Umbrellaモジュール付きJAMFを使用したCSCのmacOSへの導入

内容

はじめに

このドキュメントでは、JAMFを使用して、Umbrellaモジュールを搭載したCisco Secure Clientを管理対象のmacOSデバイスに導入する方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

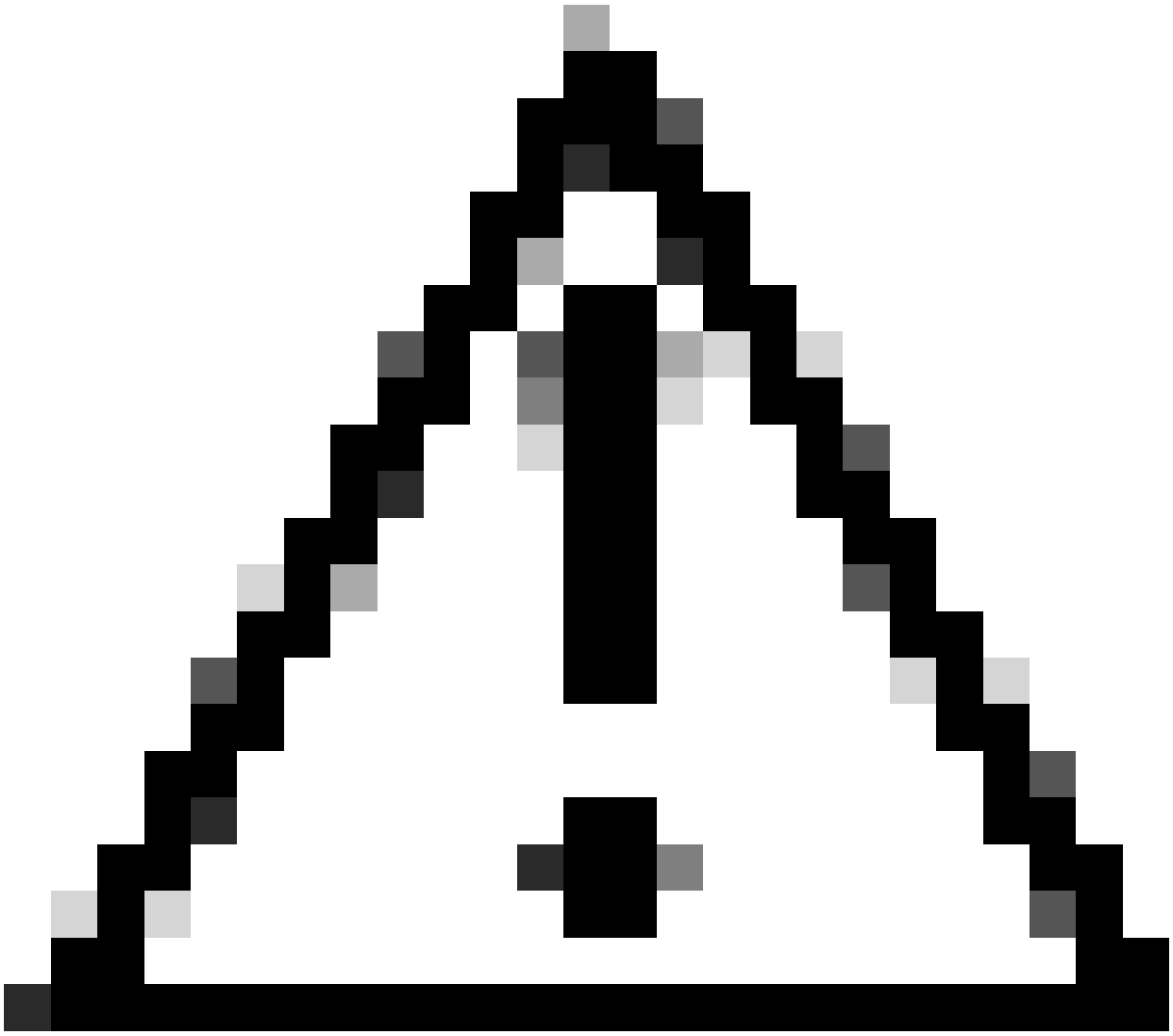
- macOSデバイスはJAMFによって管理される必要があります。
- macOSのMDM登録手順については、JAMFのドキュメントを参照してください。

使用するコンポーネント

このドキュメントの情報は、Cisco Secure Clientに基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。



注意：この記事は2025年2月1日の時点でそのまま提供されています。Cisco Umbrellaサポートでは、これらの手順がこの日付以降に有効であることを保証しません。また、JAMFおよびAppleからのアップデートに基づいて手順が変更される場合があります。

インストールパッケージ(PKG)のアップロード

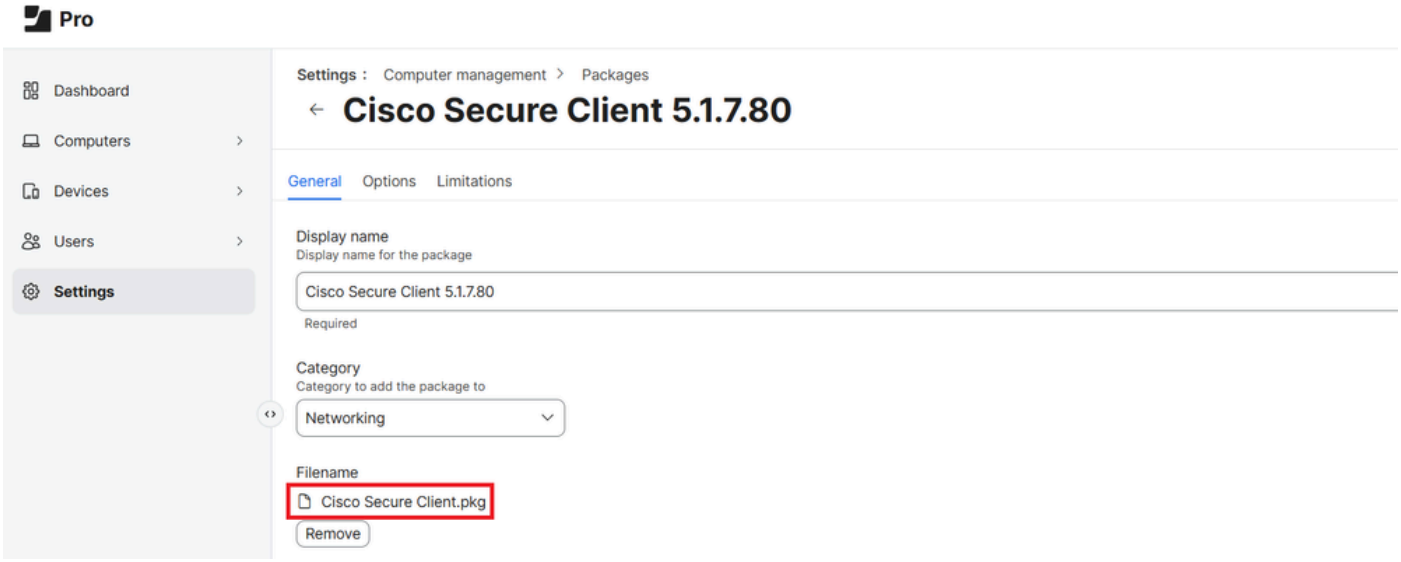
1. UmbrellaダッシュボードのDeployments > Roaming Computers > Roaming Client > Pre-Deployment Package > macOSの下から、Cisco Secure Client DMGをダウンロードします。

