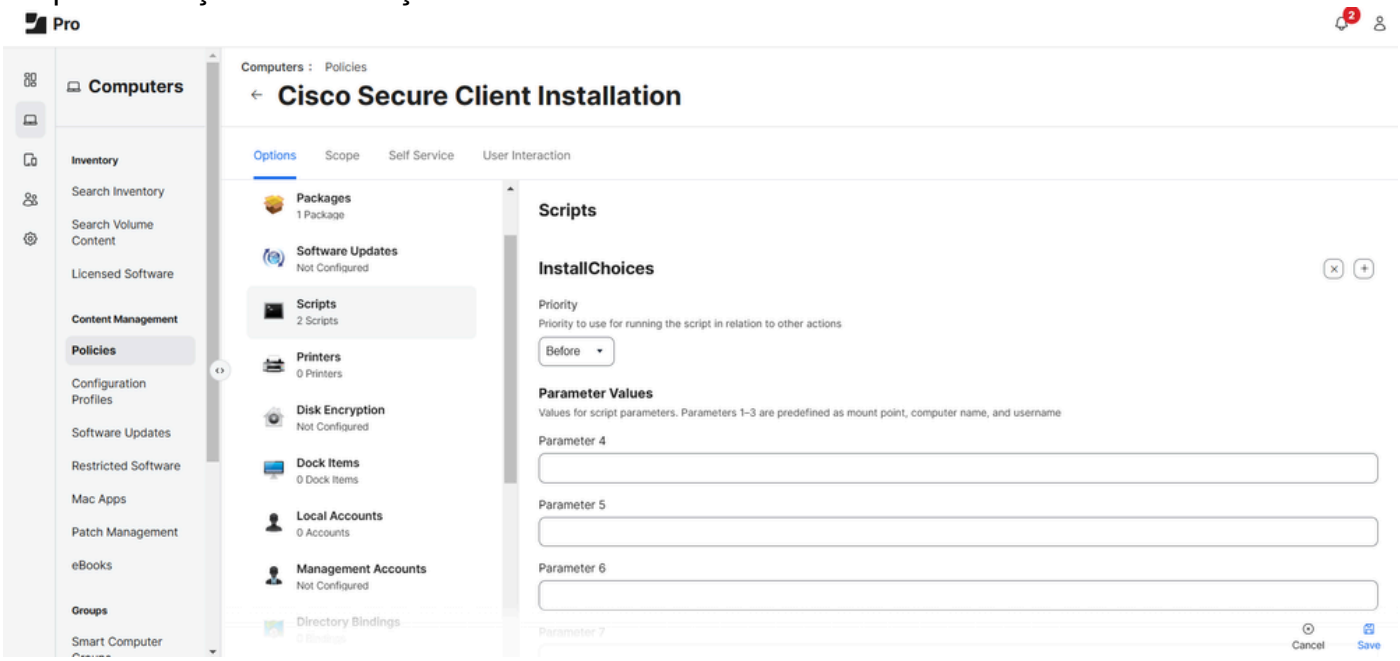
- Em Ponto de distribuição, selecione Ponto de distribuição padrão de cada computador.
- Em Action, selecione Cache.

