Déployer CSC sur macOS à l'aide de JAMF avec module Umbrella

Table des matières

Introduction

Ce document décrit comment déployer Cisco Secure Client avec le module Umbrella sur des périphériques macOS gérés à l'aide de JAMF.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

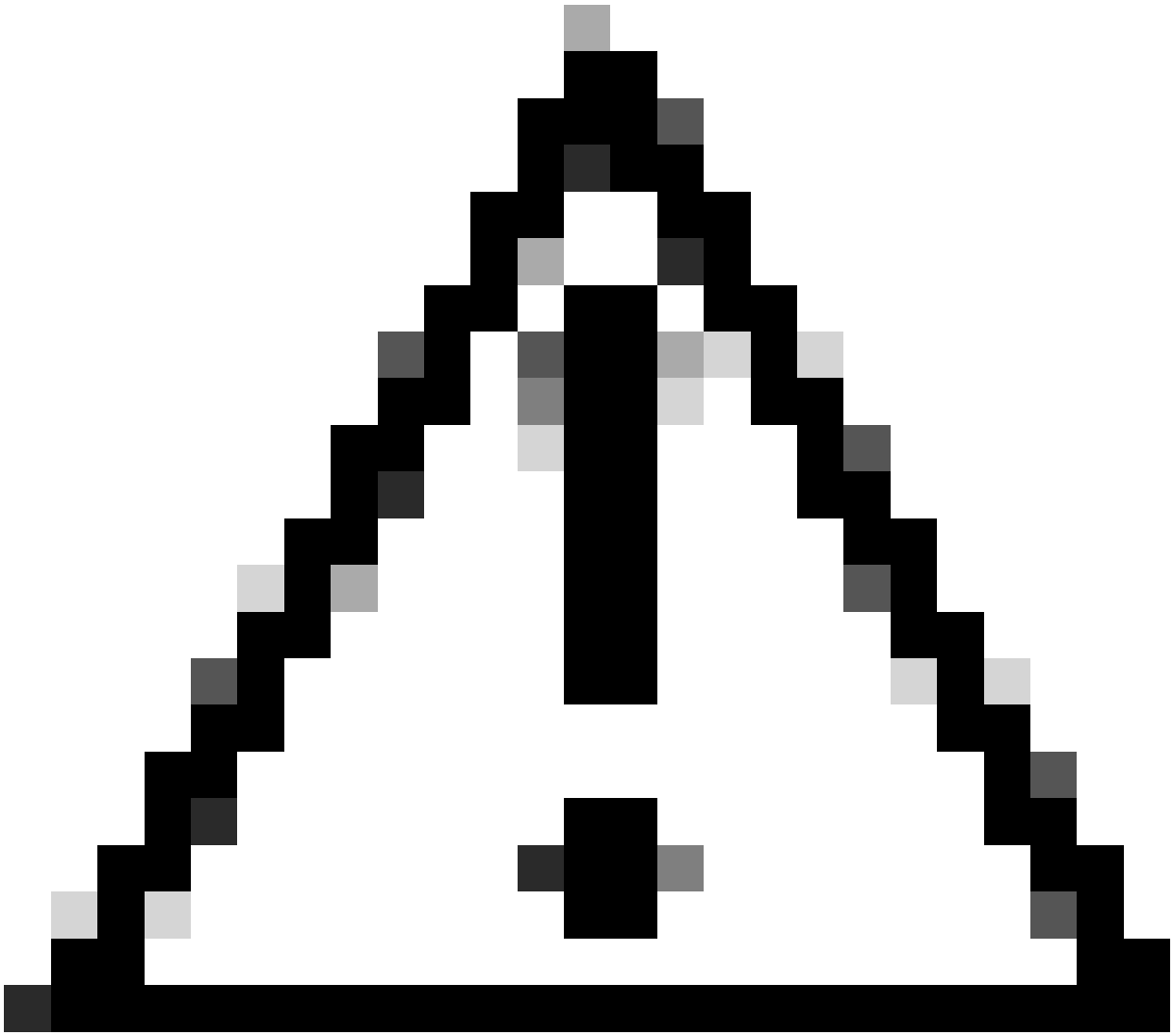
- Les périphériques macOS doivent être gérés par JAMF.
- Pour obtenir des instructions d'inscription MDM pour macOS, reportez-vous à la documentation JAMF.

Composants utilisés

Les informations contenues dans ce document sont basées sur Cisco Secure Client.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.



Mise en garde : Cet article est fourni en l'état au 1er février 2025. L'assistance Cisco Umbrella ne garantit pas que ces instructions sont valides après cette date et sujettes à modification en fonction des mises à jour de JAMF et d'Apple.

Télécharger le package d'installation (PKG)

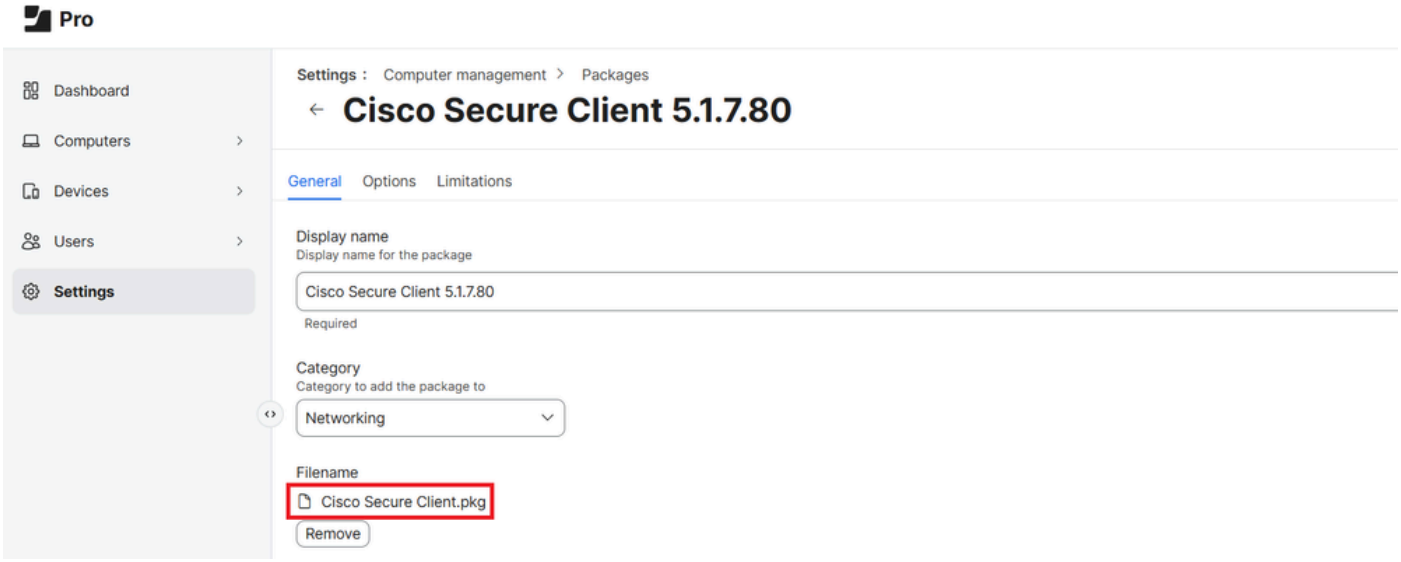
1. Téléchargez Cisco Secure Client DMG depuis le tableau de bord Umbrella sous Déploiements > Ordinateurs itinérants > Client itinérant > Package de prédéploiement > macOS.

2. Connectez-vous à votre instance de cloud JAMF Pro.

3. Accédez à Paramètres > Gestion de l'ordinateur > Packages > Nouveau.

4. Téléchargez le PKG extrait du package DMG que vous avez téléchargé depuis votre tableau de

bord Umbrella.