2. JAMF Proクラウドインスタンスにログインします。

3. [設定] > [コンピューターの管理] > [パッケージ] > [新規]に移動します。

4. Umbrellaダッシュボードからダウンロードした DMGパッケージから抽出したパッケージをアッ

プロードします。

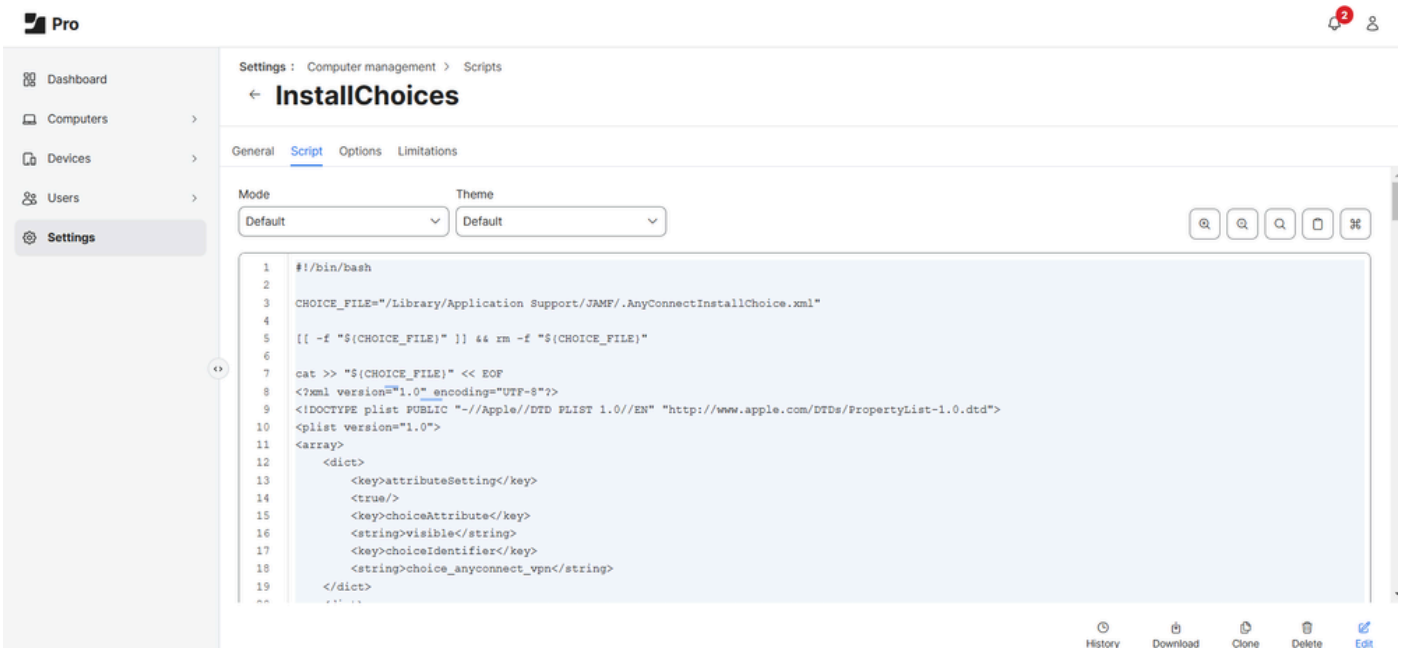


設定およびモジュール選択スクリプトの追加

1. Settings > Computer Management > Scriptsの順に選択し、このスクリプトを追加して、導入時にインストールするモジュールを制御します。

2. デフォルトですべてのモジュールをインストールするようにPKGが設定されているため、モジュールをスキップする場合は0に、インストールする場合は1に設定することで、Secure Clientモジュールのインストールを制御できます。

- サンプルXMLファイルは、Umbrellaのドキュメント「Cisco Secure ClientのmacOSインストールのカスタマイズ」から入手できます。
- Umbrellaはこのgithubリンクに「installchoices」スクリプトも追加しました。この例では、コアVPN、Umbrella、およびDARTモジュールが1に設定されており、セキュアクライアントのインストールに含めることができます。



3. Settings > Computer management > Scriptsの順に移動し、このスクリプトを追加します。これにより、Cisco Secure Clientに必要なコンフィギュレーションファイルOrginfo.jsonが作成されます。

