CSC naar macOS implementeren met behulp van JAMF met Umbrella Module

Inhoud

Inleiding

In dit document wordt beschreven hoe u Cisco Secure Client met de overkoepelende module kunt implementeren op beheerde macOS-apparaten met behulp van JAMF.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

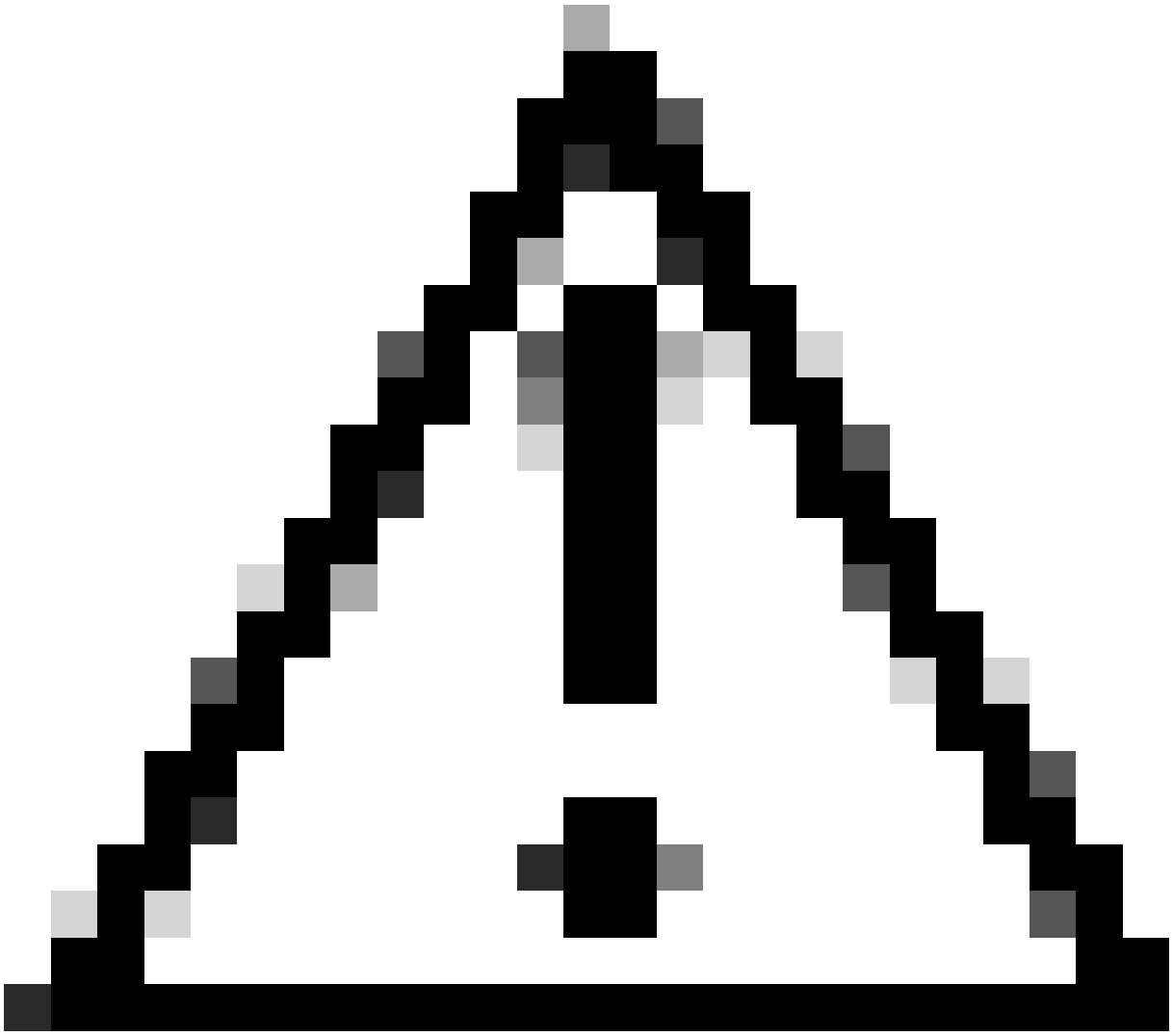
- macOS-apparaten moeten worden beheerd door JAMF.
- Voor MDM-inschrijvingsinstructies voor macOS raadpleegt u de JAMF-documentatie.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Secure Client.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.



Let op: Dit artikel is beschikbaar vanaf 1 februari 2025. Cisco Umbrella Support garandeert niet dat deze instructies na deze datum geldig zijn en kunnen worden gewijzigd op basis van updates van JAMF en Apple.

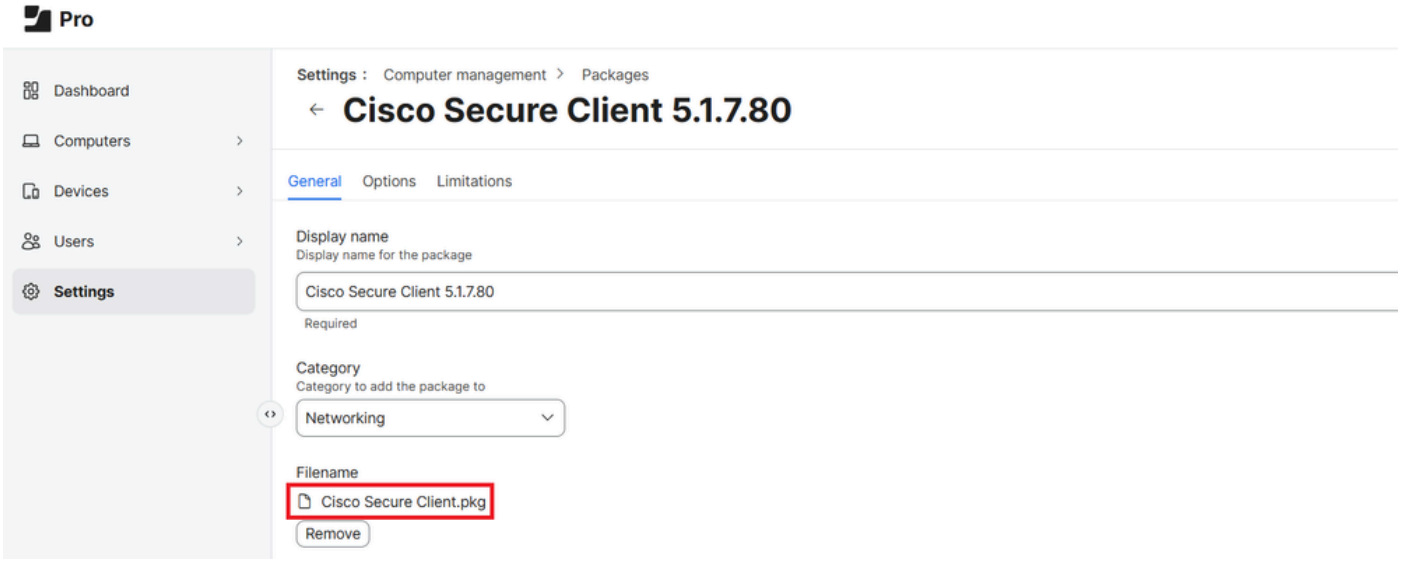
Het installatiepakket (PKG) uploaden

1. Download de Cisco Secure Client DMG van het overkoepelende dashboard onder Implementaties > Zwervende computers > Zwervende client > Pre-Deployment Package > macOS.