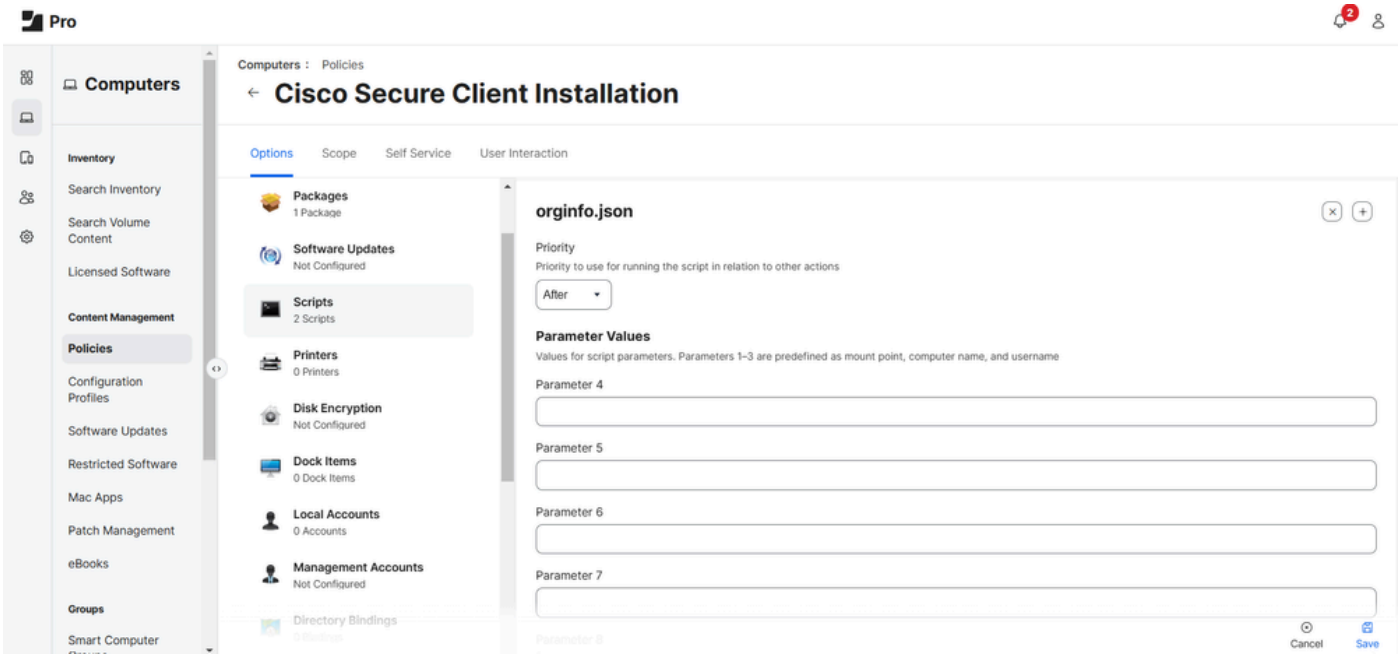


5. Defina o escopo de dispositivos ou usuários para implantação e selecione Salvar.



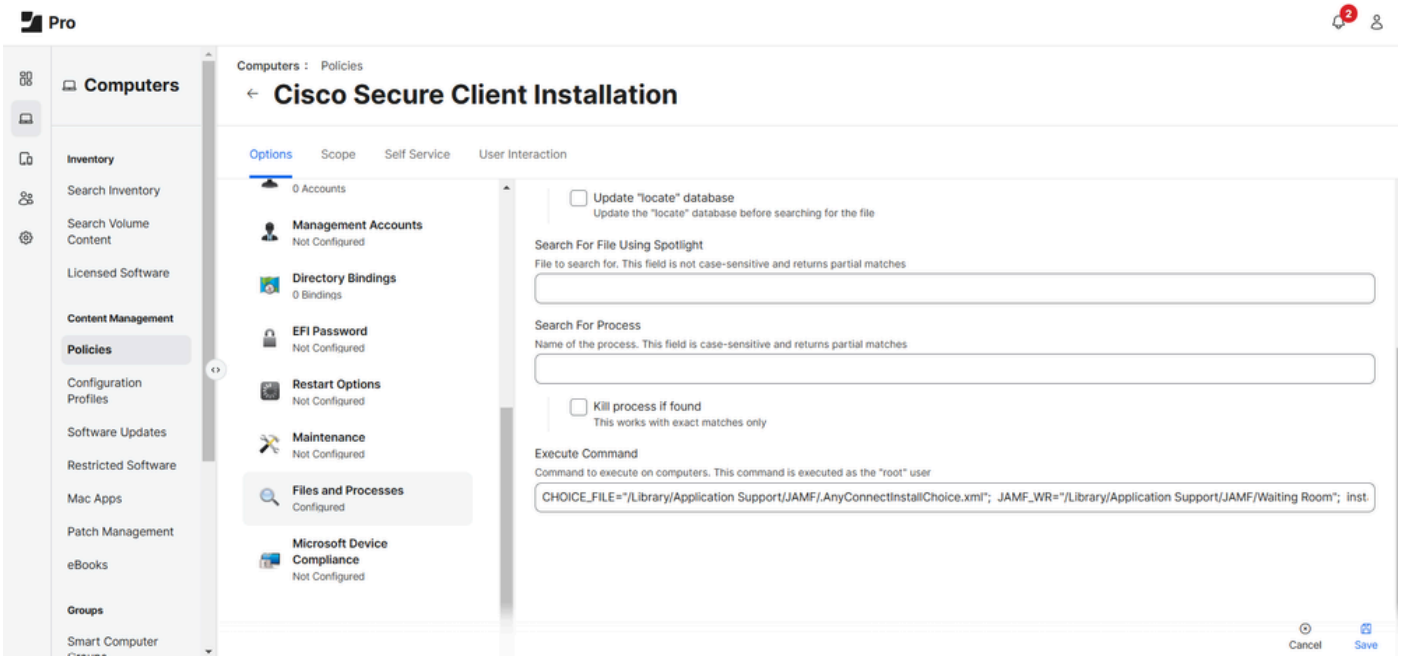
6. Adicione os scriptsInstallChoicese e **orginfo.json** dê a eles uma Prioridade a ser usada para executar o script em relação a outras ações.





7. Execute este comando para instalar o pacote Cisco Secure Client com os módulos selecionados nos dispositivos:

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



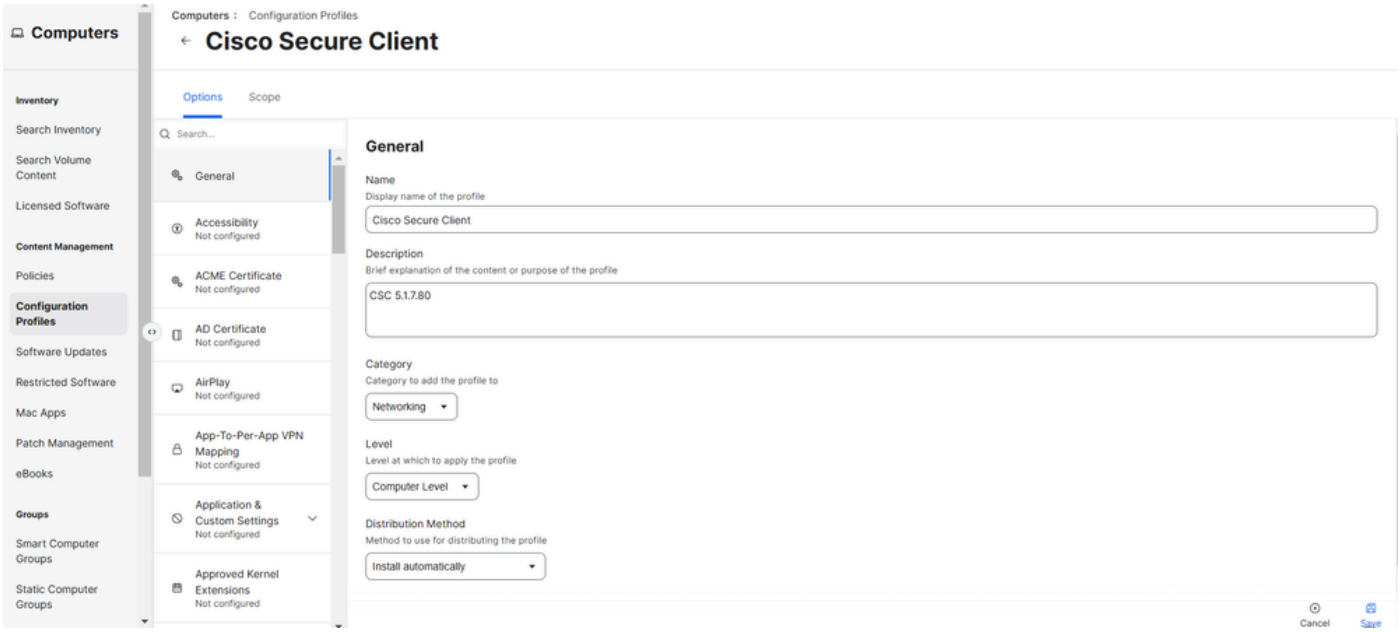
Configurar uma instalação silenciosa da extensão do sistema

Em seguida, use o JAMF para configurar e permitir as extensões de sistema necessárias do Cisco Secure Client para que o módulo Cisco Secure Client com Umbrella seja executado corretamente sem interações do usuário.