- Umbrellaダッシュボードからモジュールプロファイルを直接ダウンロードし、スクリプトに組織ID、フィンガープリント、およびユーザIDを追加します。

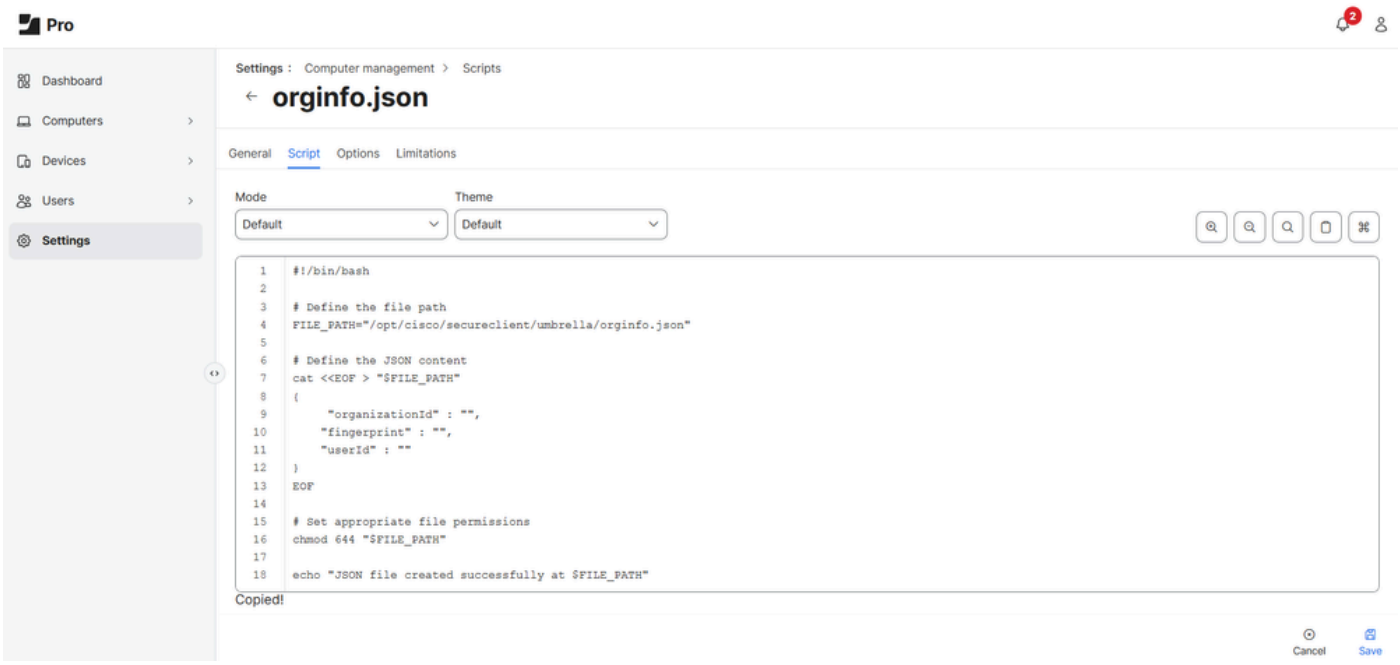
```
#!/bin/bash

# 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

JAMFポリシーの作成

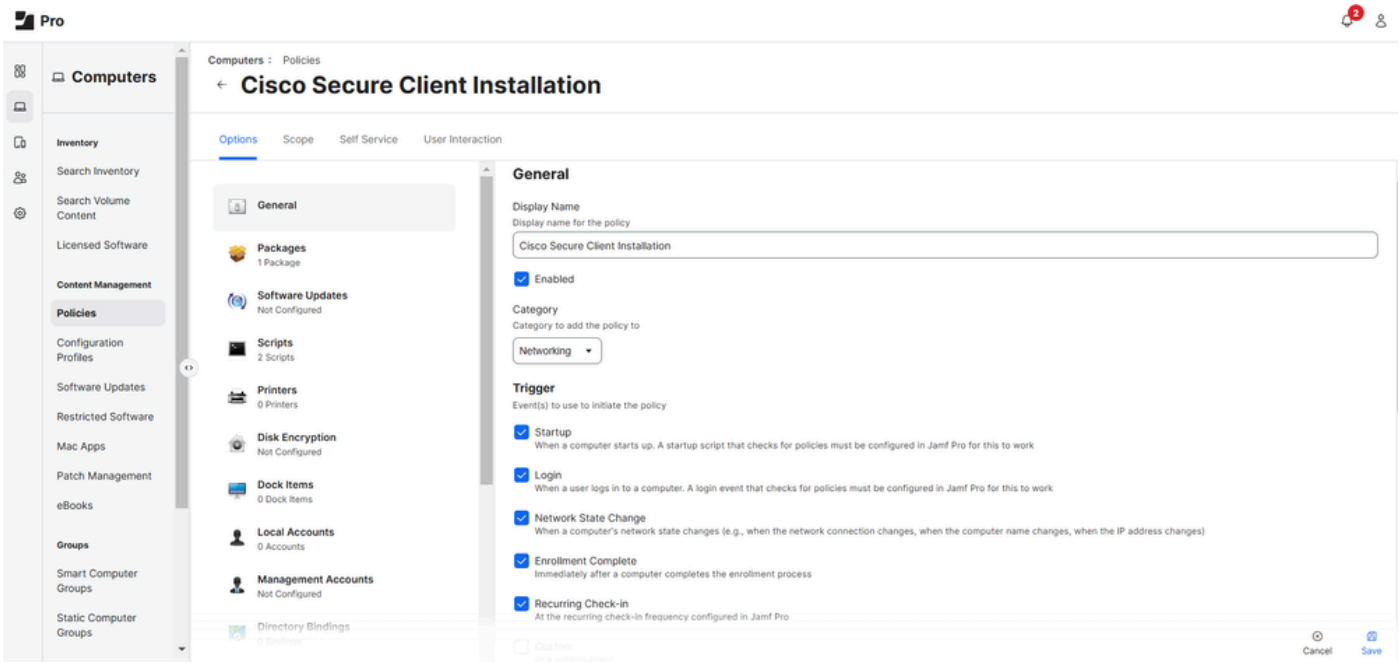
JAMFポリシーは、Umbrellaモジュールを搭載したCisco Secure Clientをプッシュする方法とタイミングを決定するために使用されます。

1. [コンピューター] > [コンテンツ管理] > [ポリシー] > [新規]に移動します。

2. ポリシーに一意の名前を割り当て、目的のカテゴリイベントとトリガーイベント（このポリシーの実行時など）を選択します。

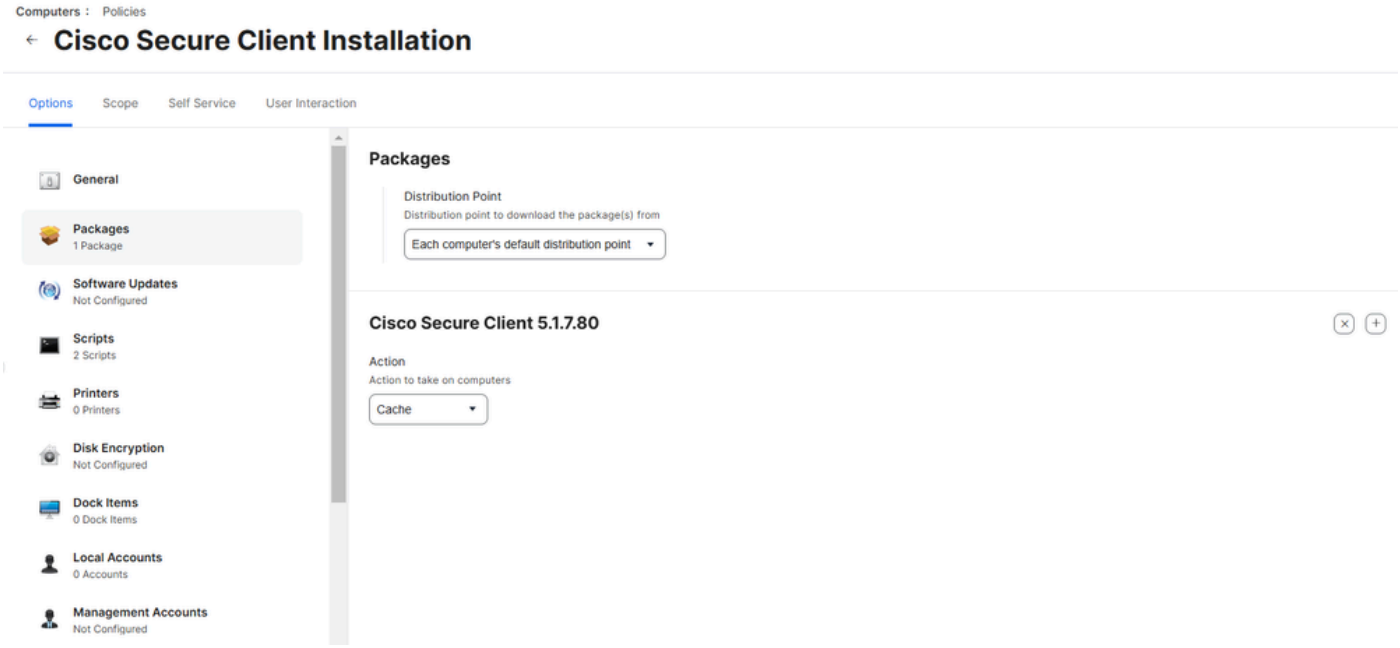
3. オプションで、[カスタム]で実行できるカスタムコマンドを構成することもできます。このポリシーを実行するコマンドは次のようになります。

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