2. Log in op uw JAMF Pro-cloudexemplaar.

3. Navigeer naar Instellingen > Computerbeheer > Pakketten > Nieuw.

4. Upload de PKG uit het DMG-pakket dat u hebt gedownload van uw Umbrella-dashboard.

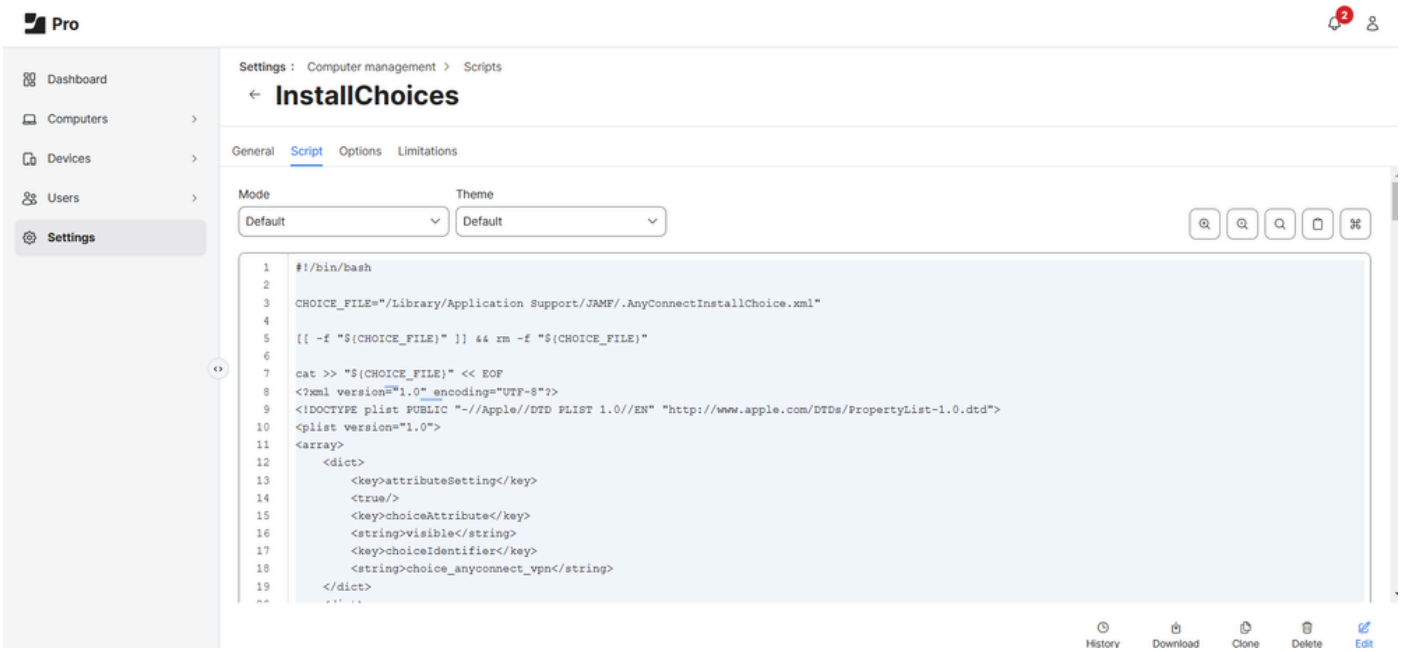


Configuratie- en moduleselectiescripts toevoegen

1. Ga naar Instellingen > Computerbeheer > Scripts en voeg dit script toe om te bepalen welke modules tijdens de implementatie worden geïnstalleerd.

2. U kunt de installatie van Secure Client-modules regelen door een module in te stellen op 0 om deze over te slaan of 1 om deze te installeren, aangezien de PKG standaard is geconfigureerd om alle modules te installeren.

- U kunt het voorbeeld XML-bestand uit de overkoepelende documentatie halen: [macOS-installatie van Cisco Secure Client aanpassen]
- Umbrella heeft ook het "installchoices" script toegevoegd aan deze [GitHub-link.] In dit voorbeeld zijn de Core VPN-, Umbrella- en DART-modules ingesteld op 1 en kunnen deze worden opgenomen in de installatie van de Secure Client.



3. Navigeer naar Instellingen > Computerbeheer > Scripts en voeg dit script toe zodat het een configuratiebestand `Orginfo.json` maakt dat door Cisco Secure Client wordt vereist.

- Download het moduleprofiel rechtstreeks vanuit het Umbrella-dashboard en voeg vervolgens de organisatie-ID, vingerafdruk en gebruikersnaam aan het script toe:

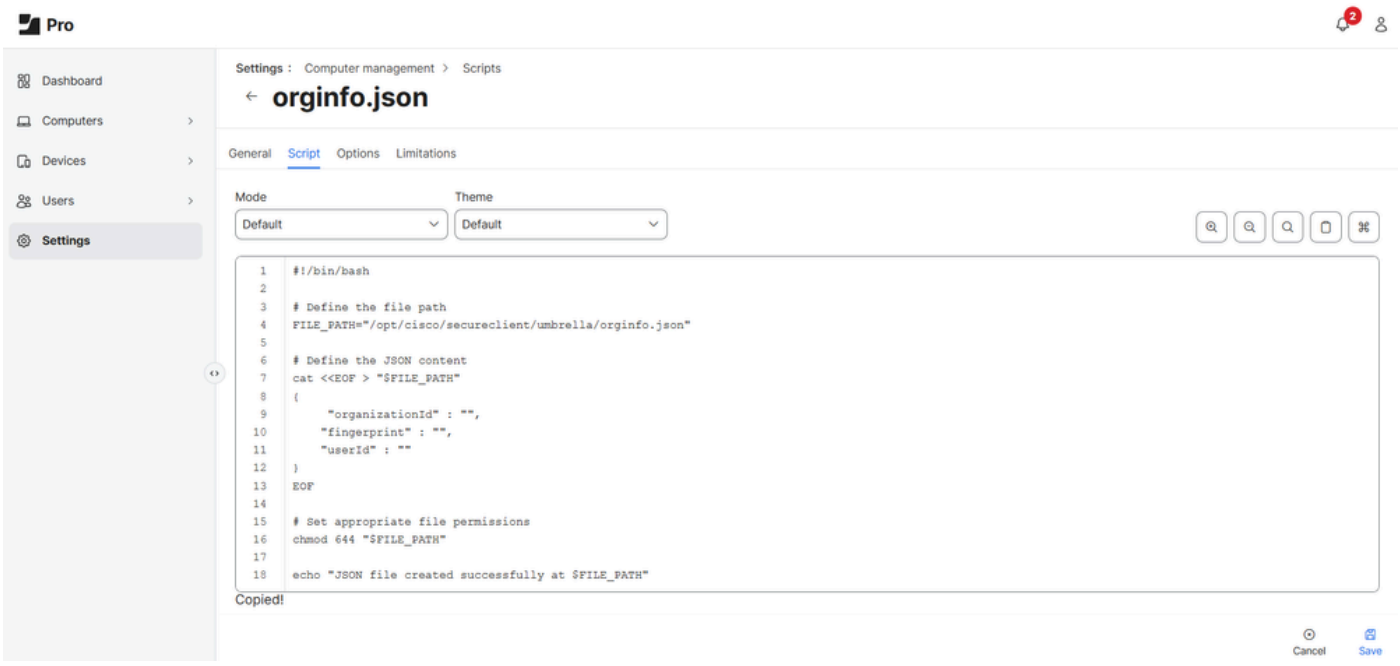
```
#!/bin/bash

# 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

Het JAMF-beleid maken

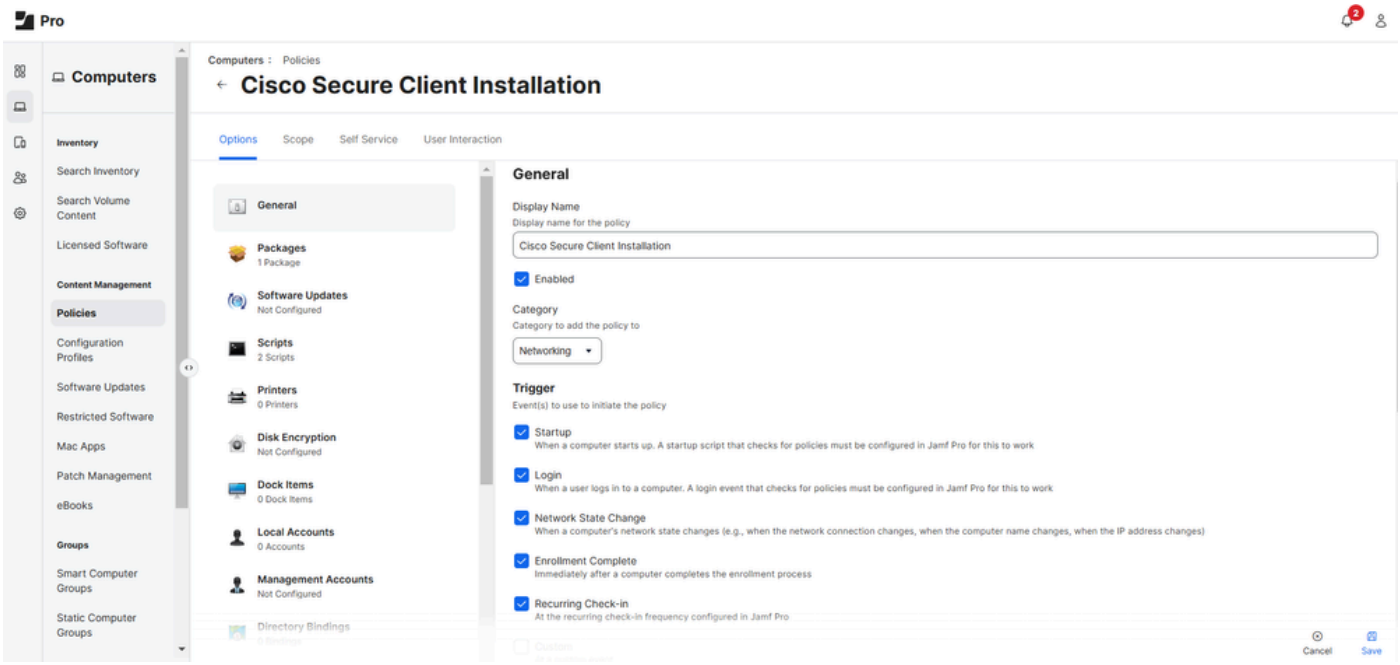
Het JAMF-beleid wordt gebruikt om te bepalen hoe en wanneer de Cisco Secure Client with Umbrella-module wordt verwijderd.

1. Navigeer naar Computers > Contentbeheer > Beleid > Nieuw.

2. Wijs een unieke naam toe aan het beleid en selecteer de gewenste categorie- en triggergebeurtenissen (bijvoorbeeld wanneer dit beleid wordt uitgevoerd).

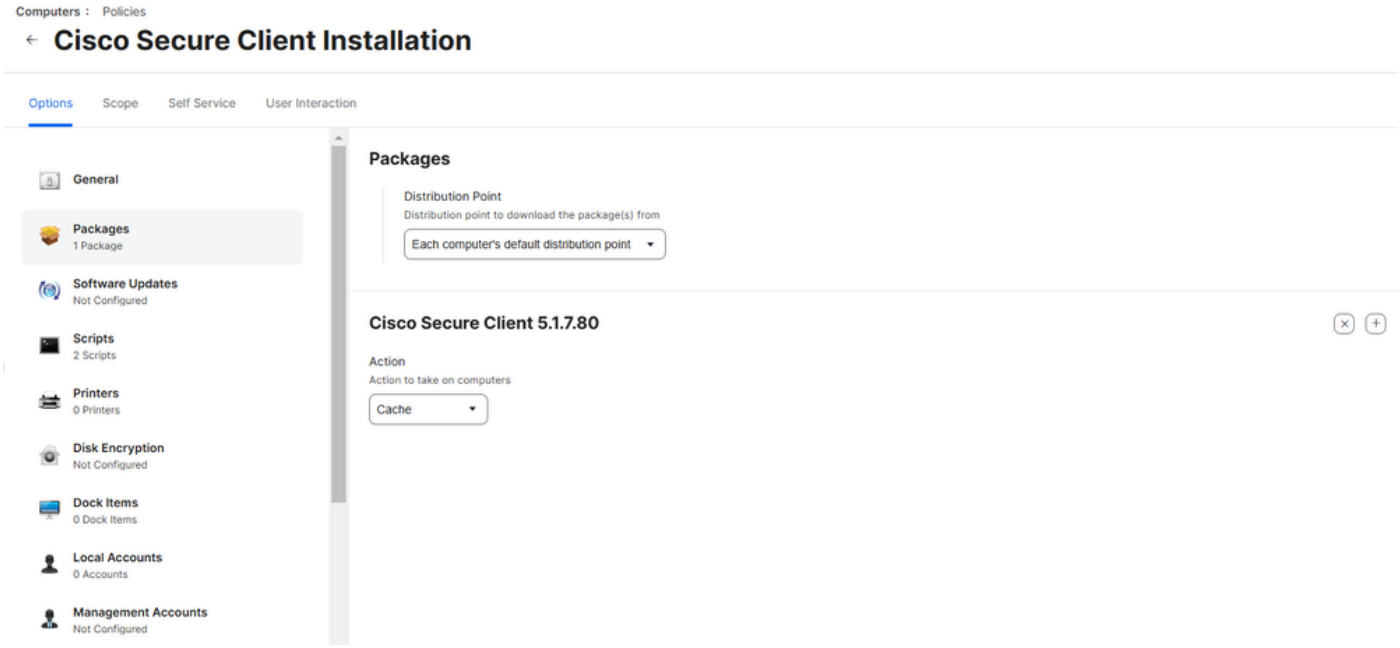
3. Optioneel kunt u ook een aangepaste opdracht configureren die onder Aangepast kan worden uitgevoerd. De opdracht om dit beleid uit te voeren en uit te voeren ziet er ongeveer als volgt uit:

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

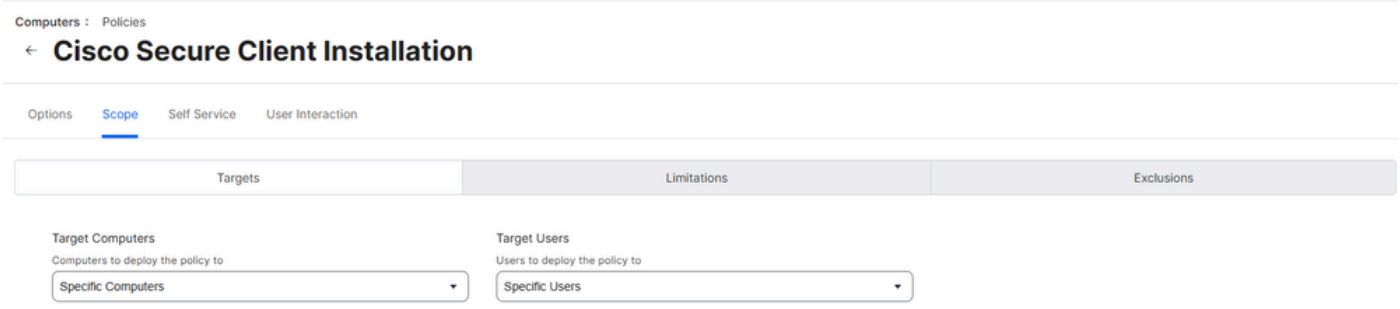


4. Selecteer Pakketten > Configureren en selecteer Toevoegen naast uw Cisco Secure Client-pakket.

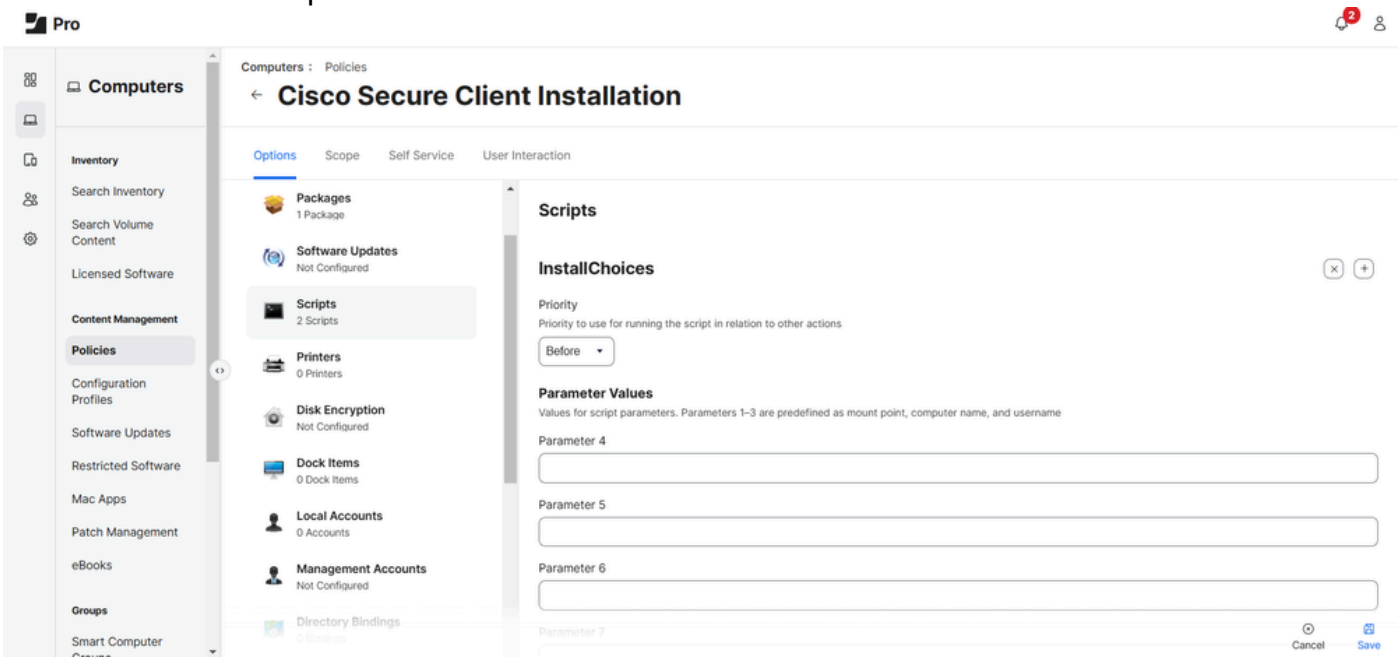
- Selecteer onder Distributiepunt de optie Standaarddistributiepunt van elke computer.
- Selecteer onder Actie de optie Cache.

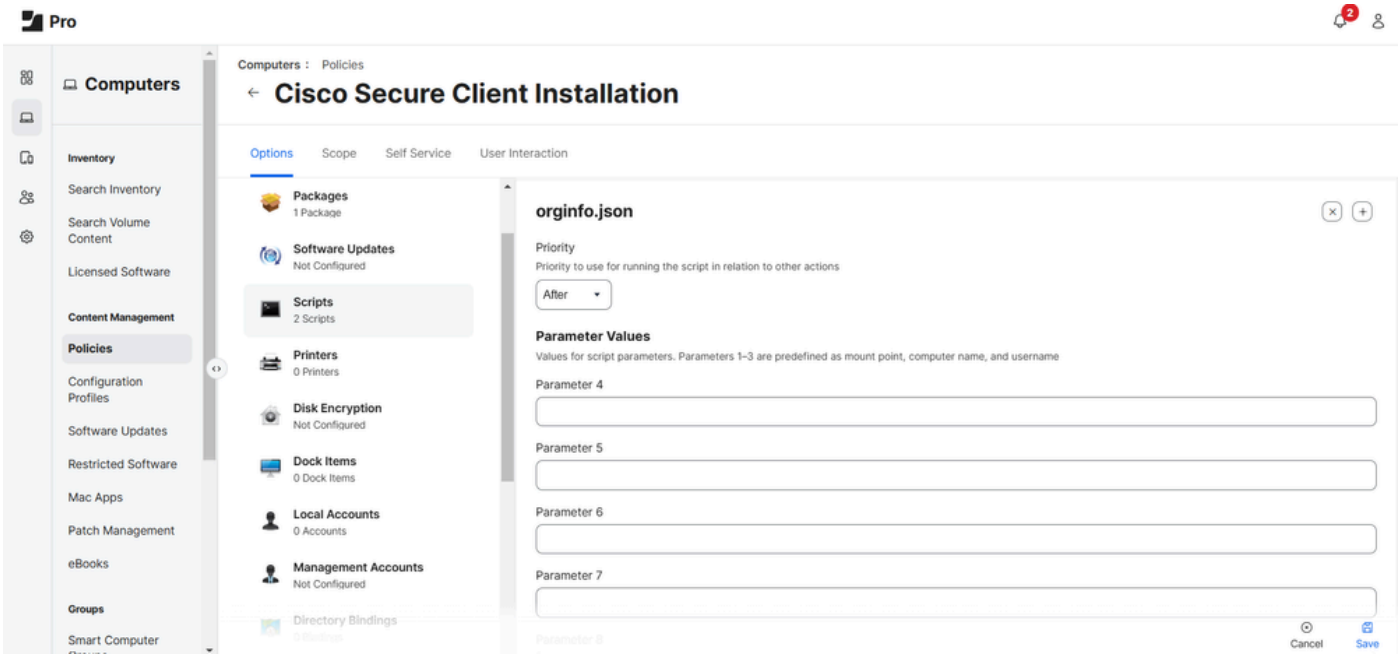


5. Definieer het bereik van apparaten of gebruikers voor implementatie en selecteer Opslaan.



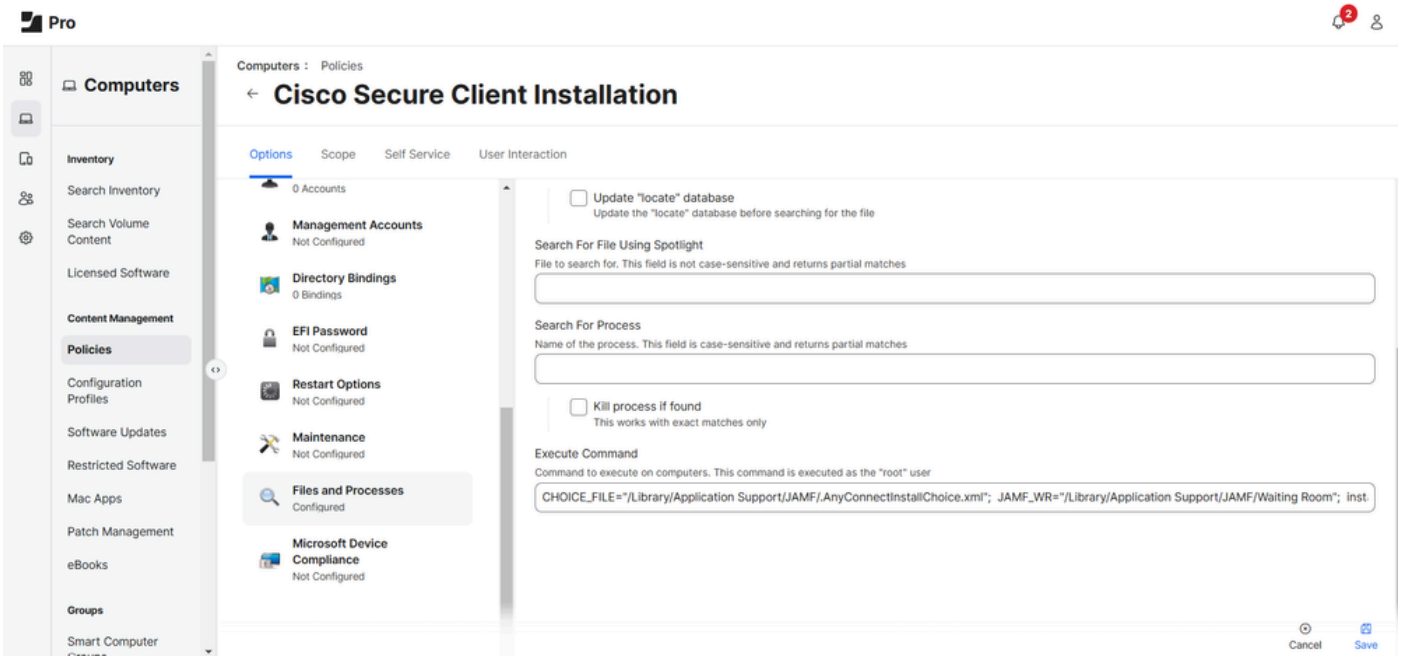
6. Voeg zowel de`InstallChoices`scripts als de **`orginfo.json`** scripts toe en geef ze een prioriteit voor het uitvoeren van het script in relatie tot andere acties.





7. Voer deze opdracht uit om het Cisco Secure Client-pakket met de geselecteerde modules te installeren op apparaten:

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



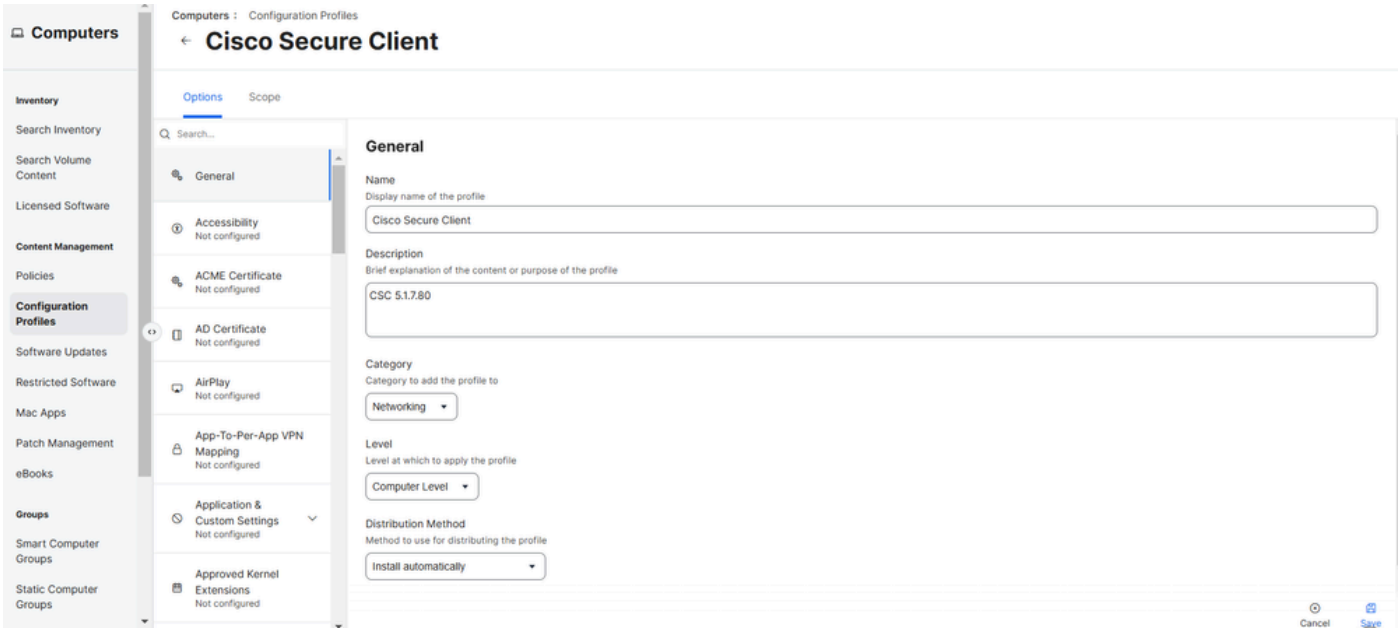
Een stille installatie van de systeemextensie configureren

Vervolgens gebruikt u JAMF om de vereiste systeemextensies van Cisco Secure Client te configureren en toe te staan, zodat Cisco Secure Client met Umbrella-module correct kan worden uitgevoerd zonder gebruikersinteracties.

1. Ga naar Computers > Contentbeheer > Configuratieprofielen > Nieuw.

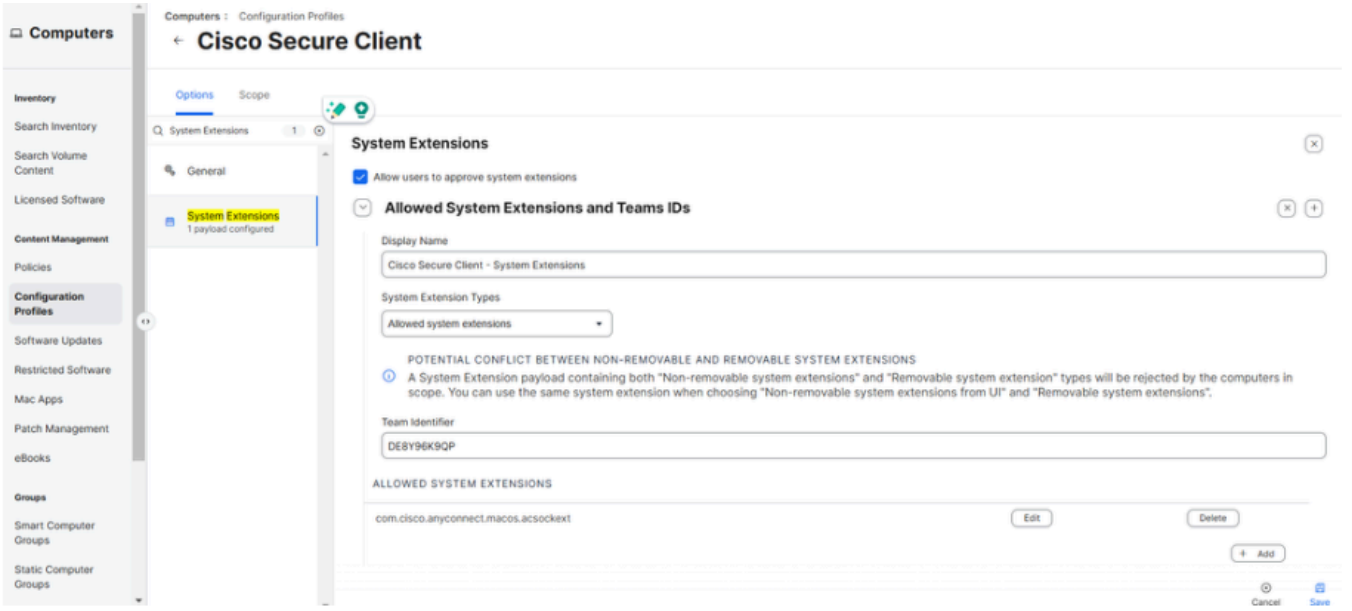
2. Geef het profiel een unieke naam en selecteer de categorie en distributiemethode.

3. EnsureLevel is ingesteld op Computerniveau.



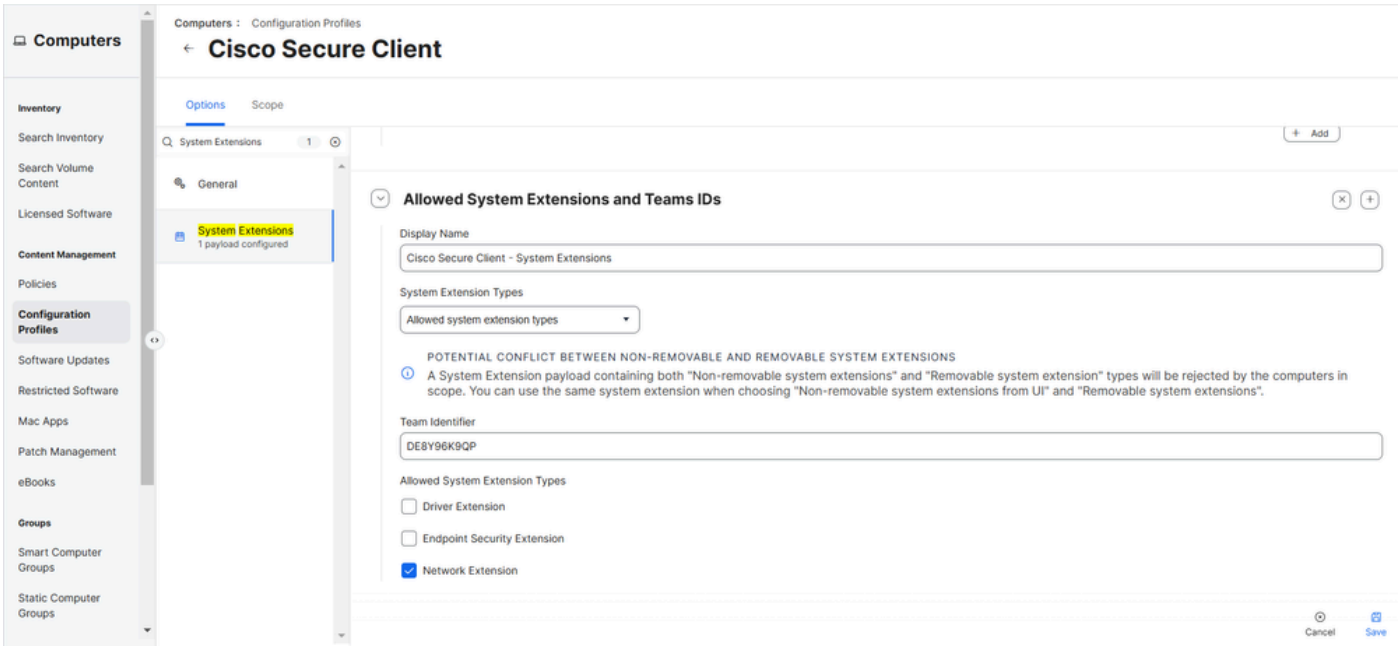
4. Zoeken naar systeemextensies > Configureren. Voer de volgende waarden in:

- Display Name: Cisco Secure Client - Systeemextensies
- Systeemextensietypen: toegestane systeemextensies
- Team-ID: DE8Y96K9QP
- Toegestane systeemextensies: com.cisco.anyconnect.macos.acsockext, selecteer vervolgens Opslaan.



5. Selecteer het + pictogram naast Toegestane team-ID's en systeemextensies om een andere systeemextensie toe te voegen. Voer vervolgens de volgende waarden in:

- Display Name: Cisco Secure Client - Systeemextensies
- Systeemextensietypen: Systeemextensietypen toestaan
- Team-ID: DE8Y96K9QP
- Systeemuitbreidingstypen toestaan: Netwerkuitbreiding

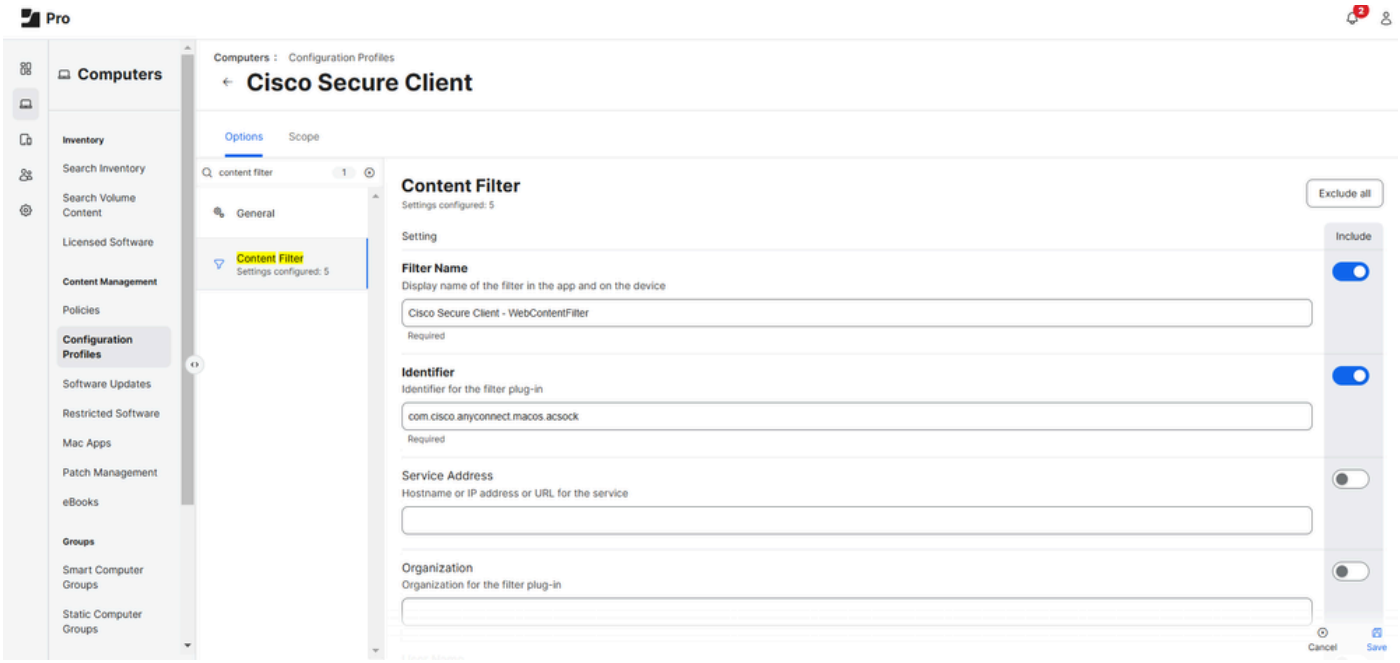


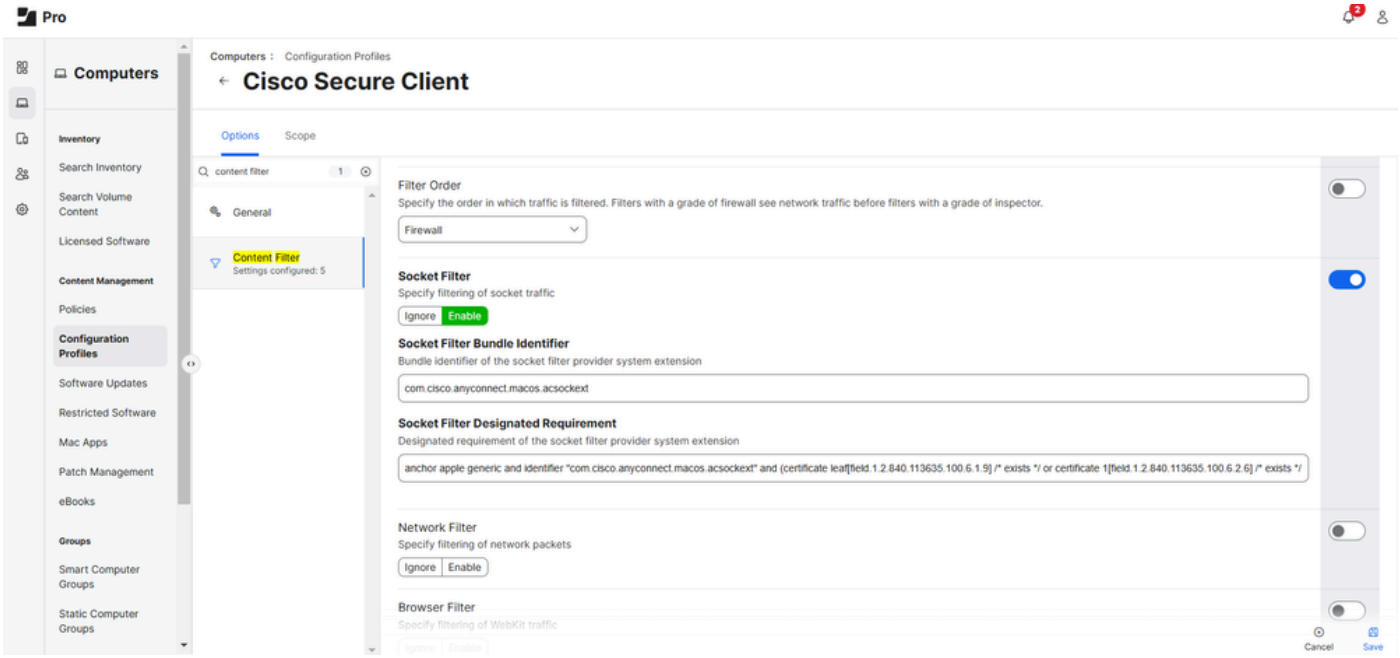
Silent Install for Content Filter configureren

Configureer vervolgens een stille installatie voor het inhoudsfilter, die correleert met het socketfilter van de Cisco Secure Client with Umbrella-module:

1. Zoeken naar inhoudsfilter. Schakel deze velden in en vul ze aan met hun respectieve waarden:

- Naam filter: Cisco Secure Client - WebContentFilter
- Identificatiecode: com.cisco.anyconnect.macos.acsock
- Socketfilter: ingeschakeld
- Socket Filter Bundle Identifier: com.cisco.anyconnect.macos.acsockext
- Aangewezen socketfilter-eis:
  ```
  Apple's generieke anker en identificatiecode "COM.Cisco.AnyConnect.macOS.SocketXT" en (certificaatblad[veld.1.2.840.113635.100.6.1.9] /* bestaat */ of certificaat 1[veld.1.2.840.113635.100.6.2.6] /* bestaat */ en certificaatblad[veld.1.2.840.113635.100.6.1.1.13] /* bestaat */ en certificaatblad[subject.OU] = DE8Y96K9QP)
  ```





2. Selecteer onder Aangepaste gegevens de optie Vijf keer toevoegen en voer de volgende waarden in:

Sleutel	Waarde
AutoFilter ingeschakeld	vals
FilterBrowsers	vals
FilterSockets	waar
FilterPackets	vals
Filterkwaliteit	firewall

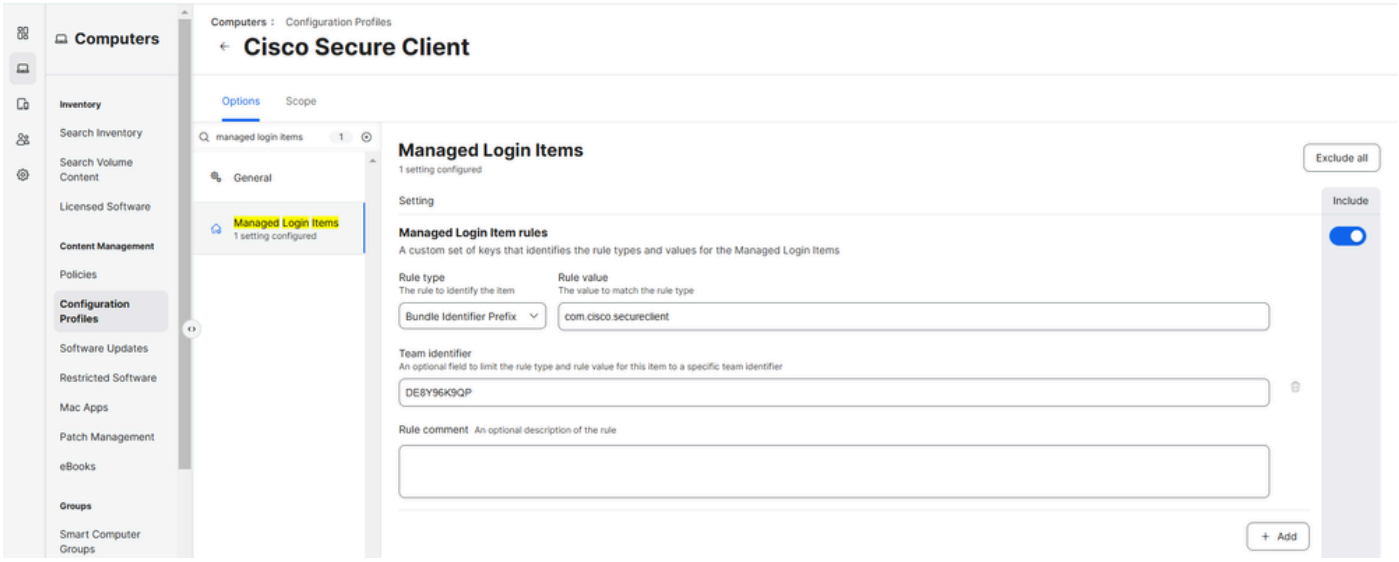
Beheerde inlogitems configureren

Als u de beheerde aanmeldingsitems voor de Cisco Secure Client met Umbrella-module

configureert, wordt de Cisco Secure Client bij het opstarten van het apparaat gestart.

Als u wilt configureren, zoekt u Beheerde aanmeldingsitems en configureert u de velden met de volgende waarden:

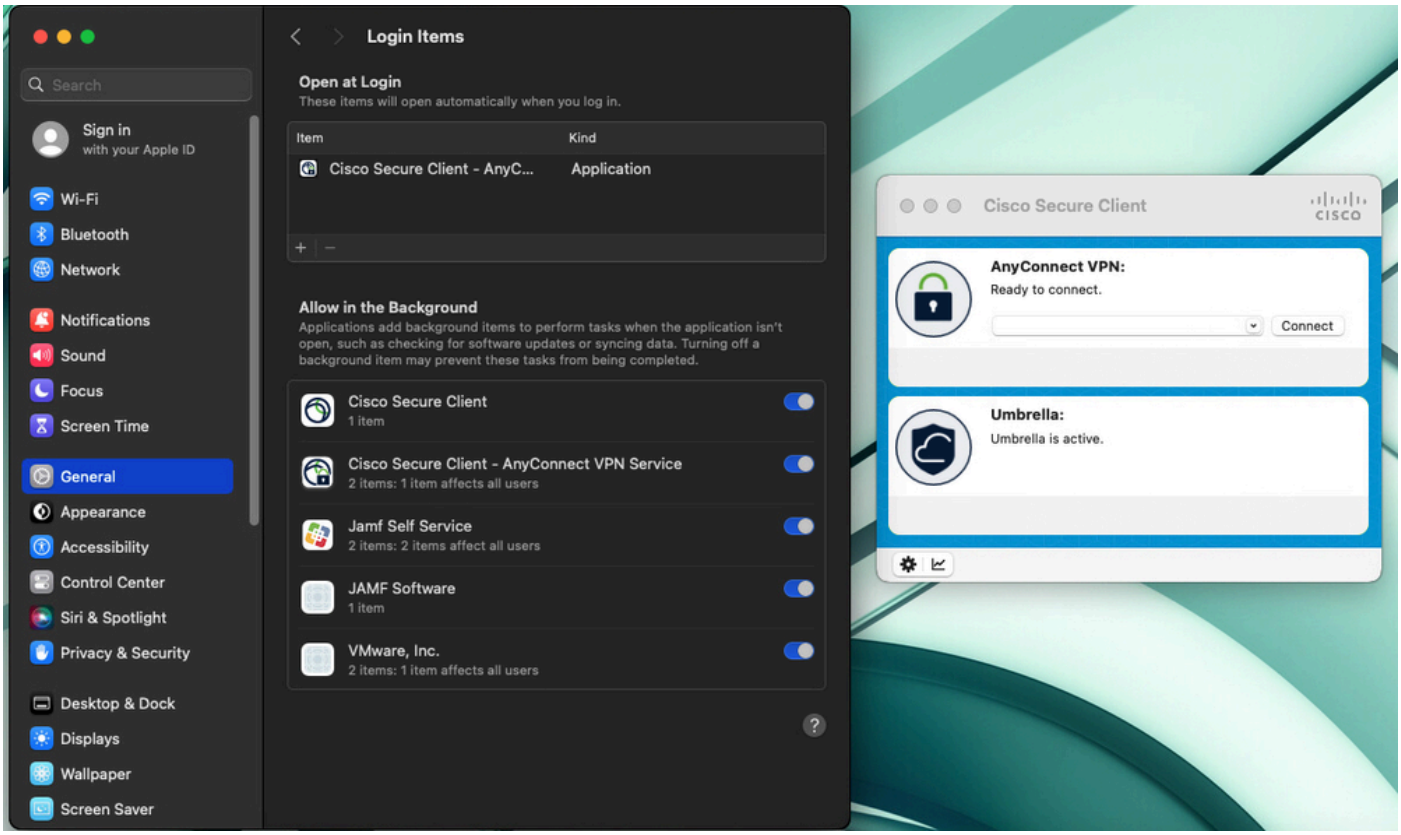
- Regeltype: voorvoegsel voor bundelidentificatie
- Regelwaarde: com.cisco.secureclient
- Team-ID: DE8Y96K9QP

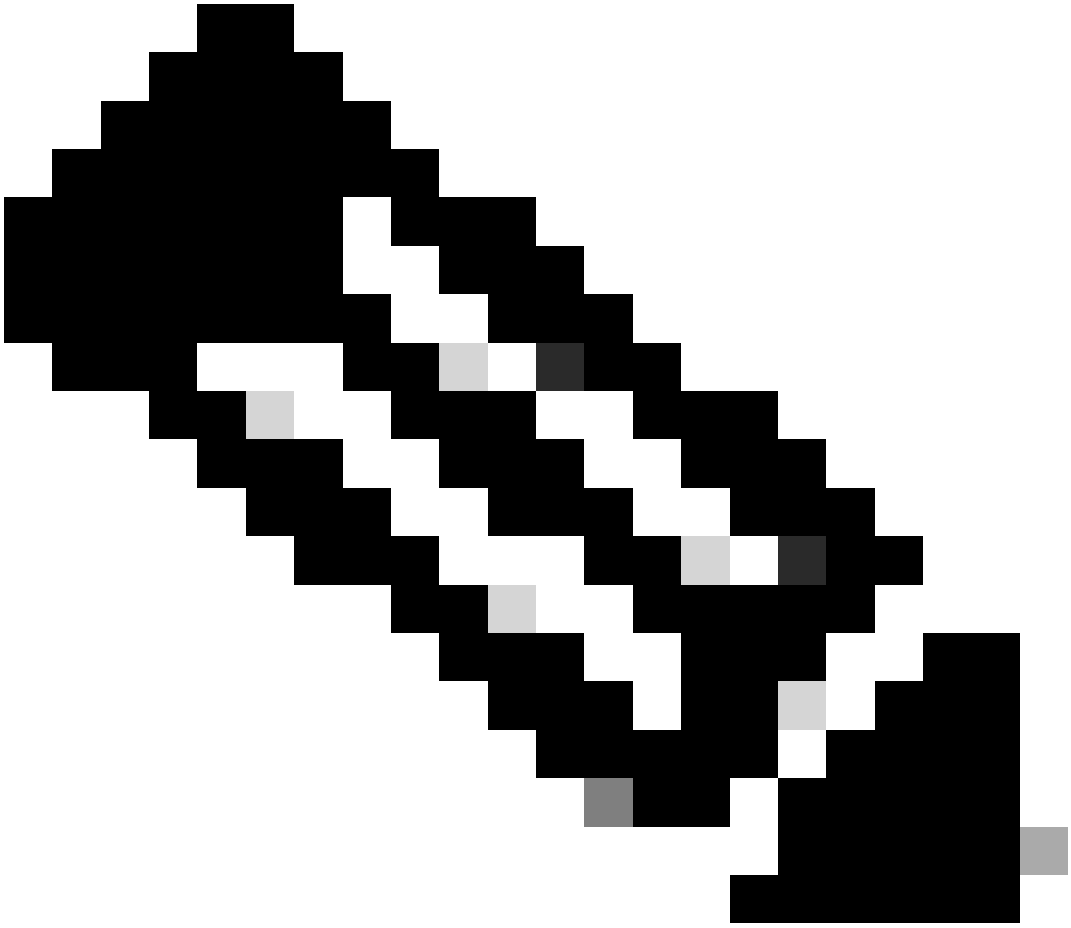


Toewijzen van bereik en push-implementatie