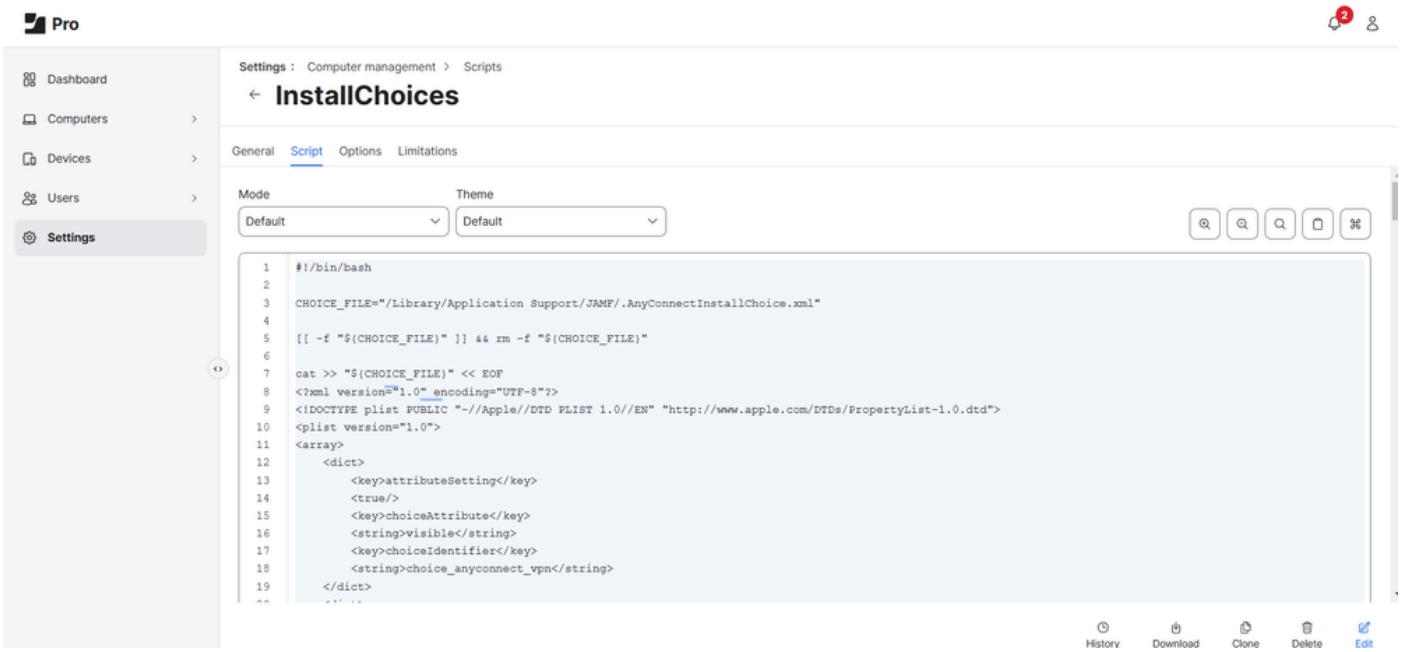


Ajouter des scripts de configuration et de sélection de module

1. Accédez à Paramètres > Gestion de l'ordinateur > Scripts et ajoutez ce script pour contrôler les modules installés au cours du déploiement.

2. Vous pouvez contrôler l'installation des modules Secure Client en définissant un module sur 0 pour l'ignorer ou sur 1 pour l'installer, car le PKG est configuré pour installer tous les modules par défaut.

- Vous pouvez obtenir l'exemple de fichier XML à partir de la documentation Umbrella : Customize macOS installation of Cisco Secure Client
- Umbrella a également ajouté le script « installchoice » à ce lien github. Dans cet exemple, les modules Core VPN, Umbrella et DART sont définis sur 1 et peuvent être inclus dans l'installation du client sécurisé.



3. Accédez à Settings > Computer management > Scripts et ajoutez ce script afin qu'il crée un fichier de configuration `Orginfo.json` qui est requis par Cisco Secure Client.

- Téléchargez le profil de module directement à partir du tableau de bord Umbrella, puis ajoutez l'ID d'organisation, l'empreinte digitale et l'ID d'utilisateur au script :