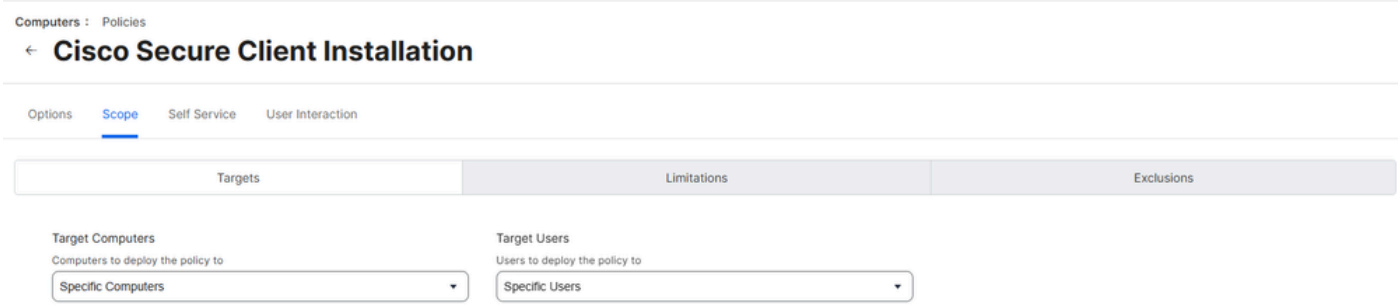


4. Packages > Configureの順に選択し、Cisco Secure Clientパッケージの横にあるAddを選択します。

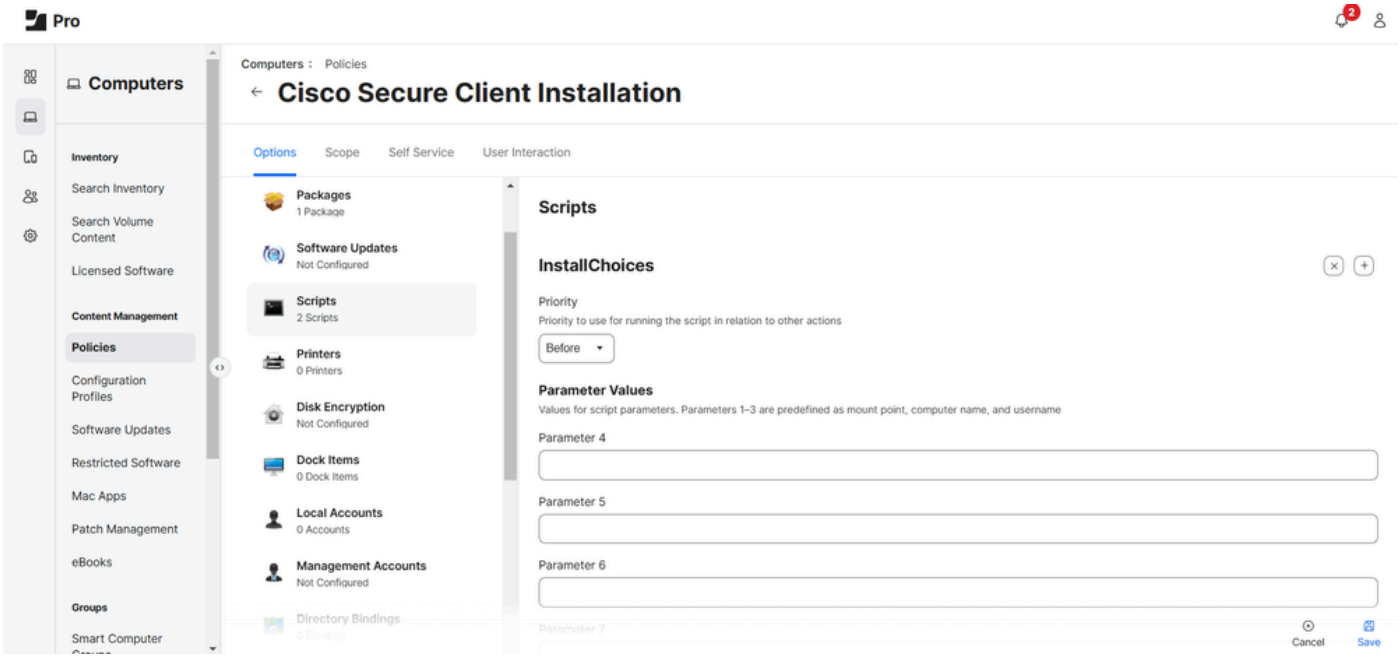
- Distribution Pointの下で、Each computer's default distribution pointを選択します。
- Actionの下で、Cacheを選択します。

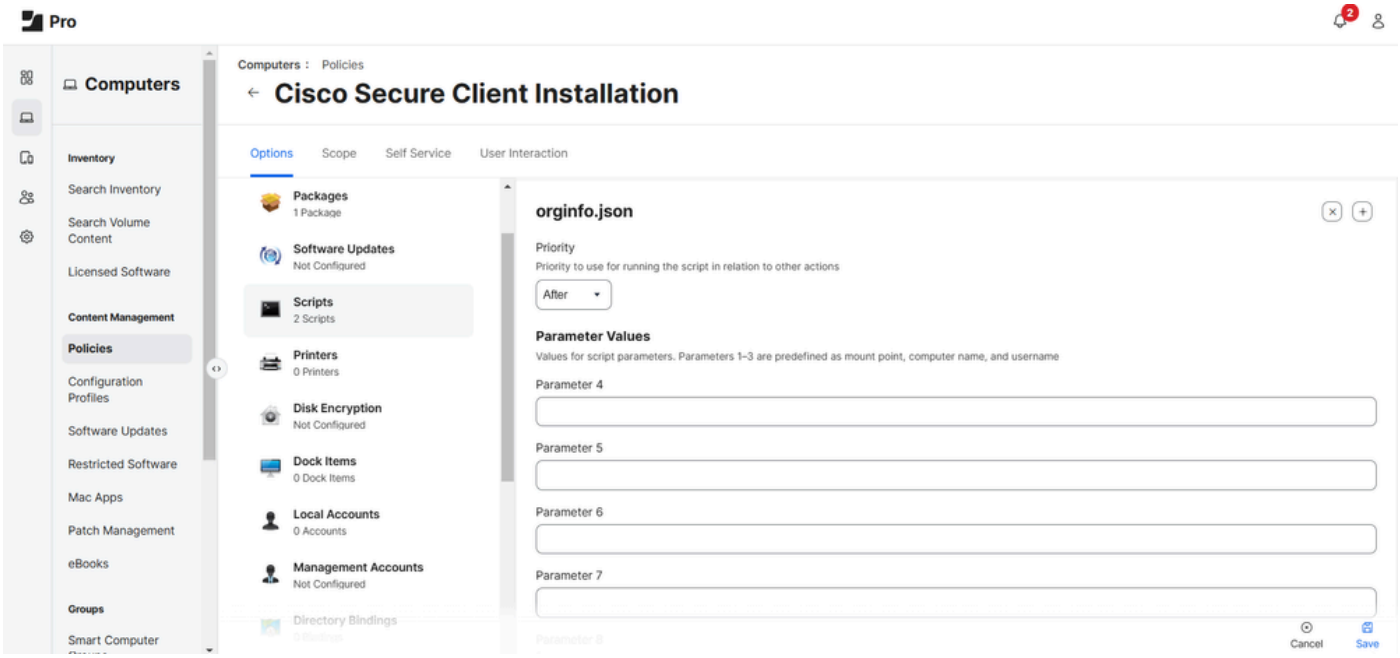


5. 導入するデバイスまたはユーザの範囲を定義し、Saveを選択します。



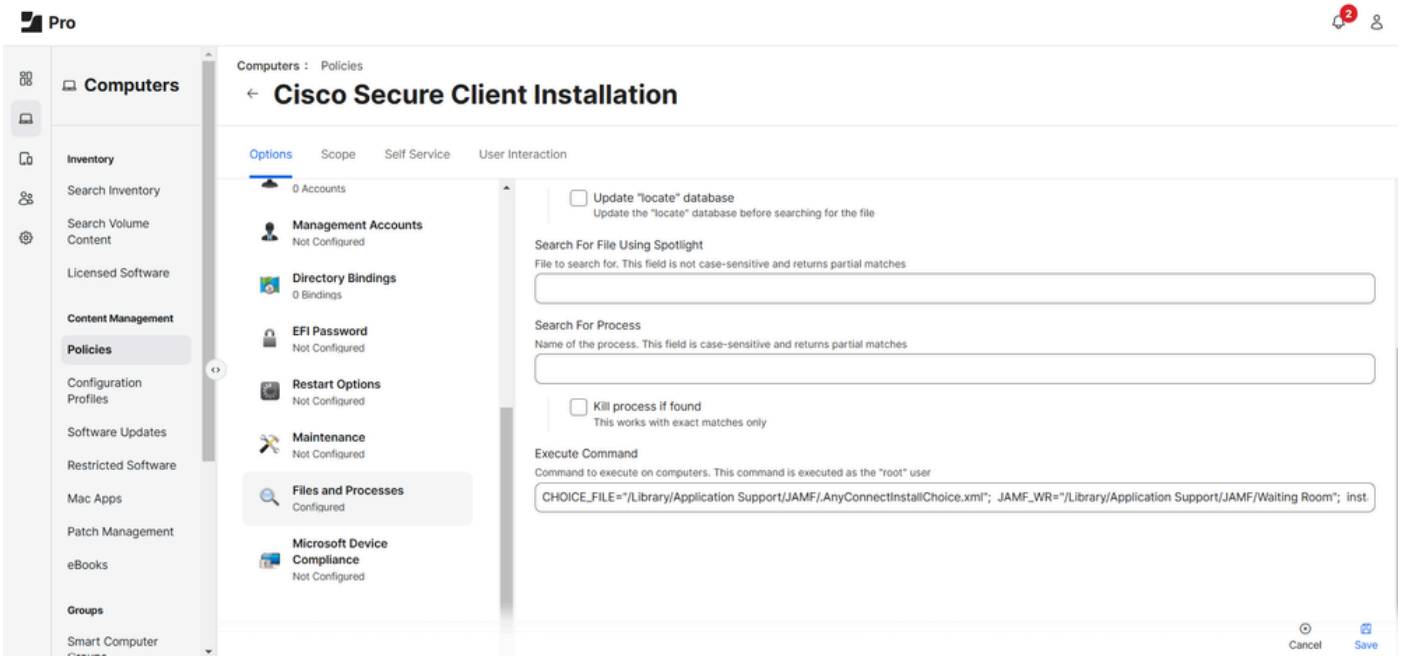
6. InstallChoicesand **orginfo.json** スクリプトの両方を追加し、他のアクションに対するスクリプトの実行に使用する優先度を指定します。





7. 次のコマンドを実行して、選択したモジュールを含むCisco Secure Clientパッケージをデバイスにインストールします。

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