1. Vá para Computadores > Gerenciamento de conteúdo > Perfis de configuração > Novo.

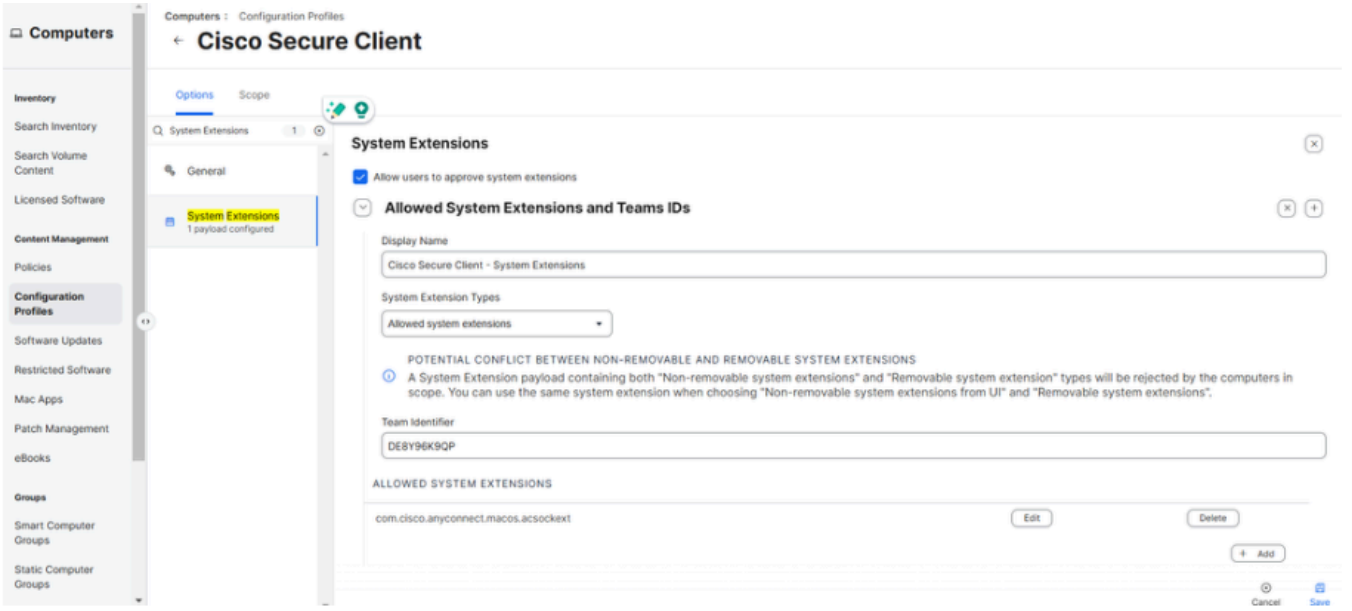
2. Dê ao perfil um nome exclusivo e selecione Categoria e Método de Distribuição.

3. EnsureLevel está definido como Nível do Computador.



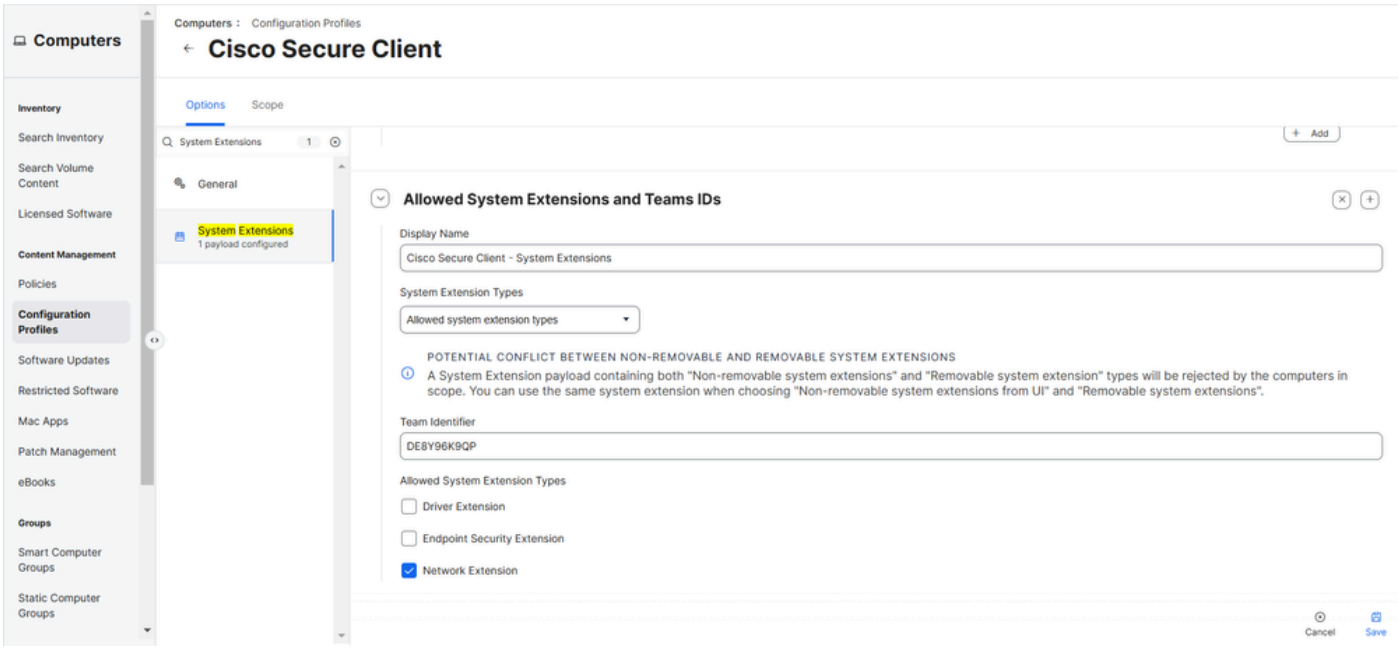
4. Procure Extensões de Sistema > Configurar. Insira estes valores:

- Nome de exibição: Cisco Secure Client - Extensões do Sistema
- Tipos de extensão do sistema: Extensões de sistema permitidas
- Identificador da Equipe: DE8Y96K9QP
- Extensões de sistema permitidas: com.cisco.anyconnect.macos.acsockext e, em seguida, selecione Salvar.