1. Navigeer naar Bereik en definieer het bereik voor apparaten of gebruikers.

2. De Cisco Secure Client with Umbrella-module kan naar de gewenste macOS-apparaten worden gepusht wanneer een van de triggers die u in stap 2 van JAMF-beleid maken hebt geconfigureerd, is geactiveerd. Als alternatief kunt u dit via JAMF's zelfbedieningsportaal uitduwen.


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.



Opmerking: Zelfs als een gebruiker probeert de DNS-proxy of transparante proxy uit te schakelen in Systeeminstellingen (Netwerk > Filter), wordt deze standaard automatisch opnieuw ingeschakeld omdat het inhoudsfilter is ingeschakeld via JAMF zoals beschreven in dit artikel en niet kan worden uitgeschakeld.

MacOS Firewall-uitzondering configureren

Als de macOS-firewall is ingesteld om alle inkomende verbindingen te blokkeren, moet u ook de Cisco Secure Client en de bijbehorende componenten toevoegen aan de lijst met uitzonderingen:

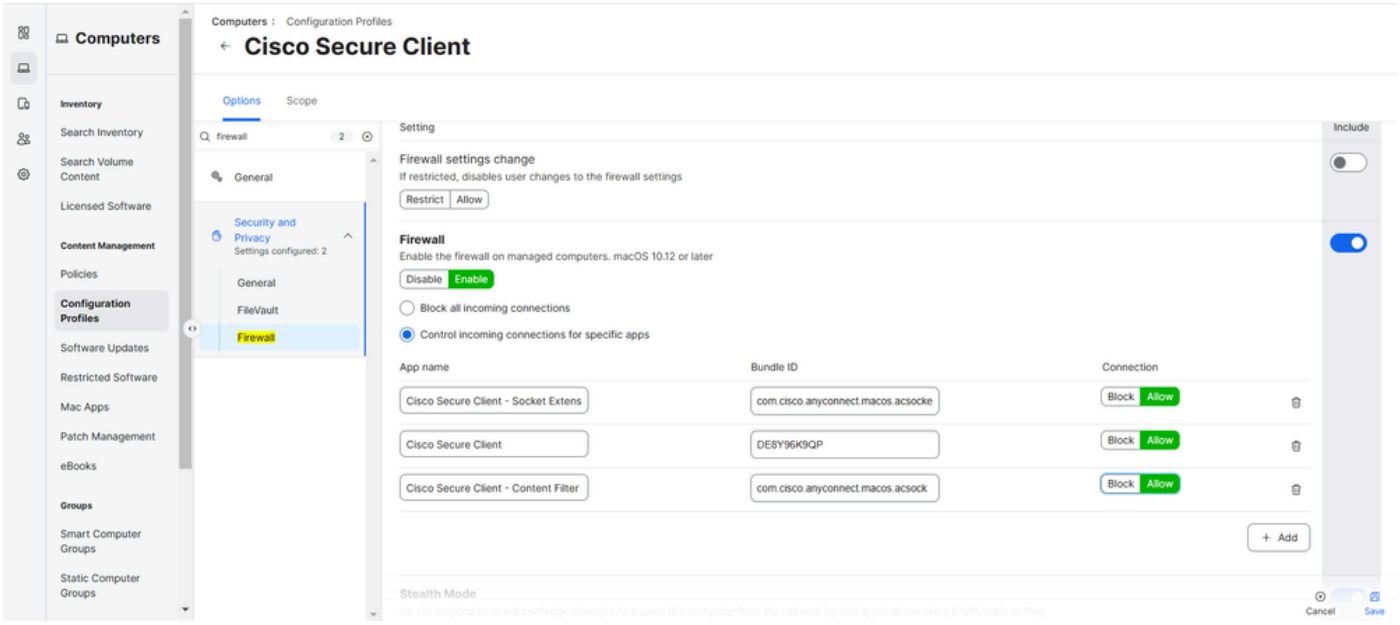
1. Navigeer naar Computers > Contentbeheer > Configuratieprofielen.

2. Selecteer uw Cisco Secure Client-configuratieprofiel en zoek Beveiliging en privacy.

3. Configureer het met de volgende instellingen:

- Firewall: inschakelen - Inkomende verbindingen voor specifieke apps beheren

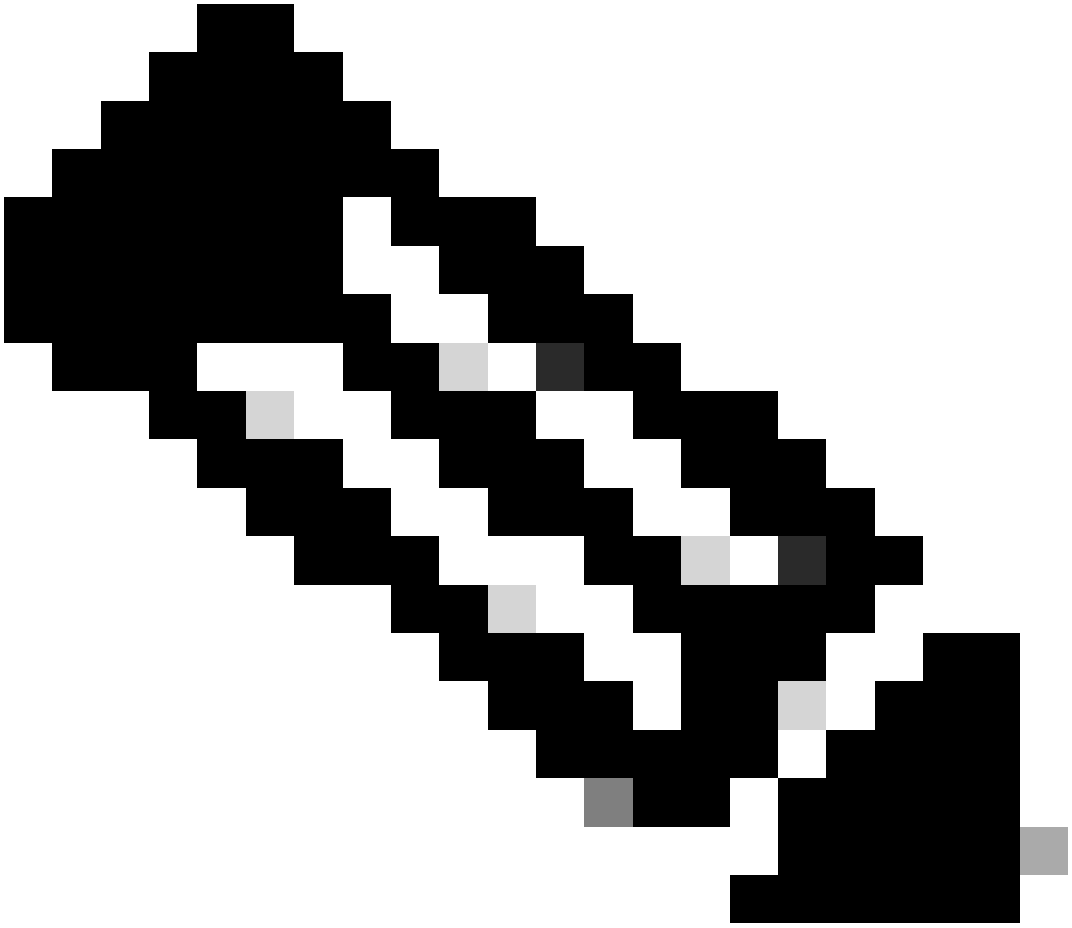
App-naam	Bundle-ID
Cisco Secure Client - Socket Extensions	com.cisco.anyconnect.macos.acsockext
Cisco Secure Client	DE8Y96K9QP
Cisco Secure Client - Inhoudsfilter	com.cisco.anyconnect.macos.acsock



4. Selecteer Opslaan.