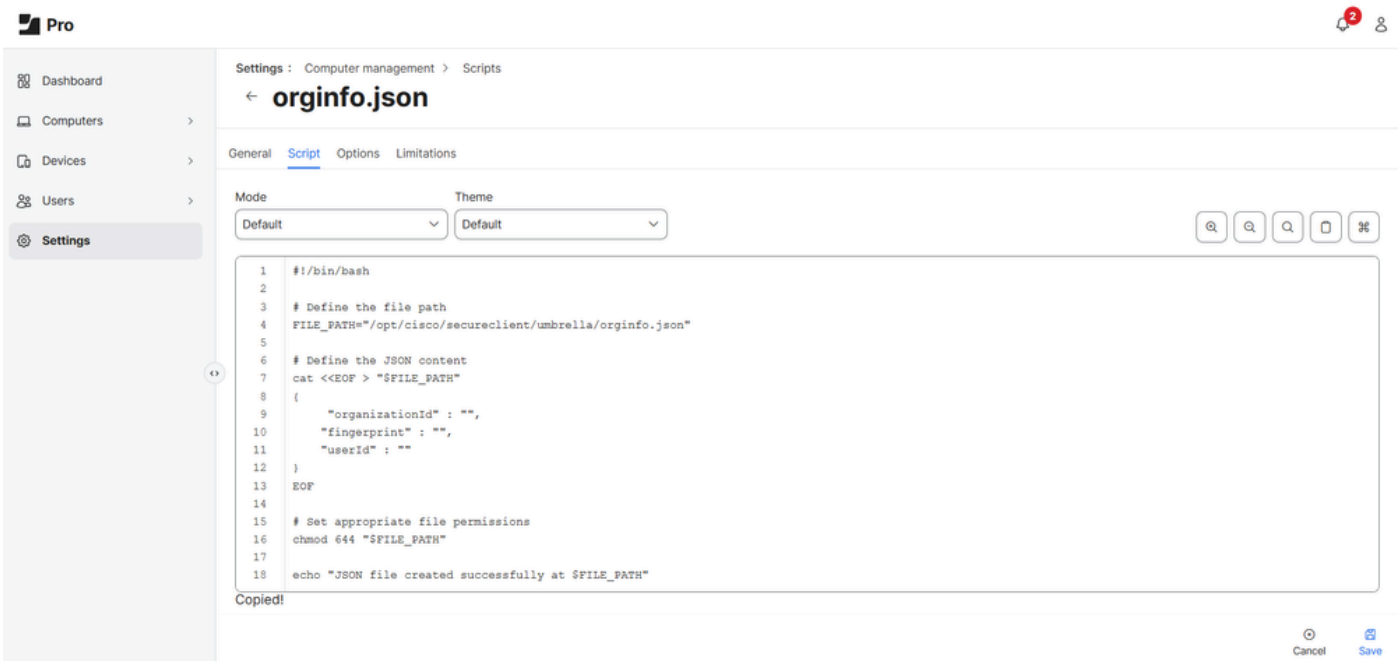
```
#!/bin/bash

# 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

Création de la stratégie JAMF

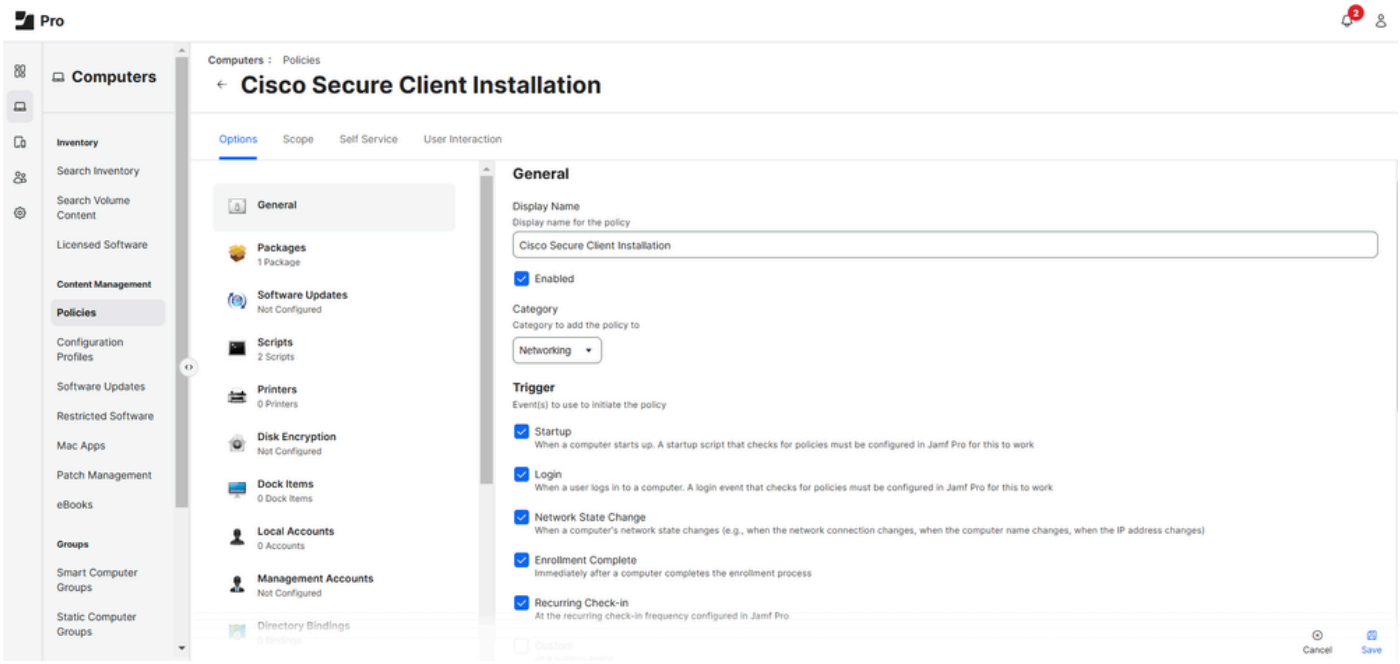
La politique JAMF est utilisée pour déterminer comment et quand le client sécurisé Cisco avec le module Umbrella est expulsé.

1. Accédez à Ordinateurs > Gestion de contenu > Stratégies > Nouveau.

2. Attribuez un nom unique à la règle et sélectionnez les événements Category et Trigger souhaités (par exemple, lorsque cette règle est exécutée).

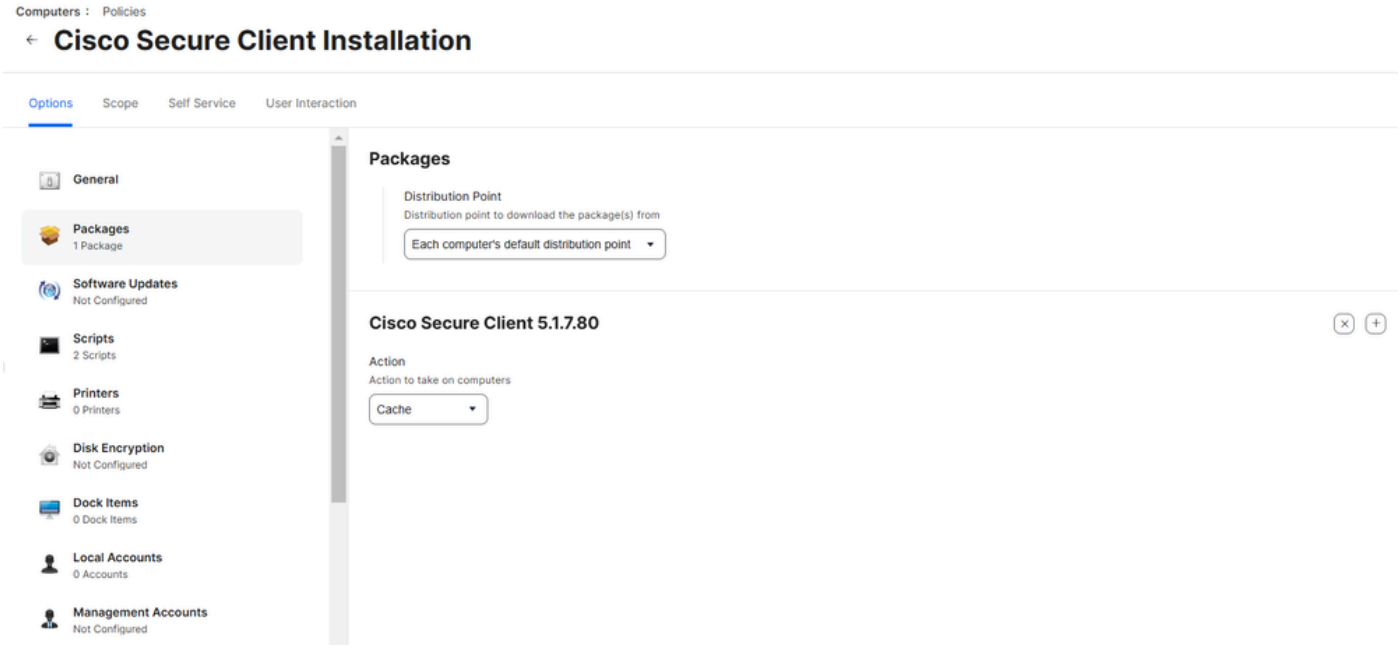
3. Vous pouvez éventuellement configurer une commande personnalisée qui peut être exécutée sous Personnalisé. La commande permettant d'exécuter et d'exécuter cette stratégie ressemblerait à ceci :

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

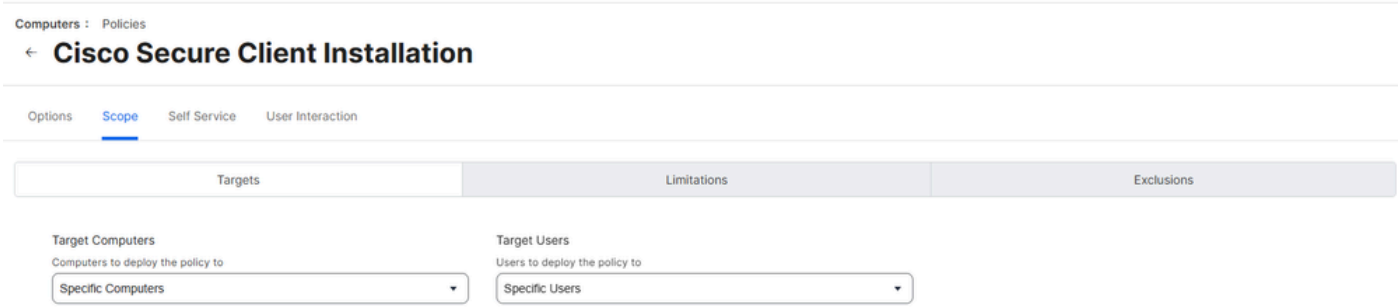


4. Sélectionnez Packages > Configure et sélectionnez Add en regard de votre package Cisco Secure Client.