5. Selecione o ícone + ao lado de IDs de grupos permitidos e extensões de sistema para adicionar outro ramal do sistema. Em seguida, insira estes valores:

- Nome de exibição: Cisco Secure Client - Extensões do Sistema
- Tipos de extensão do sistema: Permitir Tipos de Extensão do Sistema
- Identificador da Equipe: DE8Y96K9QP
- Permitir tipos de extensão do sistema: Extensão de rede

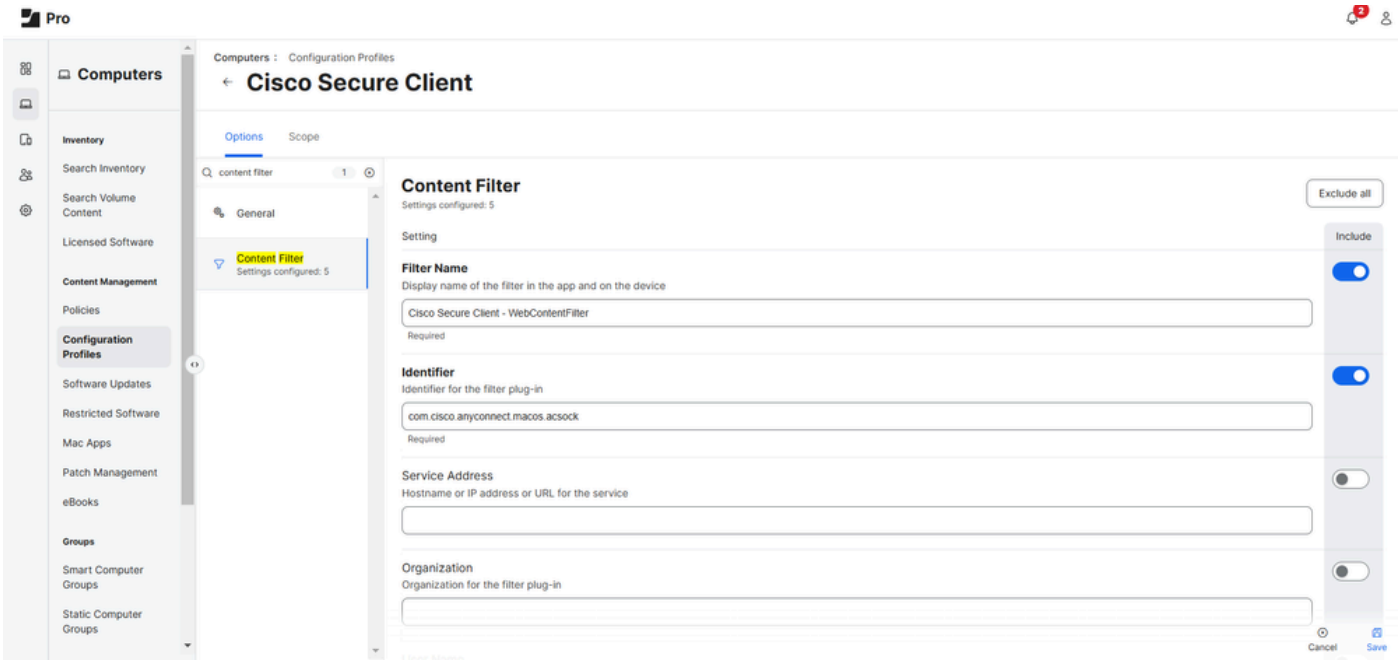


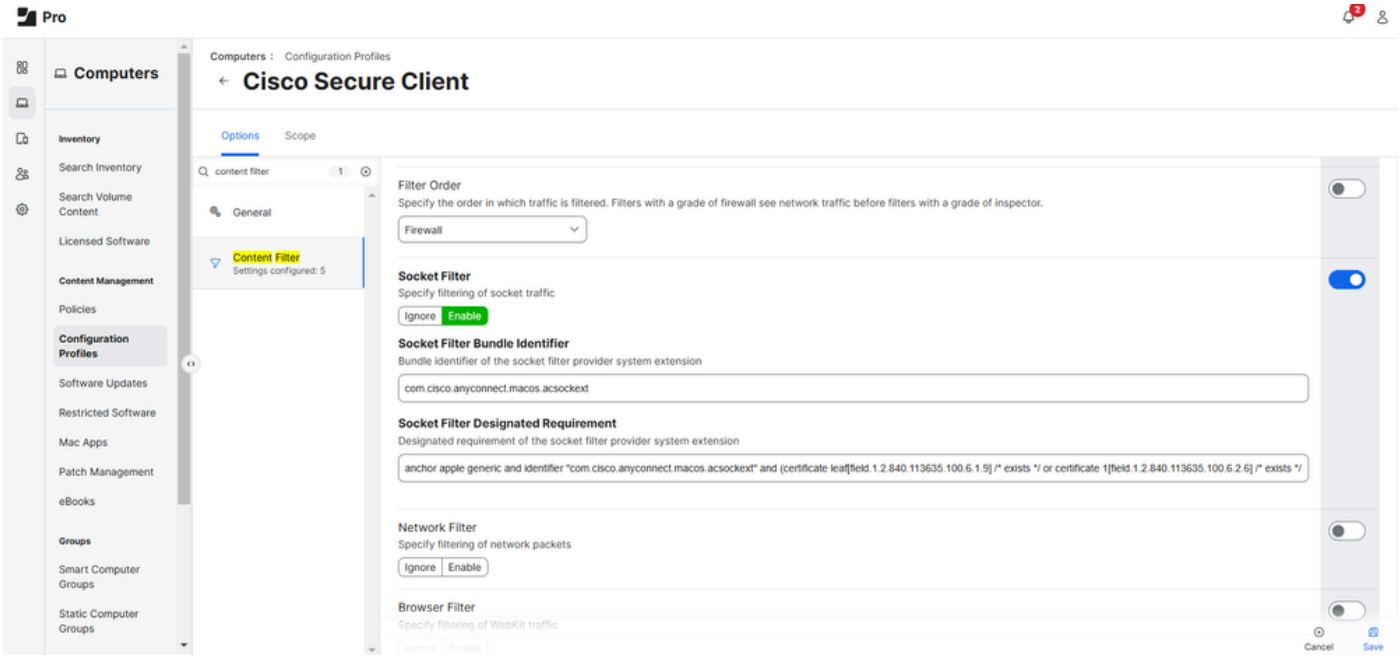
Configurar Instalação Silenciosa para Filtro de Conteúdo