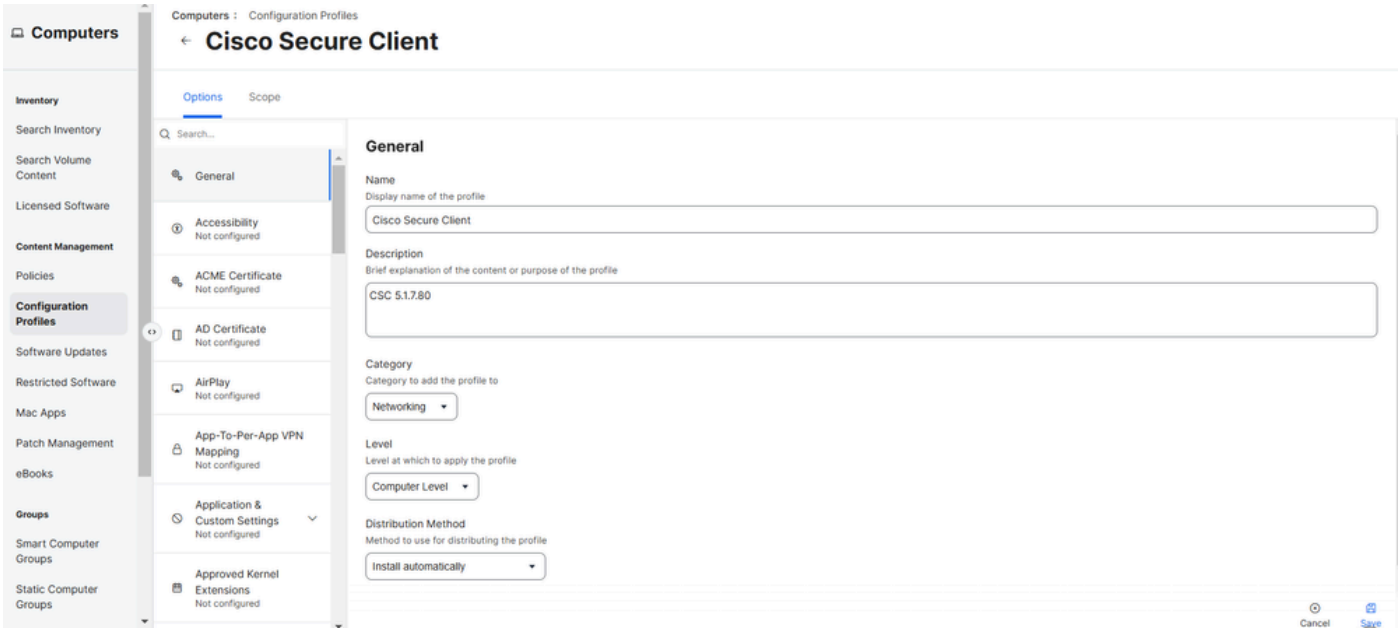
システム拡張のサイレントインストールの設定

次に、JAMFを使用して、Cisco Secure Client with Umbrellaモジュールがユーザの操作なしで正しく動作するために必要なCisco Secure Clientのシステム拡張を設定し、許可します。

1.コンピュータ>コンテンツ管理>構成プロファイル>新規に移動します。

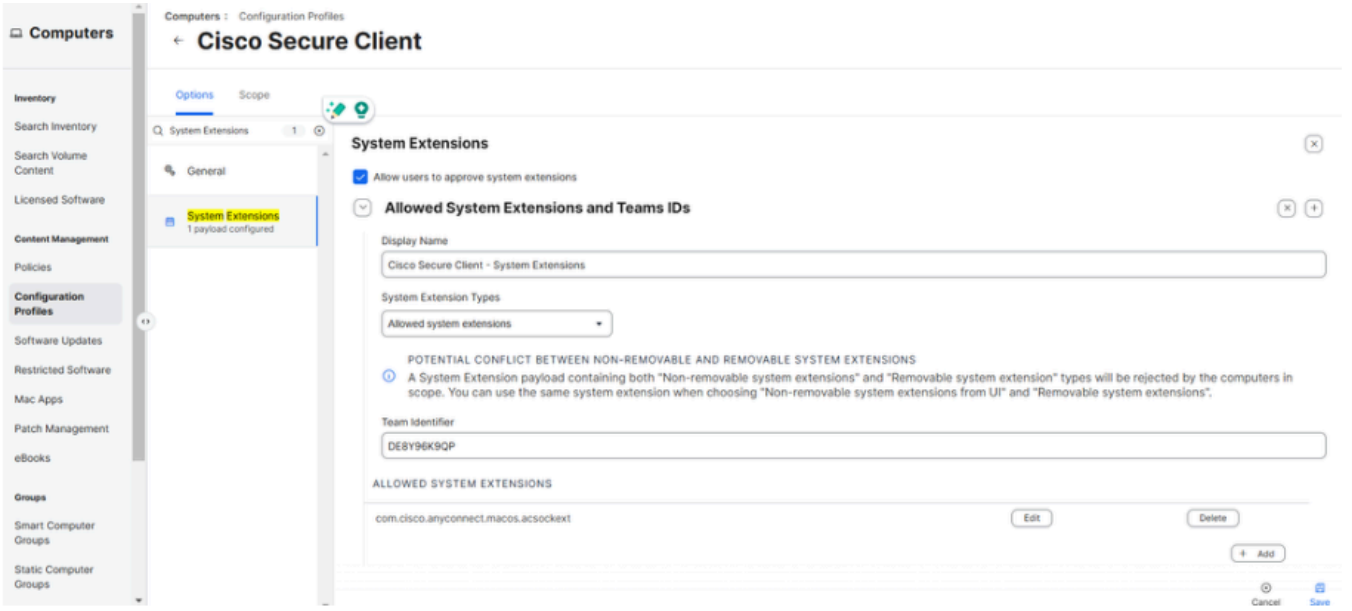
2. プロファイルに一意の名前を付け、カテゴリと分散方式を選択します。

3. EnsureLevelがComputer Levelに設定されていること。



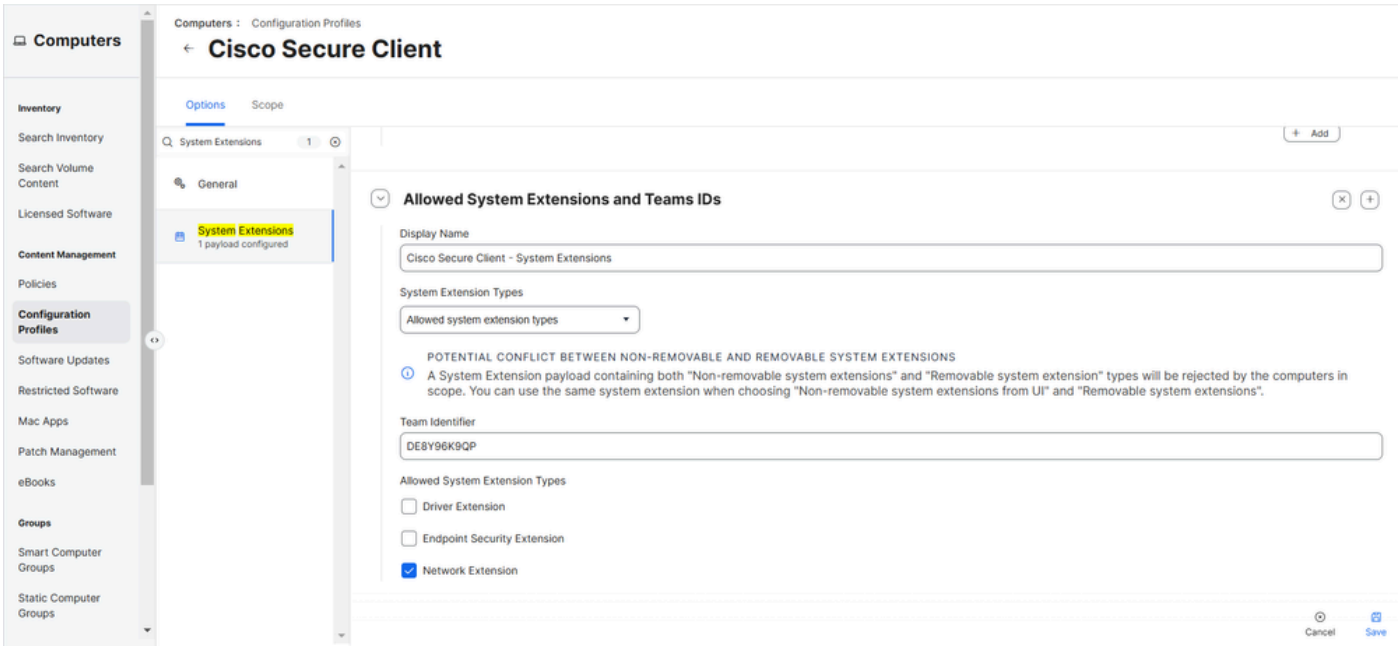
4. System Extensions > Configureを検索します。次の値を入力してください。

- 表示名：Cisco Secure Client - System Extensions
- システム拡張タイプ：許可されたシステム拡張
- チームID: DE8Y96K9QP
- Allowed System Extensions:com.cisco.anyconnect.macos.acsockextを選択してから、Saveを選択する。