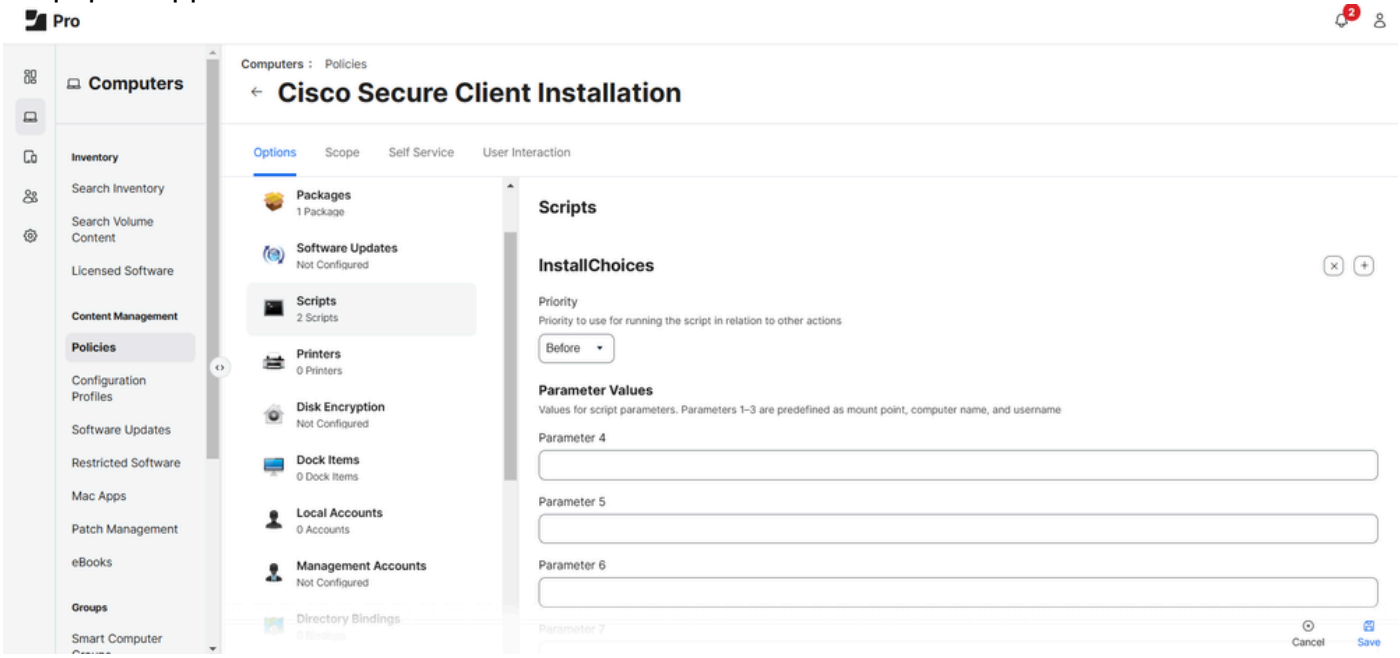
- Sous Point de distribution, sélectionnez le point de distribution par défaut de chaque ordinateur.
- Sous Action, sélectionnez Cache.

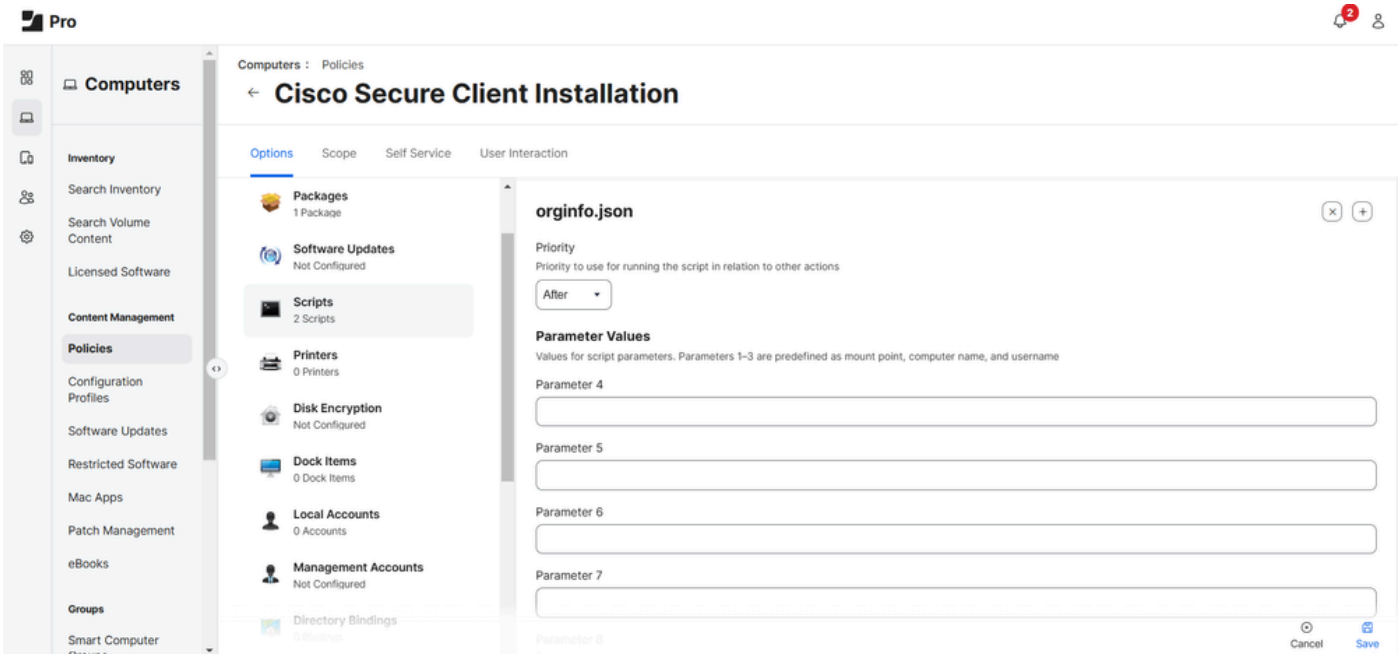


5. Définissez l'étendue des périphériques ou des utilisateurs à déployer et sélectionnez Enregistrer.



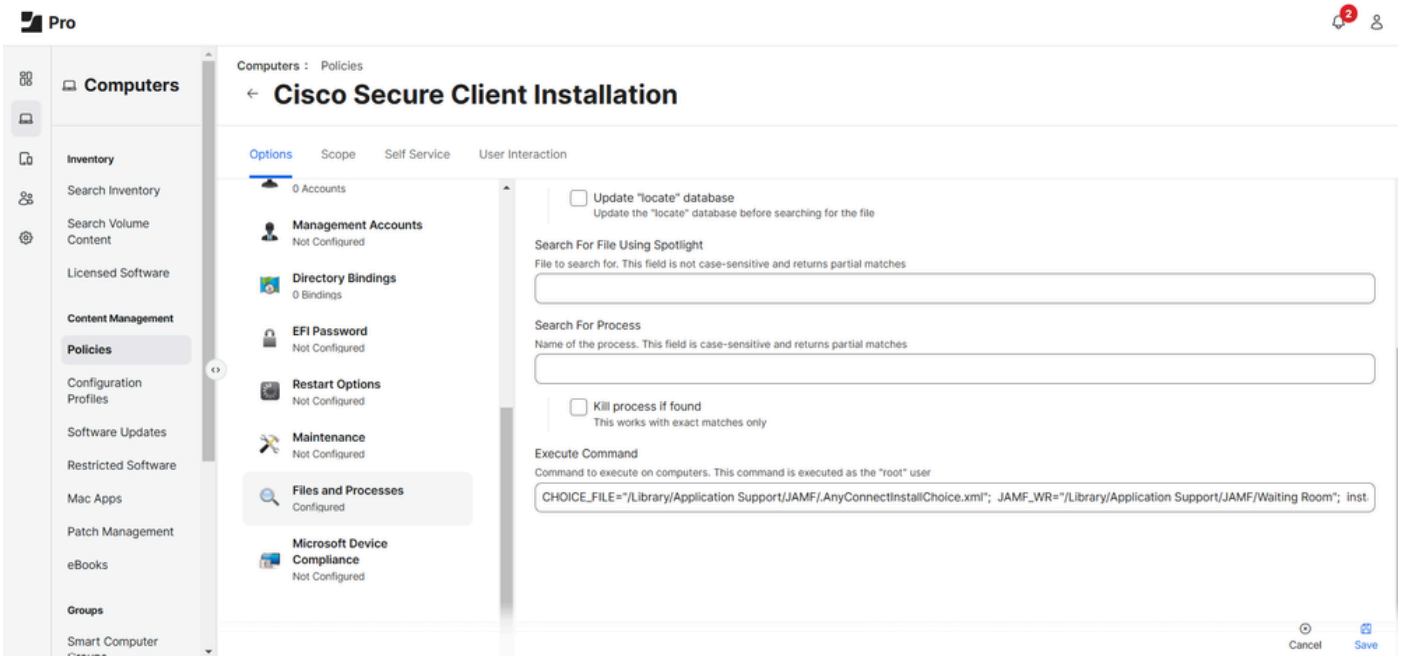
6. Ajoutez les`InstallChoices`scripts et **`orginfo.json`** et donnez-leur une priorité à utiliser pour exécuter le script par rapport à d'autres actions.





7. Exécutez cette commande pour installer le package Cisco Secure Client avec les modules sélectionnés sur les périphériques :

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



Configuration d'une installation silencieuse de l'extension système

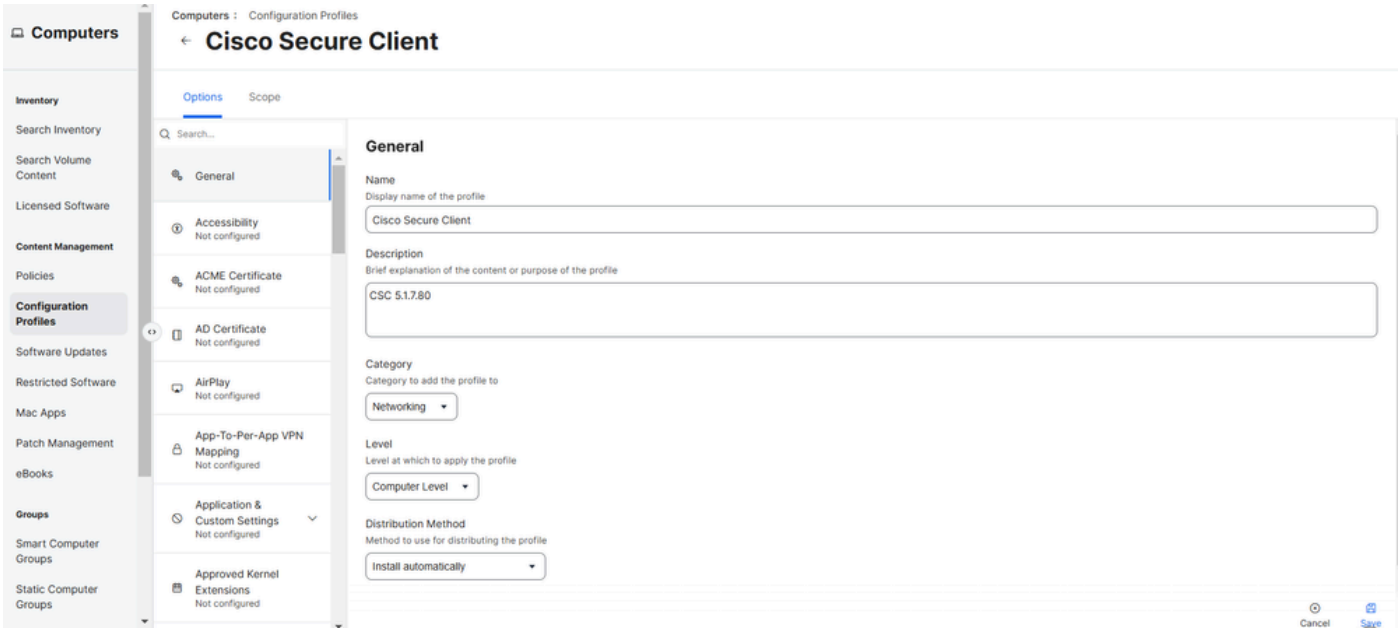
Ensuite, utilisez JAMF pour configurer et autoriser les extensions système requises par Cisco