5. Als u wordt gevraagd om herverdelingsopties, selecteert u Distribueren naar iedereen om de wijzigingen onmiddellijk naar uw gewenste macOS-apparaten te verplaatsen.

Het Cisco Umbrella Root-certificaat implementeren



Opmerking: deze stap is alleen van toepassing op nieuwe implementaties van Cisco Secure Client of apparaten waarvoor het Cisco Umbrella Root Certificate niet eerder is geïmplementeerd. Als u overstapt van de Umbrella Roaming Client of Cisco AnyConnect 4.10-client en/of het Cisco Umbrella Root Certificate al in het verleden hebt geïmplementeerd, kunt u dit gedeelte overslaan.

Download het Cisco Umbrella Root Certificate van Policies > Root Certificate in het Umbrella-dashboard.

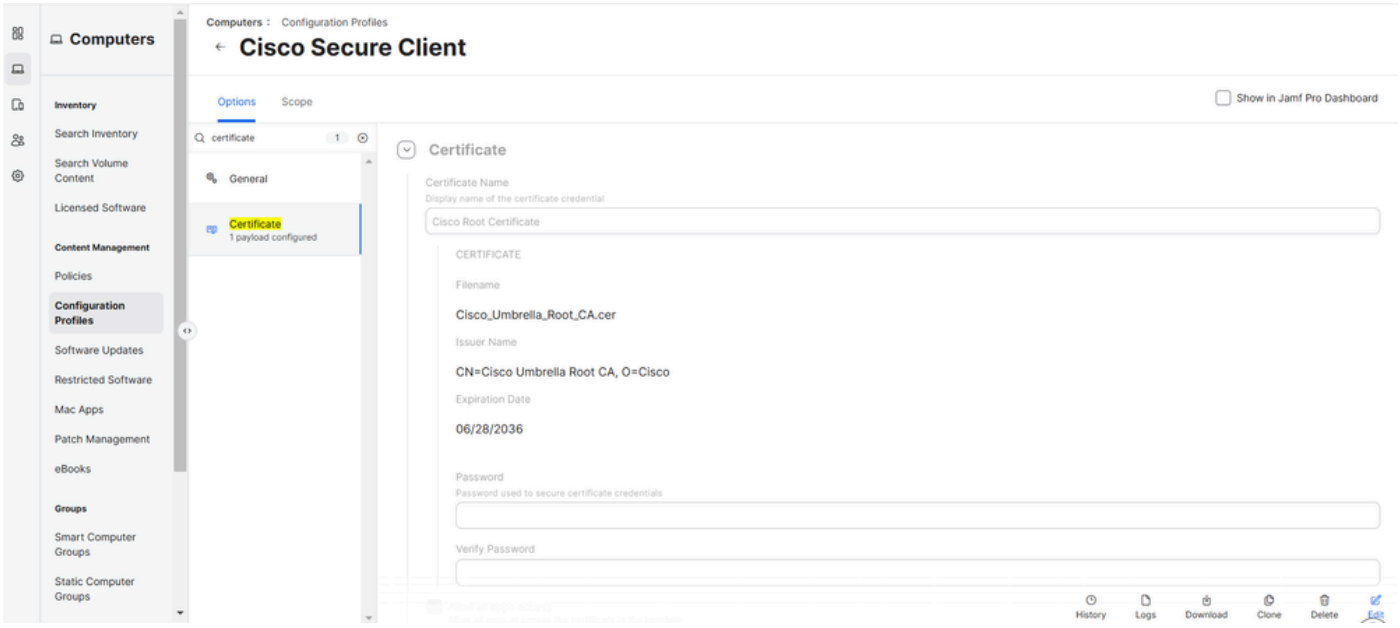
1. Download het Cisco Umbrella Root Certificate in het Umbrella-dashboard onder Beleid > Hoofdcertificaat.

2. Ga in JAMF naar Computers > Configuratieprofielen > Cisco Secure Client > Bewerken.

3. Zoeken naar certificaat > Configureren. Geef het een unieke naam.

4. Selecteer onder Certificaatoptie selecteren de optie Uploaden en het Cisco Umbrella Root Certificate uploaden dat u eerder in stap 1 hebt gedownload.

5. Zorg ervoor dat u hier geen wachtwoord configureert en selecteer Opslaan.



6. Als u wordt gevraagd om herverdelingsopties, selecteert u Distribueren naar iedereen om de wijzigingen onmiddellijk naar uw gewenste macOS-apparaten te verplaatsen.

Verificatie

Als u wilt controleren of Cisco Secure Client met Umbrella-module werkt, bladert u naar https://policy-debug.checkumbrella.com of voert u deze opdracht uit:

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

Elk van beide output moet unieke en relevante informatie bevatten voor uw overkoepelende organisatie, zoals uw OrgID.

Workaround voor macOS 14.3

Voor macOS 14.3 (of hoger) met Cisco Secure Client 5.1.x, als u tegenkomt dat "de VPN-client agent het interprocescommunicatiedepot niet kon maken":

1. Navigeer in JAMF naar Instellingen > Computerbeheer > Scripts > Nieuw.

2. Geef het een unieke naam en definieer uw categorie.

3. Navigeer naar het tabblad Script en voeg dit toe:

```
#!/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. Zorg er onder Opties voor dat de prioriteit is ingesteld op Na. Dit bash-script controleert of de Cisco Secure Client - AnyConnect VPN service.app wordt uitgevoerd via het retourneren van een verwachte uitvoer met de proces-ID van `pgrep -fl`.

- Als een lege uitvoer wordt geretourneerd, kunt u bevestigen dat de `Cisco Secure Client - AnyConnect VPN service.app` niet wordt uitgevoerd en dat het script wordt uitgevoerd om de Cisco Secure Client-kernservices te starten die nodig zijn om de overkoepelende module correct uit te voeren.

Automatische updates

Cisco heeft besloten de ondersteuning voor automatische updates van het Umbrella-dashboard uit te breiden met Secure Client vanaf Secure Client 5.1.6.103 (MR6). In de toekomst kunnen klanten die een upgrade hebben uitgevoerd naar ten minste Cisco Secure Client 5.1.6 MR6 automatisch updaten naar nieuwere versies als de automatische update is geconfigureerd in het Umbrella-dashboard.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.