5. Allowed Team IDs and System Extensionsの横にある+アイコンを選択して、別のシステム拡張子を追加します。次に、次の値を入力します。

- 表示名：Cisco Secure Client - System Extensions
- システム拡張タイプ：システム拡張タイプの許可
- チームID: DE8Y96K9QP
- システム拡張の種類を許可：ネットワーク拡張



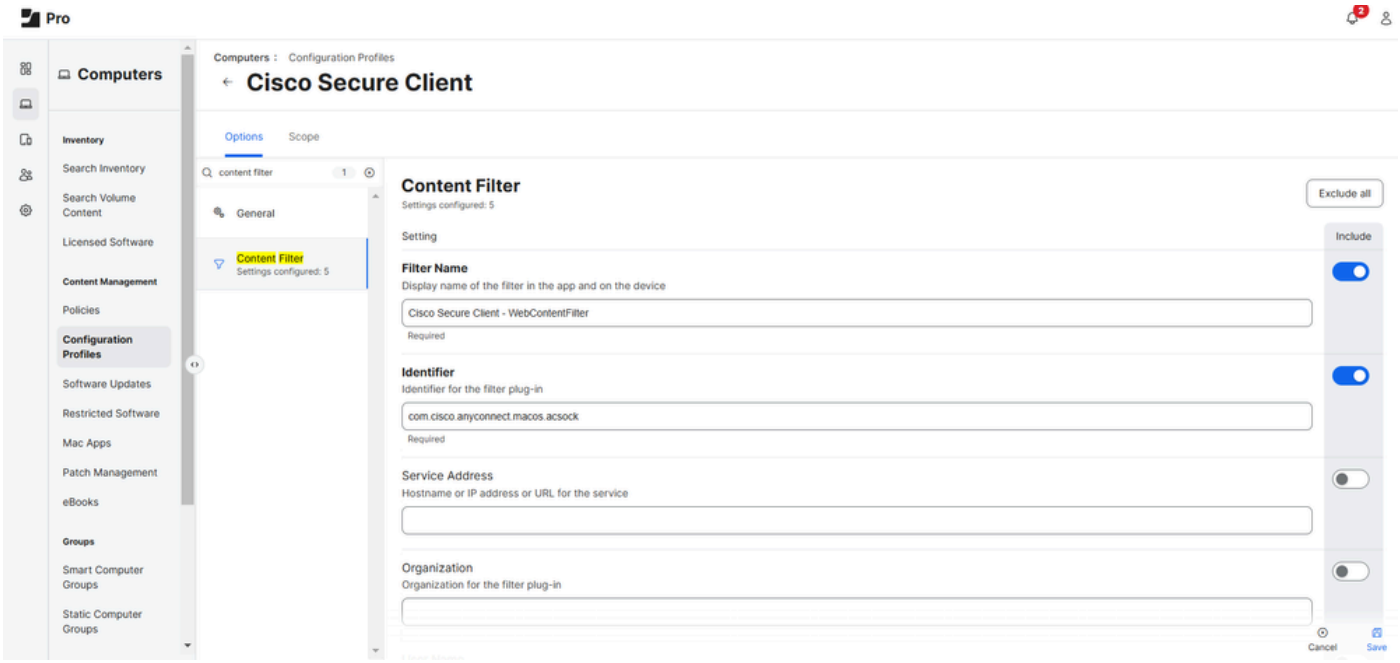
コンテンツフィルタのサイレントインストールの設定

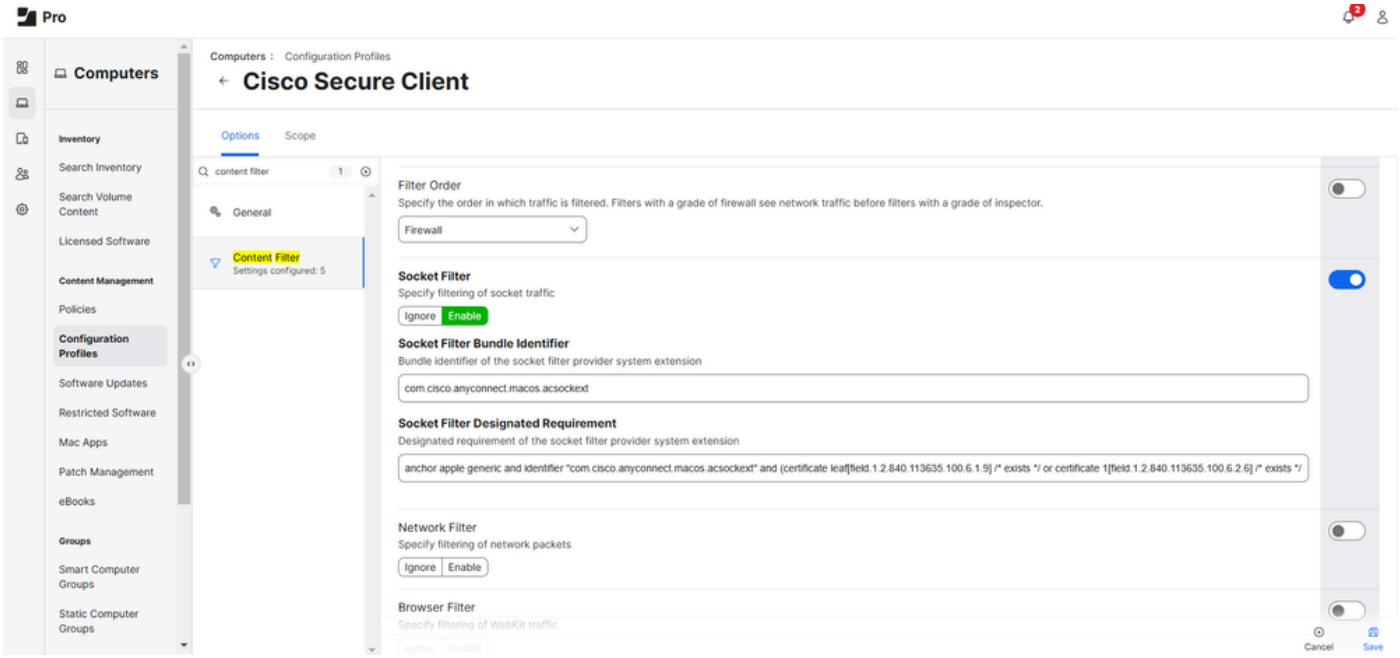
次に、コンテンツフィルタにサイレントインストールを設定します。これは、Cisco Secure ClientとUmbrellaモジュールのソケットフィルタに関連付けられます。

1.コンテンツフィルタを検索します。次のフィールドを有効にし、それぞれの値を入力します。

- フィルタ名：Cisco Secure Client - WebContentFilter
- 識別子：com.cisco.anyconnect.macos.acsock
- ソケットフィルタ：有効
- ソケットフィルタバンドルID:com.cisco.anyconnect.macos.acsockext
- ソケットフィルタ指定要件：