Secure Client afin que Cisco Secure Client avec le module Umbrella s'exécute correctement sans interaction de l'utilisateur.

1. Accédez à Ordinateurs > Gestion de contenu > Profils de configuration > Nouveau.

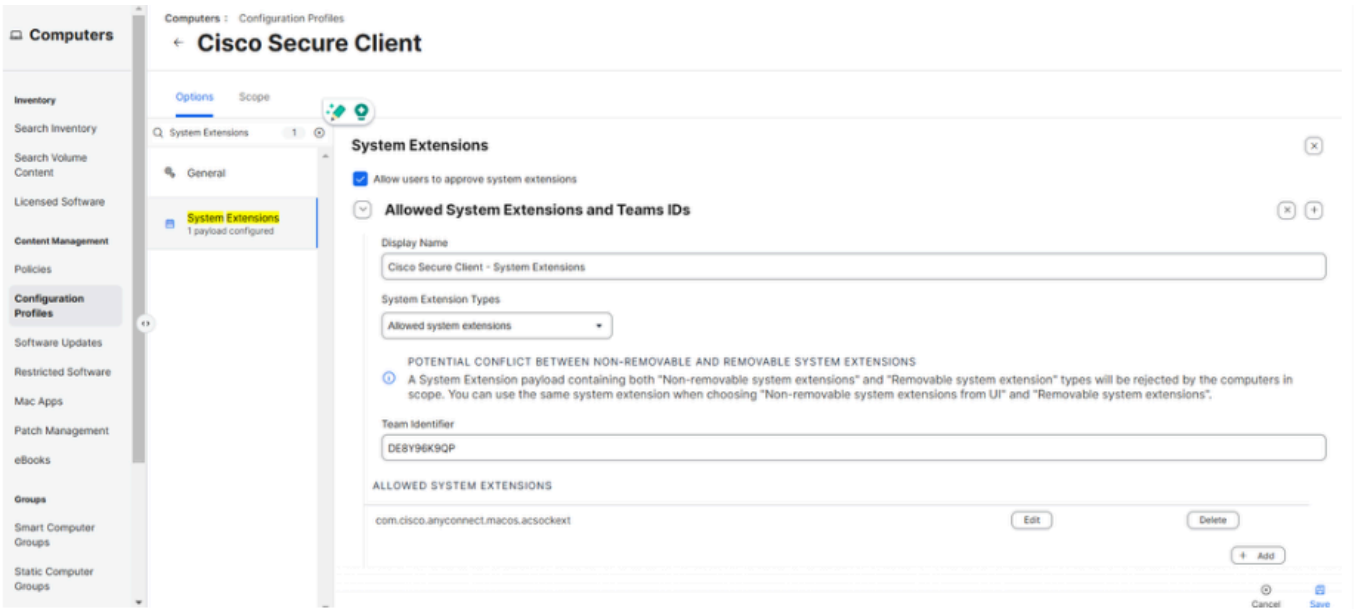
2. Attribuez un nom unique au profil et sélectionnez votre catégorie et votre mode de distribution.

3. Assurez-vous queLevel est défini sur Computer Level.



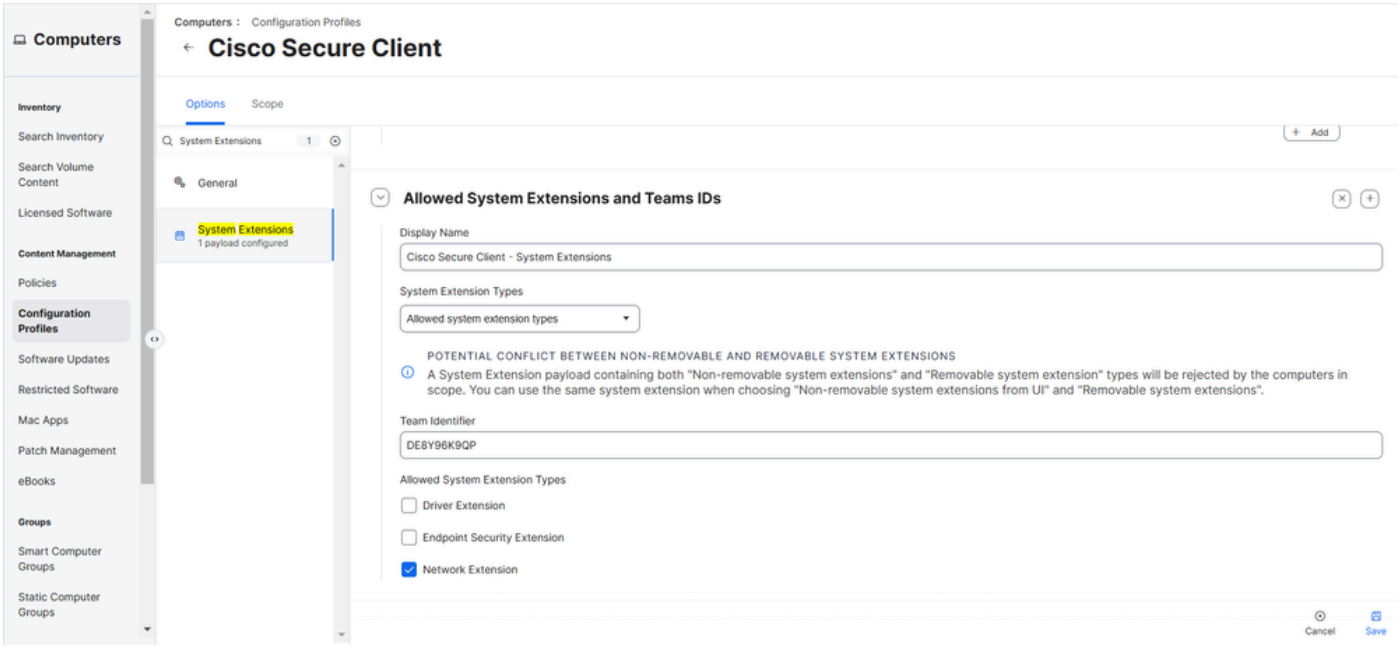
4. Recherchez System Extensions > Configure. Entrez les valeurs suivantes :

- Nom complet : Client sécurisé Cisco - Extensions système
- Types d'extensions système : Extensions système autorisées
- Identifiant de l'équipe : DE8Y96K9QP
- Extensions système autorisées : com.cisco.anyconnect.macos.acsockext, puis sélectionnez Enregistrer.



5. Cliquez sur l'icône + en regard de ID d'équipe autorisés et de postes système pour ajouter un autre poste système. Saisissez ensuite les valeurs suivantes :