Em seguida, configure uma instalação silenciosa para o filtro de conteúdo, que está correlacionado ao Cisco Secure Client com o filtro de soquete do módulo Umbrella:

1. Procure filtro de conteúdo. Habilite e preencha estes campos com seus respectivos valores:

- Nome do filtro: Cisco Secure Client - Filtro de Conteúdo da Web
- Identifier: com.cisco.anyconnect.macos.acsock
- Filtro de Soquete: Habilitado
- Identificador de Pacote de Filtro de Soquete: com.cisco.anyconnect.macos.acsockext
- Requisito Designado do Filtro de Soquete:
  `genérico e identificador da anchor apple "com.cisco.anyconnect.macos.acsockext" 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] = DE8Y96K9QP)`





2. Em Dados Personalizados, selecione Adicionar cinco vezes e insira estes valores:

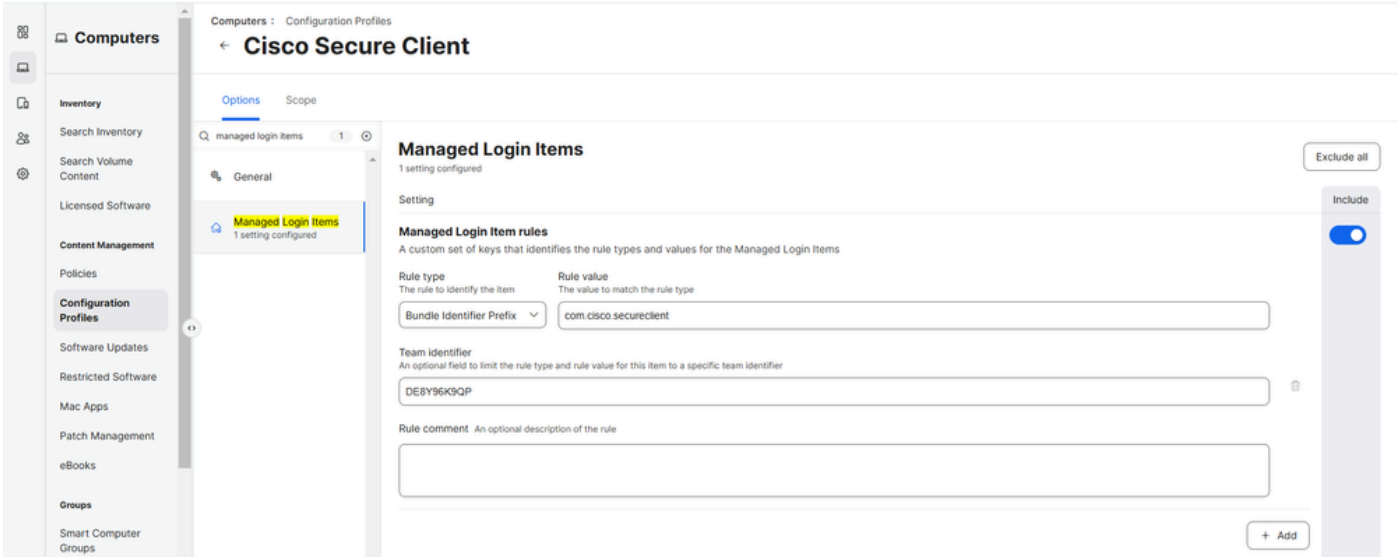
Chave	Valor
AutoFiltroHabilitado	falso
FiltrarNavegadores	falso
FiltrarSoquetes	verdadeiro
FiltrarPacotes	falso
FiltrarGrau	firewall

Configurar Itens de Logon Gerenciados

A configuração dos itens de login gerenciados para o módulo Cisco Secure Client com Umbrella garante que o Cisco Secure Client seja iniciado na inicialização do dispositivo.

Para configurar, procure Itens de login gerenciados e configure os campos com estes valores:

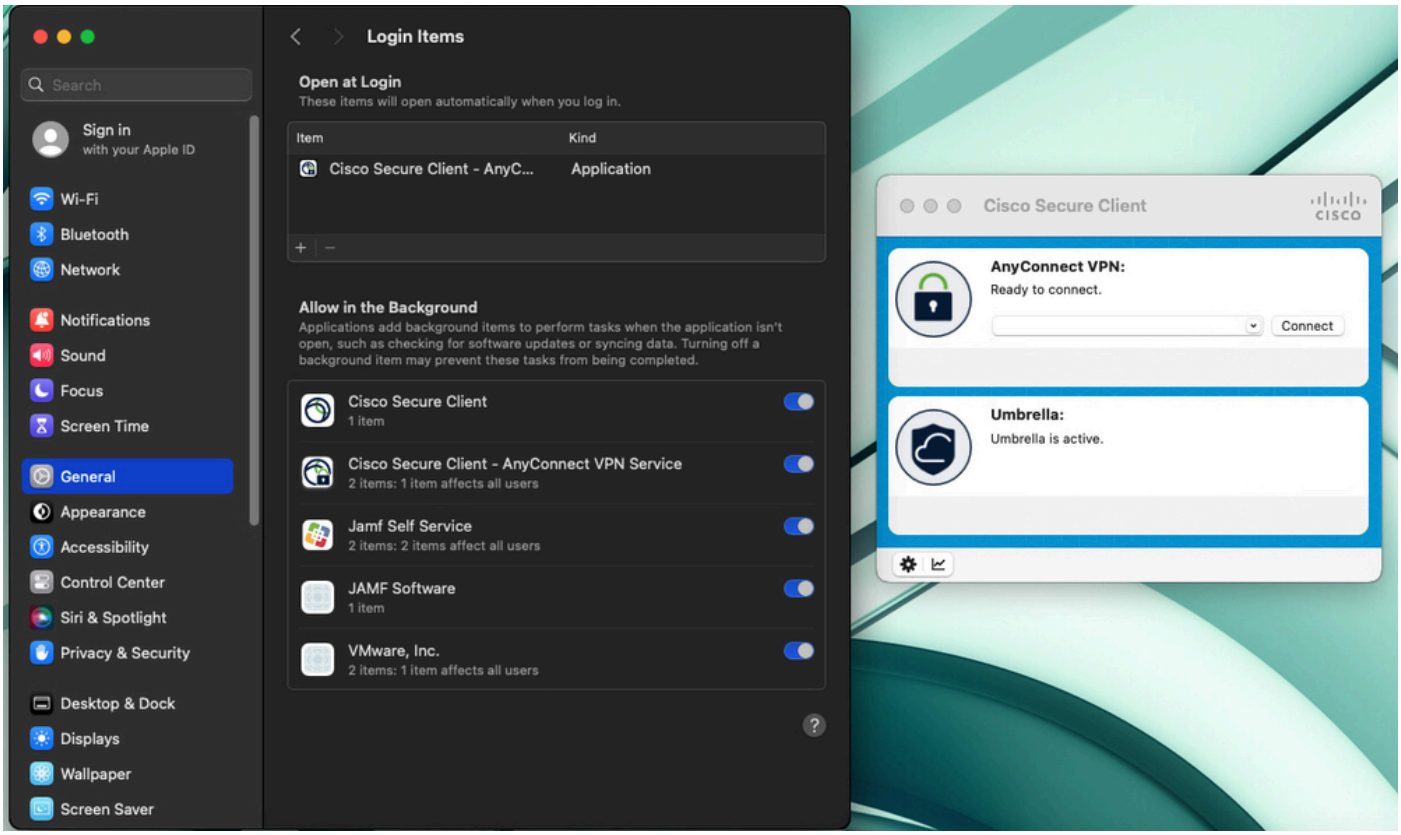
- Tipo de regra: Prefixo do identificador de pacote
- Valor da regra: com.cisco.secureclient
- Identificador da Equipe: DE8Y96K9QP