```
anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */またはcertificate 1[field.1.2.840.113635.100 0.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = DE8Y96K9QP)
```





2. 「カスタム・データ」で、「追加」を5回選択して、次の値を入力します：

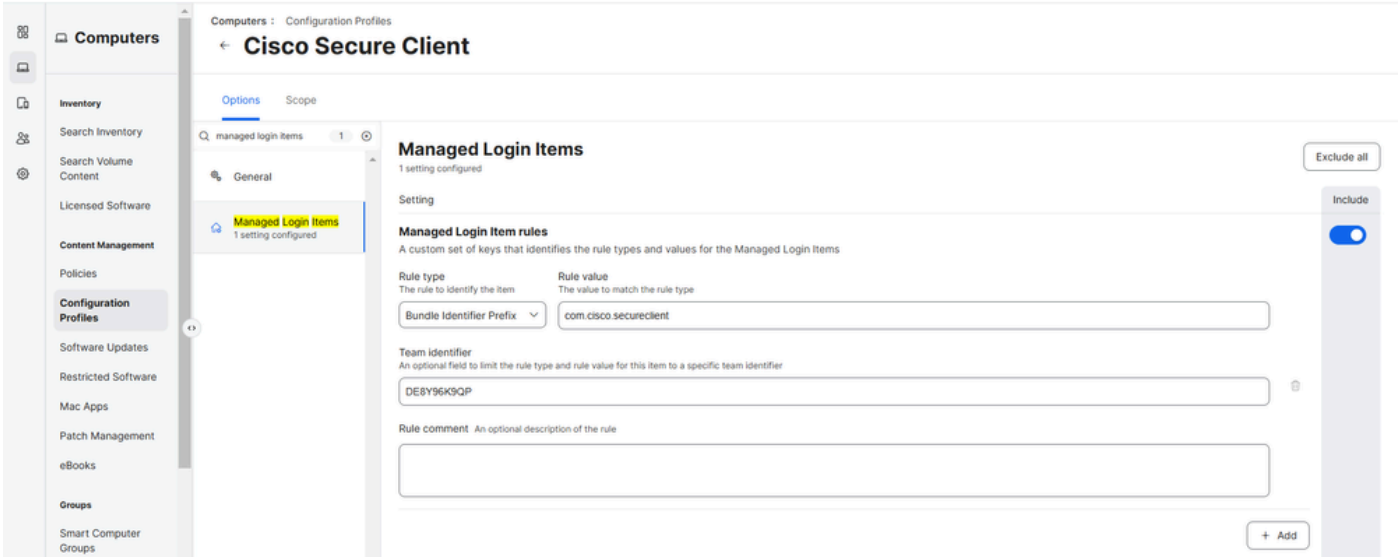
キー	値
オートフィルタ有効	false
FilterBrowser	false
フィルタソケット	true
フィルタパケット	false
フィルタのグレード	ファイアウォール

管理対象ログイン項目の設定

Umbrellaモジュールを使用してCisco Secure Clientの管理対象ログイン項目を設定すると、デバイスの起動時にCisco Secure Clientが起動されるようになります。

設定するには、管理対象ログイン項目を検索し、次の値でフィールドを設定します。

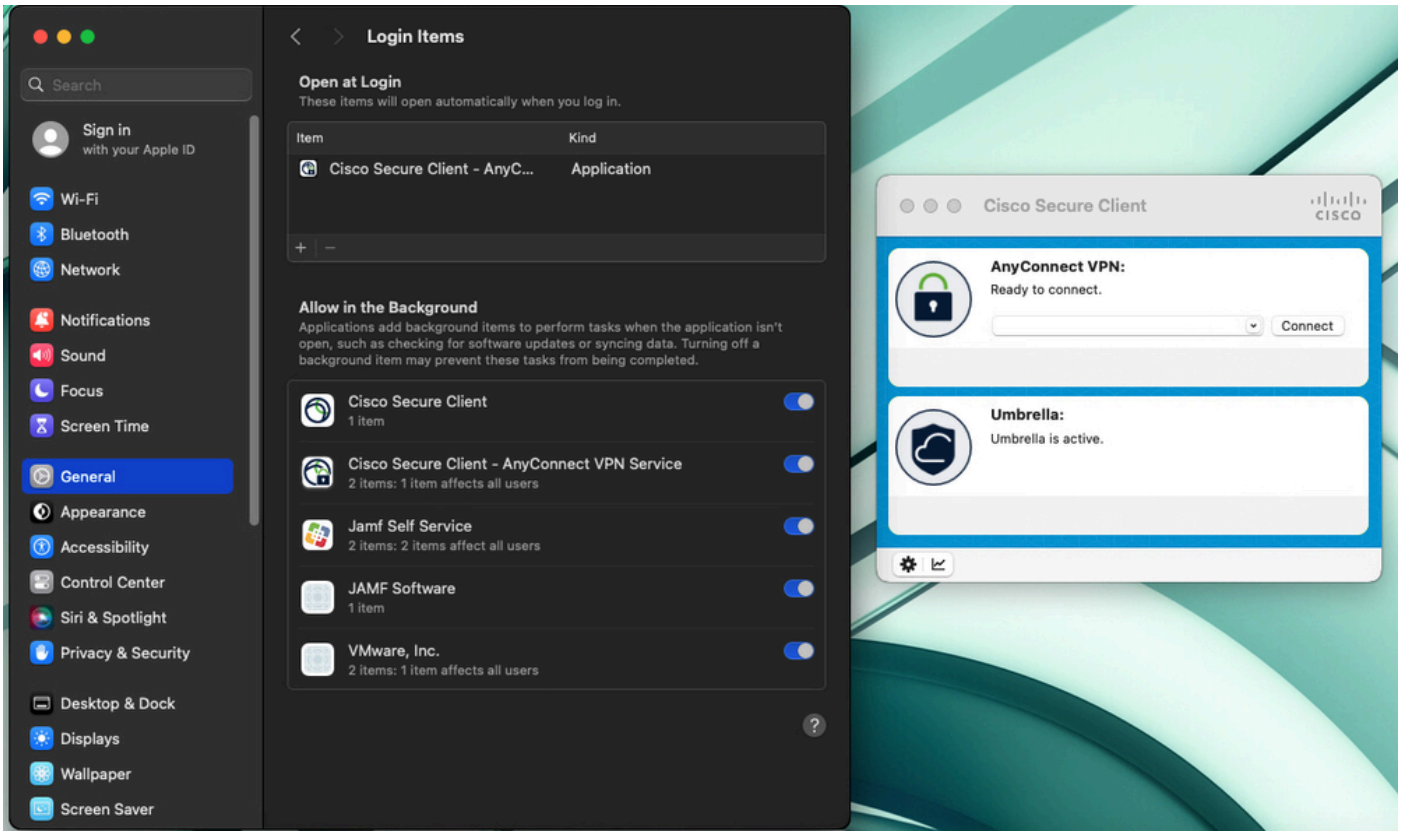
- ルールタイプ：バンドルIDプレフィクス
- ルール値：com.cisco.secureclient
- チームID: DE8Y96K9QP

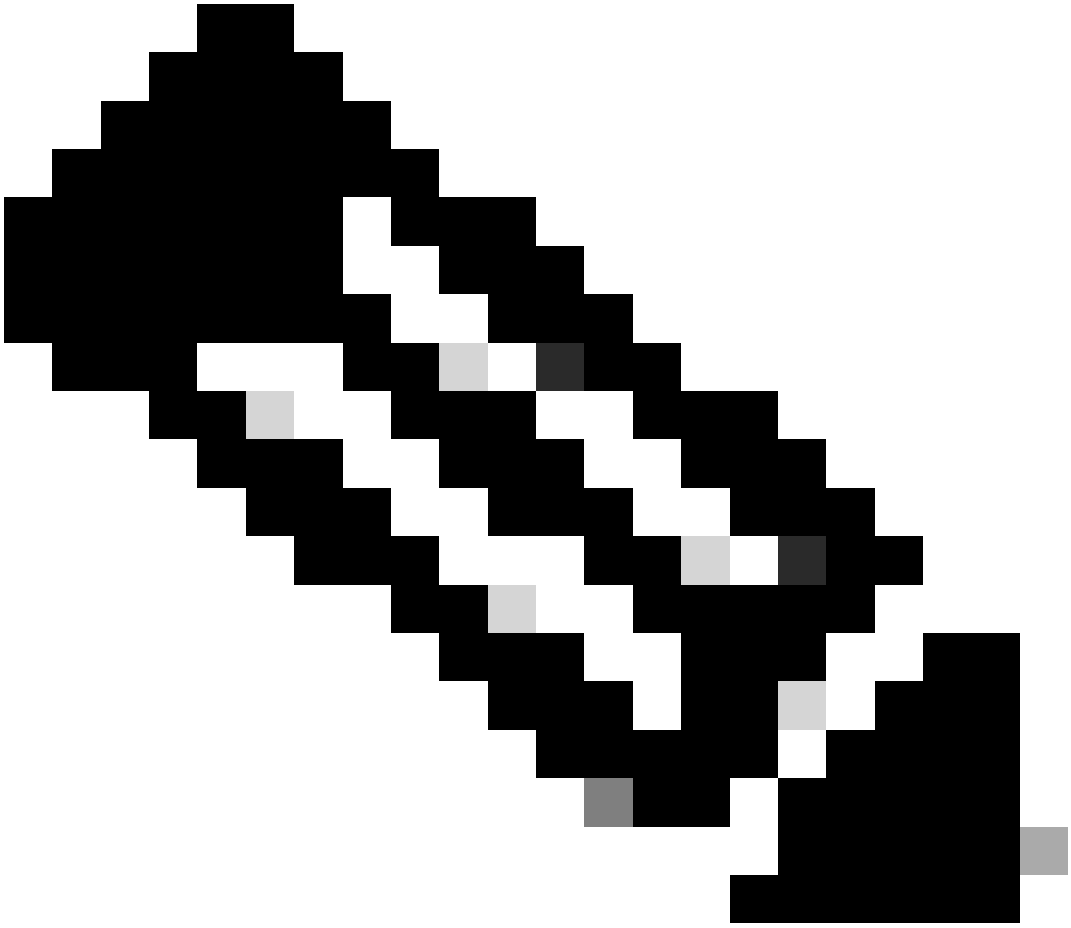


スコープの割り当てとプッシュ展開