- Nom complet : Client sécurisé Cisco - Extensions système
- Types d'extensions système : Autoriser les types d'extensions système
- Identifiant de l'équipe : DE8Y96K9QP
- Autoriser les types d'extensions système : Extension du réseau



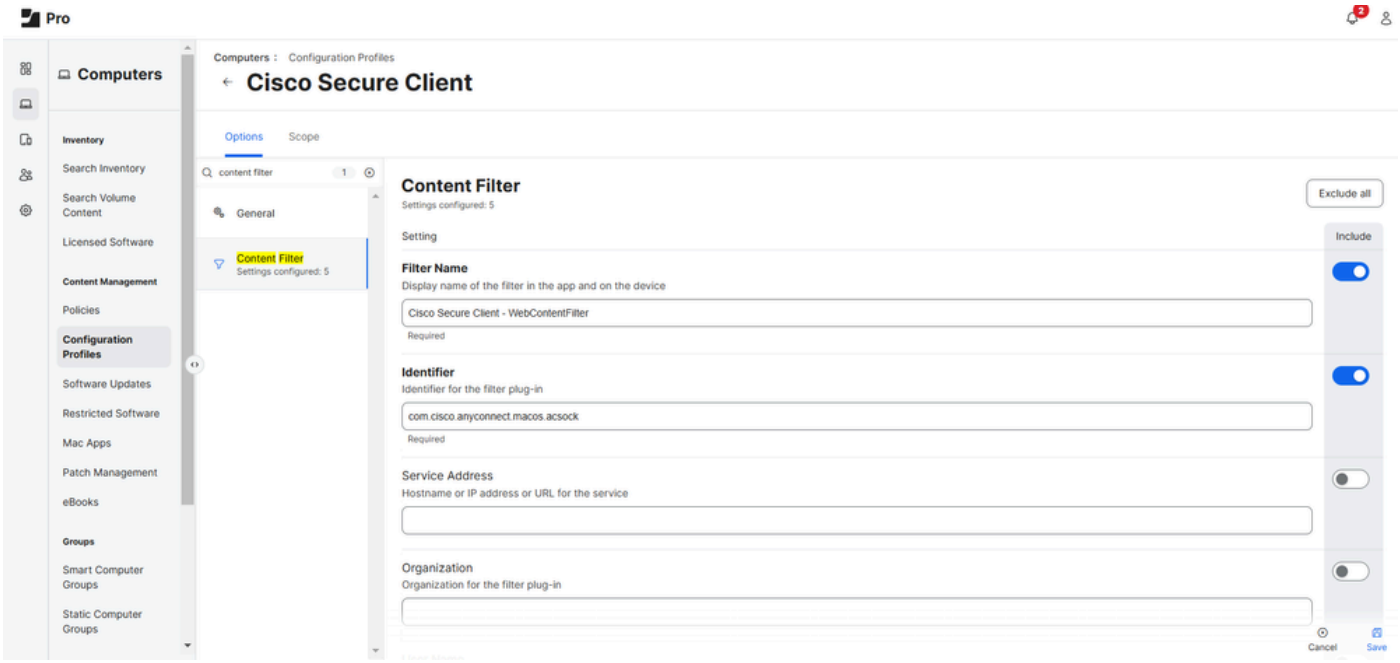
Configurer l'installation silencieuse pour le filtre de contenu

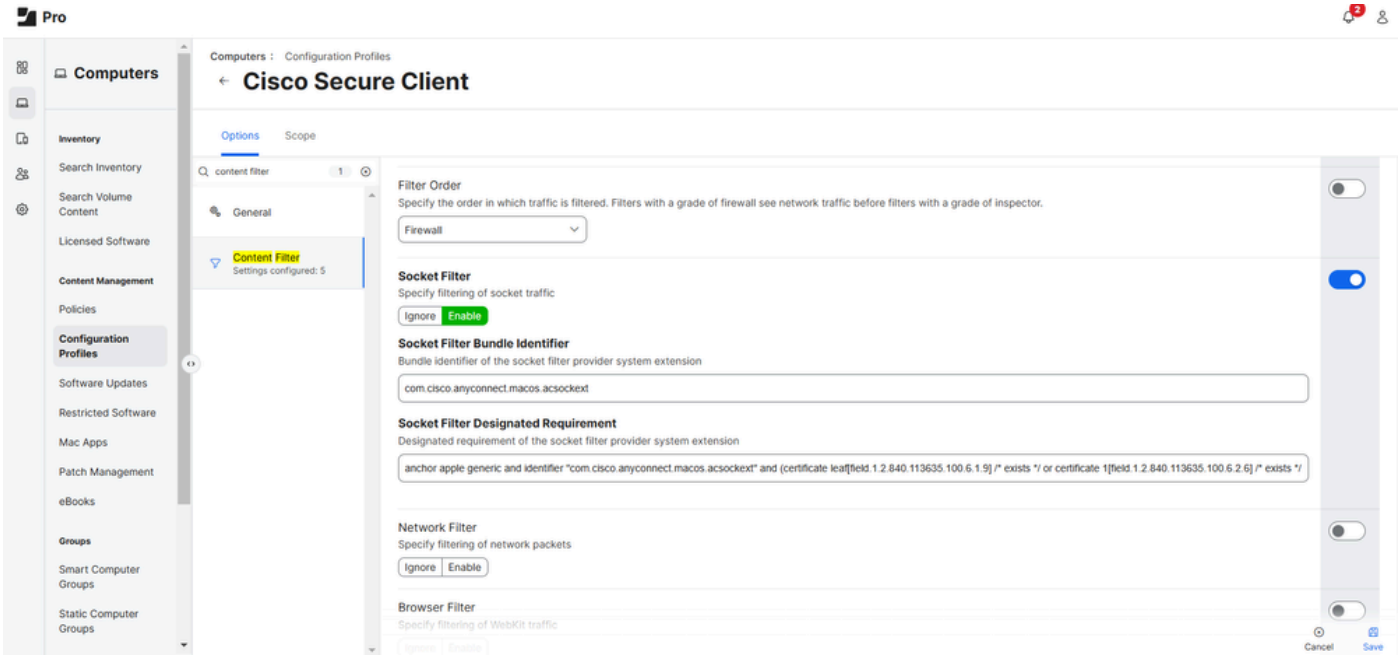
Configurez ensuite une installation silencieuse pour le filtre de contenu, qui est en corrélation avec le filtre de socket du module Cisco Secure Client with Umbrella :

1. Recherchez le filtre de contenu. Activez et renseignez ces champs avec leurs valeurs respectives :

- Nom du filtre : Client sécurisé Cisco - WebContentFilter
- Identifiant: com.cisco.anyconnect.macos.acsock
- Filtre de socket : Activée
- Identificateur d'ensemble de filtre de socket : com.cisco.anyconnect.macos.acsockext
- Filtre de prise Exigence désignée :