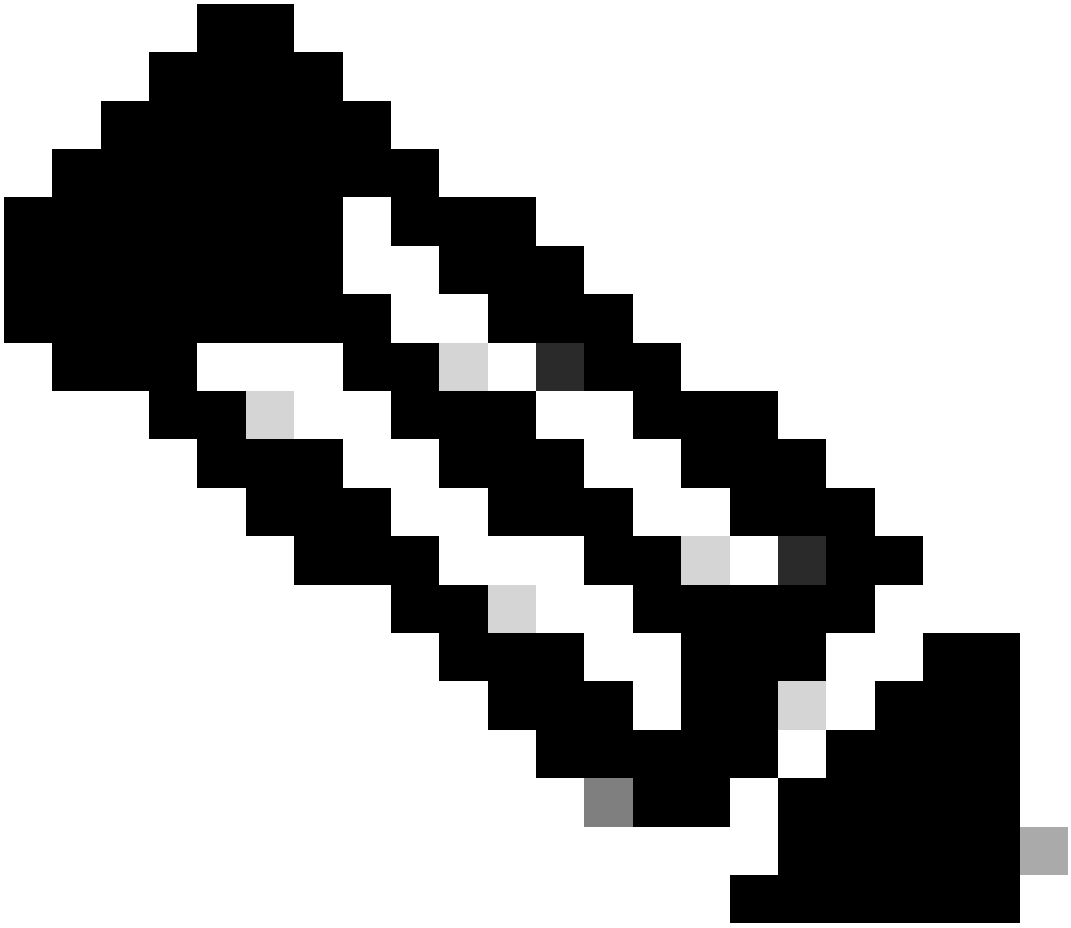


Atribuir Implantação de Escopo e Envio

1. Navegue até Escopo e defina o escopo para dispositivos ou usuários.

2. O módulo Cisco Secure Client com Umbrella pode ser enviado para os dispositivos macOS desejados quando um dos Triggers que você configurou na etapa 2 de Criar uma Política JAMF é ativado. Como alternativa, você pode distribuir isso pelo portal Self Service do JAMF.


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.



Note: Mesmo que um usuário tente desabilitar o Proxy DNS ou o Proxy Transparente nas Configurações do Sistema (Rede > Filtro), ele é automaticamente reabilitado por padrão, pois o Filtro de Conteúdo é habilitado via JAMF, conforme descrito neste artigo, e não pode ser desabilitado.

Configurar exceção do firewall do macOS

Se o firewall do macOS estiver configurado para Bloquear todas as conexões de entrada, você também deverá adicionar o Cisco Secure Client e seus componentes à sua lista de exceções:

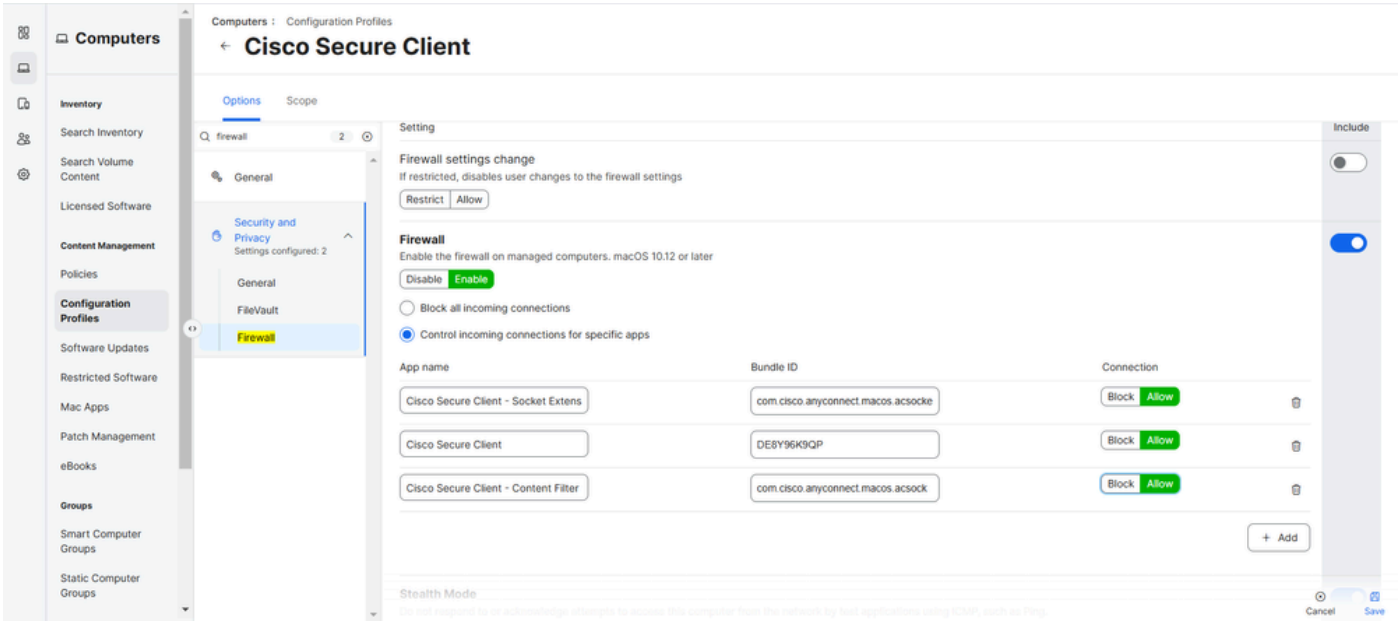
1. Navegue até Computadores > Gerenciamento de conteúdo > Perfis de configuração.

2. Selecione o perfil de configuração do Cisco Secure Client e localize Security and Privacy.

3. Defina-o com estas configurações:

- Firewall: Habilitar - Controlar conexões de entrada para aplicativos específicos

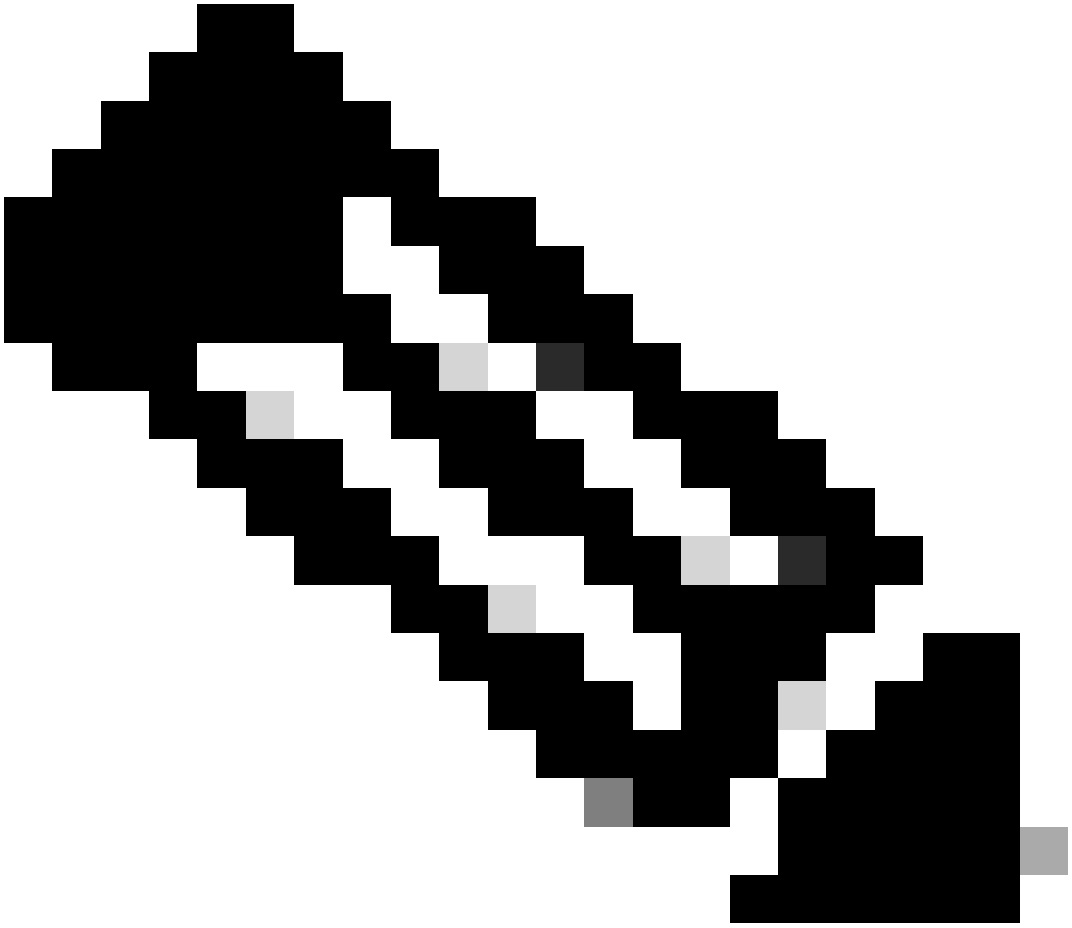
Nome do aplicativo	ID do pacote
Cisco Secure Client - Extensões de soquete	com.cisco.anyconnect.macos.acsockext
Cisco Secure Client	DE8Y96K9QP
Cisco Secure Client - Filtro de conteúdo	com.cisco.anyconnect.macos.acsock



4. Selecione Salvar.

5. Se aparecer o prompt Redistribution Options, selecione Distribute to All para enviar imediatamente as alterações para os dispositivos macOS desejados.