```
anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* existing */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* existing */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* existing */ and certificate leaf[subject.OU] = DE8Y96K9QP)
```





2. Sous Données personnalisées, sélectionnez Ajouter cinq fois et entrez les valeurs suivantes :

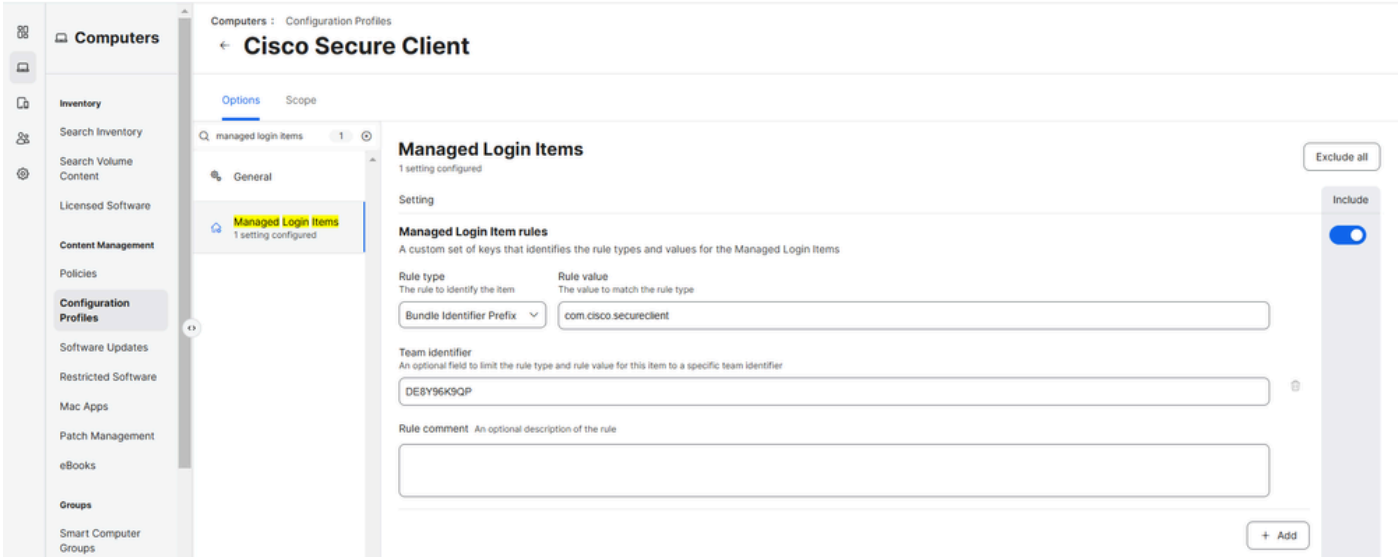
Key (Clé)	Valeur
FiltreAutomatiqueActivé	falsifié
FiltrerNavigateurs	falsifié
FilterSockets	vrai
PaquetsFiltres	falsifié
CatégorieFiltre	cloison pare-feu

Configurer les éléments de connexion gérés

La configuration des éléments de connexion gérés pour le module Cisco Secure Client with Umbrella permet de s'assurer que Cisco Secure Client démarre au démarrage du périphérique.

Pour configurer, recherchez Managed Login Items et configurez les champs avec ces valeurs :

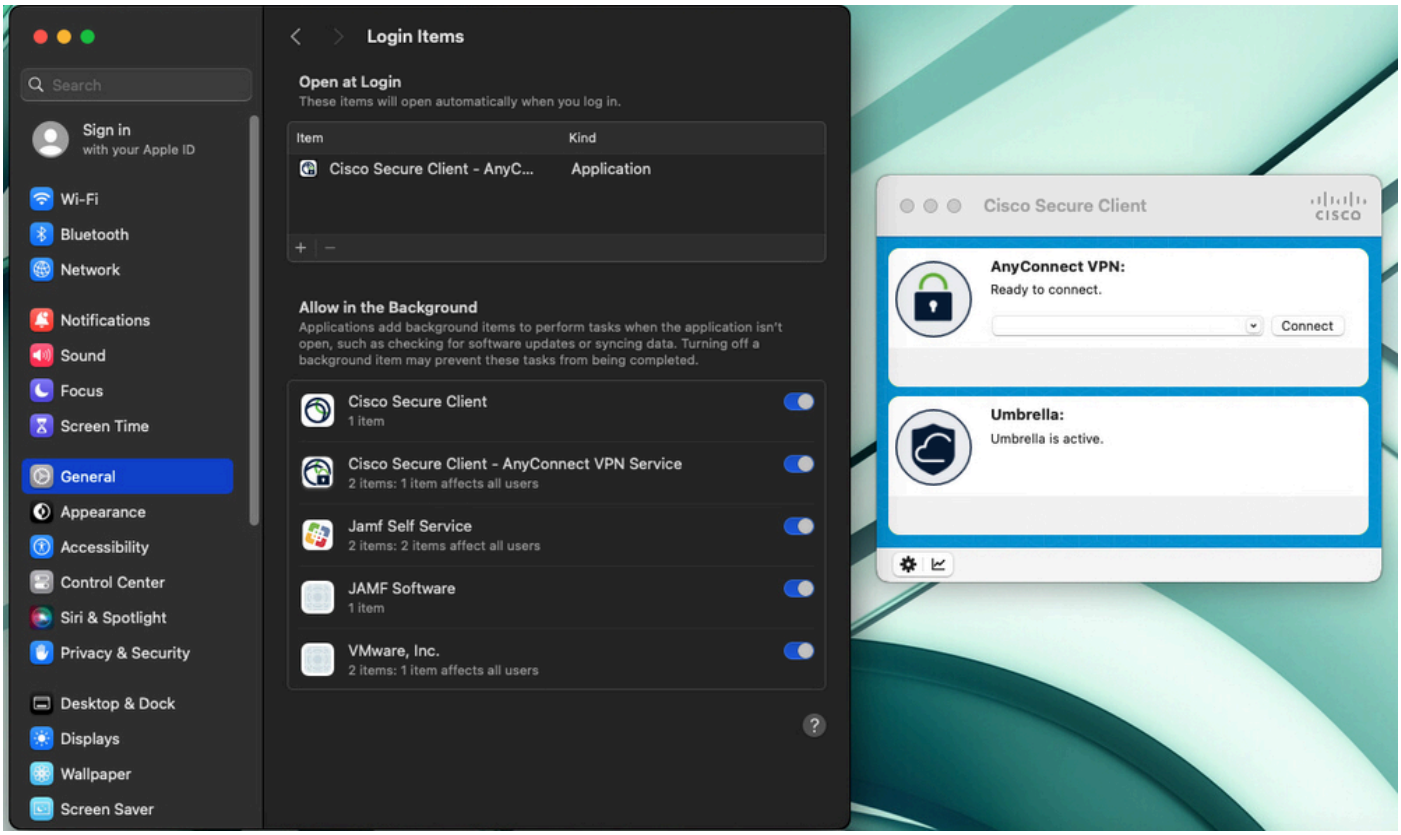
- Type de règle : Préfixe d'identificateur de bundle
- Valeur de la règle : com.cisco.secureclient
- Identifiant de l'équipe : DE8Y96K9QP

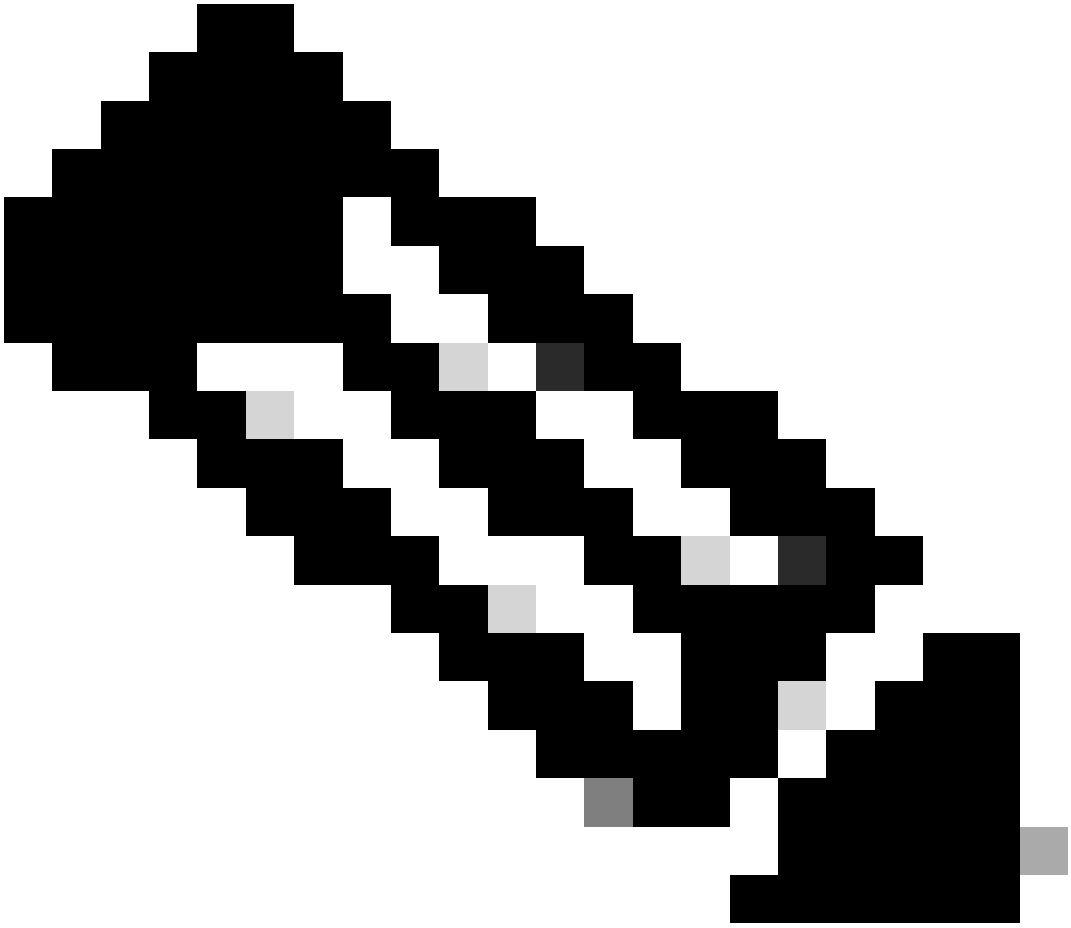


Attribuer une étendue et pousser le déploiement

1. Accédez à Portée et définissez la portée pour les périphériques ou les utilisateurs.

2. Le module Cisco Secure Client with Umbrella peut être poussé vers les périphériques macOS souhaités lorsque l'un des déclencheurs que vous avez configurés à l'étape 2 de Create a JAMF Policy est activé. Vous pouvez également le diffuser via le portail en libre-service de 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.



Remarque : Même si un utilisateur tente de désactiver le proxy DNS ou le proxy transparent dans les paramètres système (Réseau > Filtre), il est automatiquement réactivé par défaut car le filtre de contenu est activé via JAMF comme décrit dans cet article et ne peut pas être désactivé.

Configuration de l'exception macOS Firewall

Si le pare-feu macOS est configuré pour Bloquer toutes les connexions entrantes, vous devez également ajouter le client sécurisé Cisco et ses composants à sa liste d'exceptions :

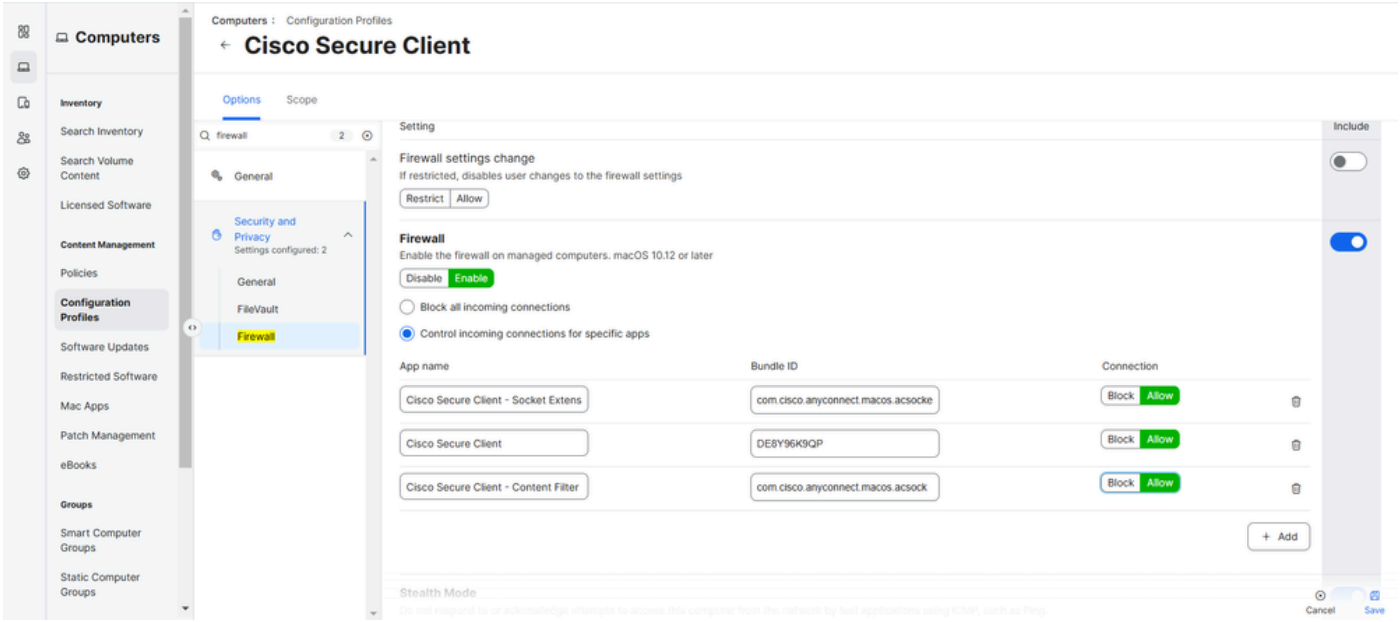
1. Accédez à Ordinateurs > Gestion de contenu > Profils de configuration.

2. Sélectionnez votre profil de configuration Cisco Secure Client et recherchez Sécurité et confidentialité.

3. Configurez-le avec les paramètres suivants :

- Pare-feu : Activer - Contrôler les connexions entrantes pour des applications spécifiques

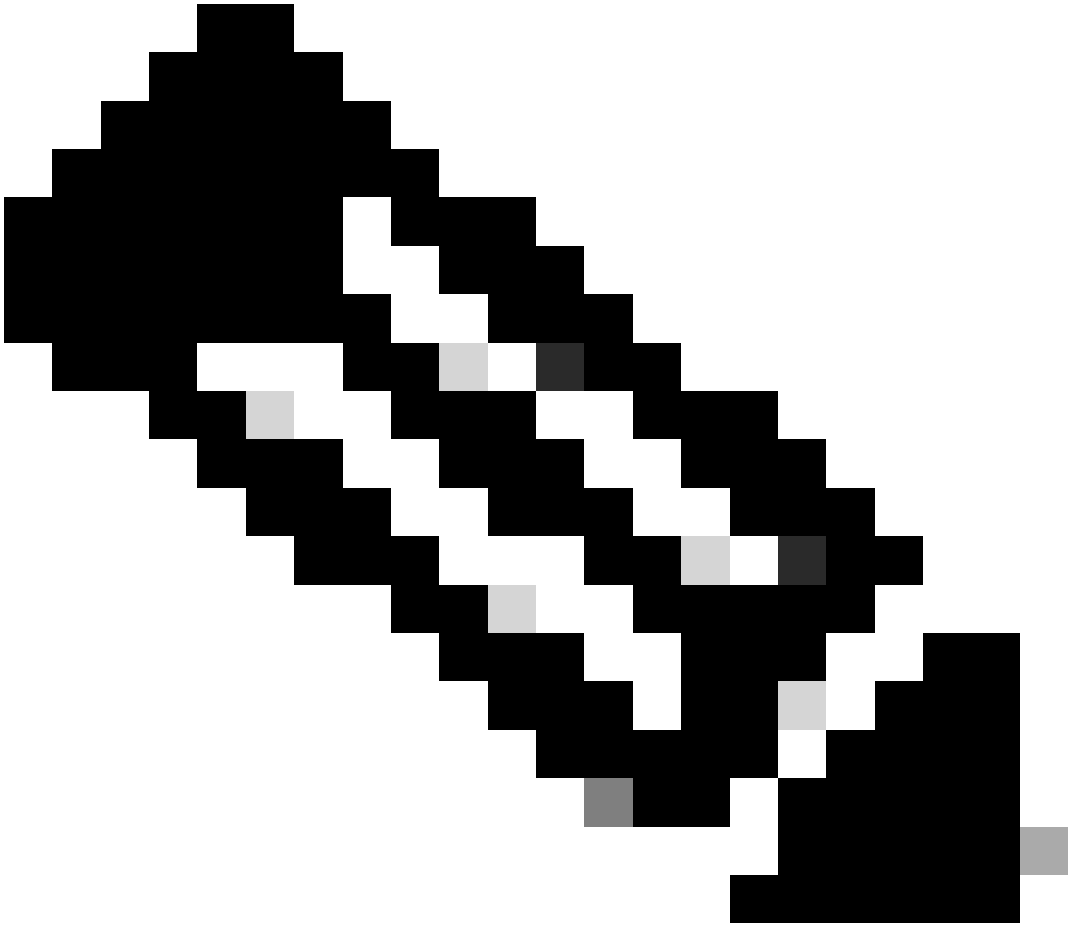
Nom de l'application	ID d'offre
Client sécurisé Cisco - Extensions de sockets	com.cisco.anyconnect.macos.acsockext
Client sécurisé Cisco	DE8Y96K9QP
Client sécurisé Cisco - Filtre de contenu	com.cisco.anyconnect.macos.acsock



4. Sélectionnez Enregistrer.

5. Si vous êtes invité avec Options de redistribution, sélectionnez Distribuer à tous pour diffuser immédiatement les modifications vers vos périphériques macOS souhaités.

Déployer le certificat racine Cisco Umbrella