Implante o certificado raiz do Cisco Umbrella



Note: Esta etapa se aplica somente a novas implantações do Cisco Secure Client ou a dispositivos que não tenham o Certificado Raiz de Guarda-Chuva Cisco implantado anteriormente. Se você estiver migrando do cliente de roaming de guarda-chuva ou do cliente Cisco AnyConnect 4.10, e/ou já tiver implantado o Certificado Raiz de Guarda-chuva Cisco no passado, ignore esta seção.

Faça o download do certificado raiz do Cisco Umbrella emPolicies > Root Certificateno painel do Umbrella.

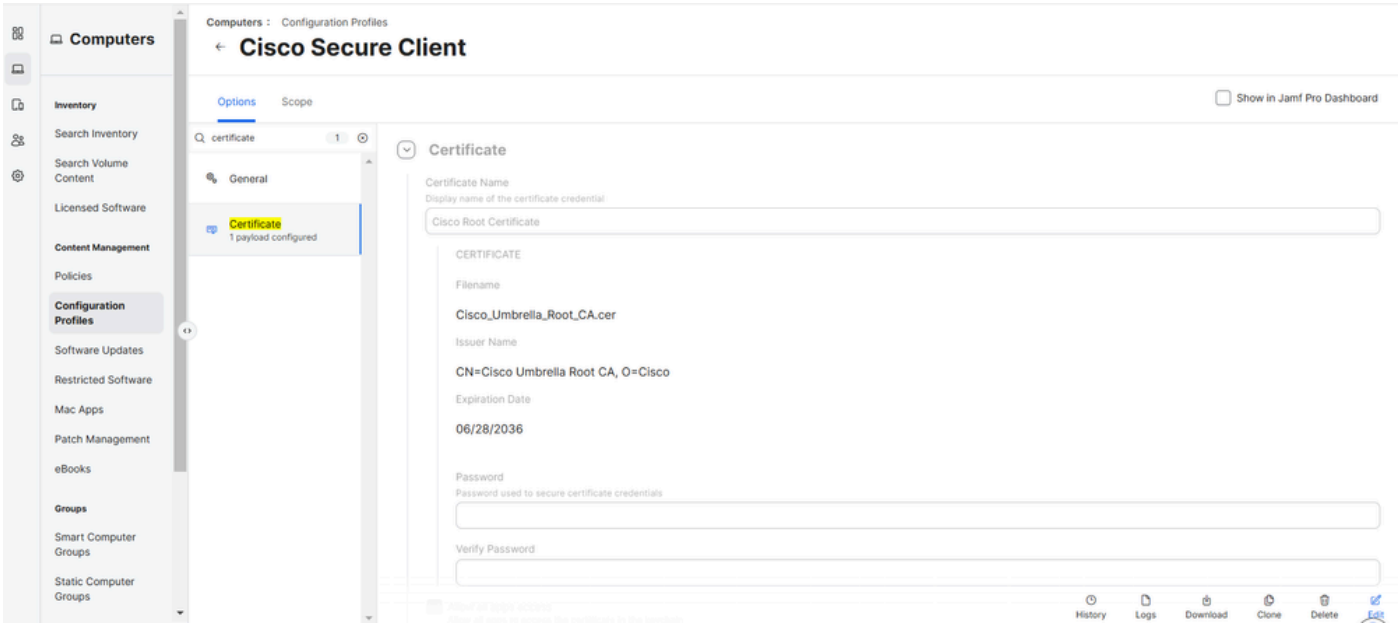
1. No painel Umbrella em Policies > Root Certificate, faça o download do Cisco Umbrella Root Certificate.

2. No JAMF, navegue até Computers > Configuration Profiles > Cisco Secure Client > Edit.

3. Procure Certificado > Configurar. Dê a ele um nome exclusivo.

4. Em Selecionar opção de certificado, selecione Carregar e carregue o Certificado raiz do Cisco Umbrella que você baixou anteriormente na Etapa 1.

5. Certifique-se de não configurar uma senha aqui e selecione Salvar.



6. Se aparecer o prompt Redistribution Options, selecione Distribute to All para enviar imediatamente as alterações para os dispositivos macOS desejados.

Verificação

Para verificar se o Cisco Secure Client com módulo Umbrella está funcionando, navegue até https://policy-debug.checkumbrella.com ou execute este comando:

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

Qualquer resultado deve conter informações exclusivas e relevantes para sua organização Umbrella, como sua OrgID.

Solução alternativa para macOS 14.3

Para o macOS 14.3 (ou posterior) com o Cisco Secure Client 5.1.x, se você encontrar "O agente de cliente VPN não conseguiu criar o depósito de comunicação entre processos":

1. No JAMF, navegue atéConfigurações > Gerenciamento do computador > Scripts > Novo.

2. Dê a ele um nome exclusivo e defina sua categoria.

3. Navegue até a guia Script e adicione isto:

```
#!/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. Em Opções, certifique-se de que Prioridade esteja definida como Depois. Este script bash verifica se o Cisco Secure Client - AnyConnect VPN service.app está sendo executado por meio do retorno de uma saída esperada com o ID do processo de `pgrep -fl`.

- Se retornar uma saída vazia, você poderá confirmar se o `Cisco Secure Client - AnyConnect VPN service.app` não está em execução e se o script é executado para iniciar os serviços principais do Cisco Secure Client necessários para que o módulo Umbrella seja executado corretamente.

Atualizações automáticas

A Cisco decidiu estender o suporte à atualização automática do painel Umbrella para incluir o Secure Client a partir do Secure Client 5.1.6.103 (MR6). No futuro, os clientes que fizeram a atualização para pelo menos o Cisco Secure Client 5.1.6 MR6 poderão fazer a atualização automática para versões mais recentes se a atualização automática tiver sido configurada no painel do Umbrella.

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.