Remarque : Cette étape ne s'applique qu'aux nouveaux déploiements de Cisco Secure Client ou de périphériques pour lesquels le certificat racine Cisco Umbrella n'a pas été déployé précédemment. Si vous effectuez une migration à partir du client d'itinérance Umbrella ou du client Cisco AnyConnect 4.10 et/ou si vous avez déjà déployé le certificat racine Cisco Umbrella dans le passé, vous pouvez ignorer cette section.

Téléchargez le certificat racine Cisco Umbrella à partir de Politiques > Certificat racine dans le tableau de bord Umbrella.

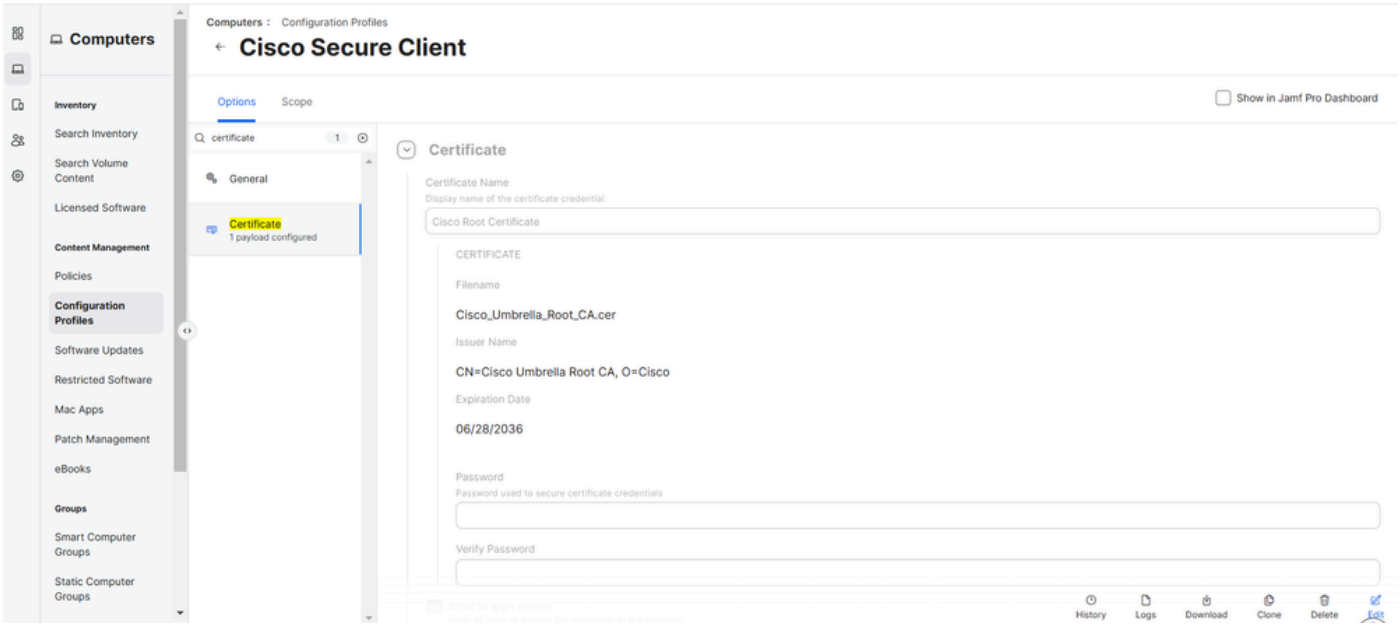
1. Dans le tableau de bord Umbrella, sous Policies > Root Certificate, téléchargez le certificat racine Cisco Umbrella.

2. Dans JAMF, accédez à Computers > Configuration Profiles > Cisco Secure Client > Edit.

3. Recherchez Certificate > Configure. Donnez-lui un nom unique.

4. Sous Select Certificate Option, sélectionnez Upload et téléchargez le certificat racine Cisco Umbrella que vous avez téléchargé précédemment à l'étape 1.

5. Assurez-vous que vous ne configurez pas de mot de passe ici et sélectionnez Enregistrer.



6. Si vous êtes invité à saisir les Options de redistribution, sélectionnez Distribuer à tous pour répercuter immédiatement les modifications sur les périphériques macOS souhaités.

Vérification

Pour vérifier si le module Cisco Secure Client with Umbrella fonctionne, accédez à https://policy-debug.checkumbrella.com ou exécutez cette commande :

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

Chaque sortie doit contenir des informations uniques et pertinentes pour votre organisation parapluie, telles que votre OrgID.

Solution pour macOS 14.3

Pour macOS 14.3 (ou version ultérieure) avec Cisco Secure Client 5.1.x, si vous rencontrez « L'agent client VPN n'a pas pu créer le dépôt de communication interprocessus » :

1. Dans JAMF, accédez à Paramètres > Gestion de l'ordinateur > Scripts > Nouveau.

2. Donnez-lui un nom unique et définissez votre catégorie.

3. Accédez à l'onglet Script et ajoutez ceci :

```
#!/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. Sous Options, vérifiez que la priorité est définie sur Après. Ce script bash vérifie si le client sécurisé Cisco - AnyConnect VPN service.app est en cours d'exécution en retournant une sortie attendue avec l'ID de processus de `pgrep -fl`.

- S'il renvoie une sortie vide, alors vous pouvez confirmer que le `client sécurisé Cisco - service VPN AnyConnect.app` n'est pas en cours d'exécution et le script s'exécute pour lancer les services de base du client sécurisé Cisco qui sont nécessaires pour que le module Umbrella fonctionne correctement.

Mises à jour automatiques

Cisco a décidé d'étendre la prise en charge de la mise à jour automatique à partir du tableau de bord Umbrella pour inclure le client sécurisé à partir de la version 5.1.6.103 (MR6). À l'avenir, les clients qui ont effectué une mise à niveau vers au moins Cisco Secure Client 5.1.6 MR6 peuvent effectuer une mise à jour automatique vers des versions plus récentes si la mise à jour automatique a été configurée dans le tableau de bord Umbrella.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.