1. スコープに移動し、デバイスまたはユーザのスコープを定義します。

2. 「JAMFポリシーの作成」のステップ2で設定したトリガーの1つがアクティブ化されると、Cisco Secure Client with Umbrellaモジュールを目的のmacOSデバイスにプッシュできます。または、JAMFのセルフサービスポータルを通じてプッシュすることもできます。


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：ユーザがシステム設定（ネットワーク>フィルタ）でDNSプロキシまたはトランスペアレントプロキシを無効にしようとしても、この記事で説明されているように、コンテンツフィルタがJAMFを介して有効になっており、無効にすることができないため、デフォルトで自動的に再度有効になります。

macOSファイアウォール例外の設定

macOSファイアウォールがすべての着信接続をブロックするように設定されている場合は、Cisco Secure Clientとそのコンポーネントも例外リストに追加する必要があります。

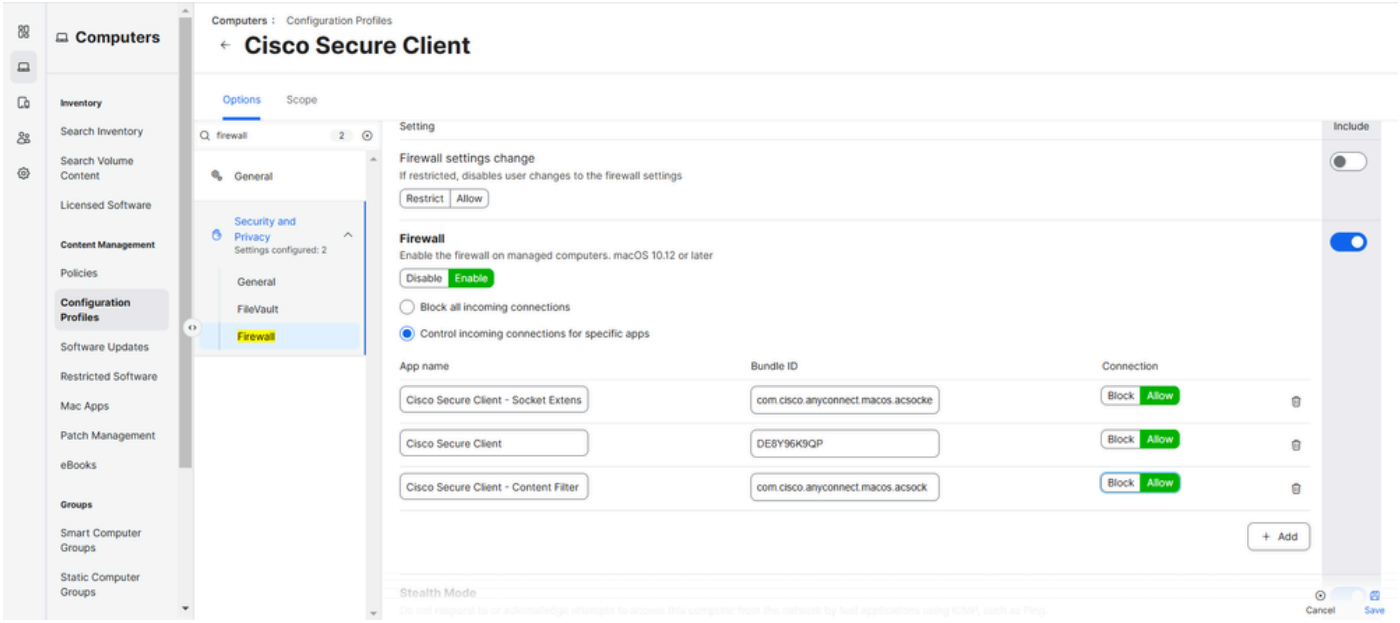
1. [コンピューター] > [コンテンツ管理] > [構成プロファイル]に移動します。

2. Cisco Secure Client設定プロファイルを選択し、Security and Privacyを見つけます。

3. 次の設定で設定します。

- ファイアウォール：有効 – 特定のアプリケーションの受信接続を制御します

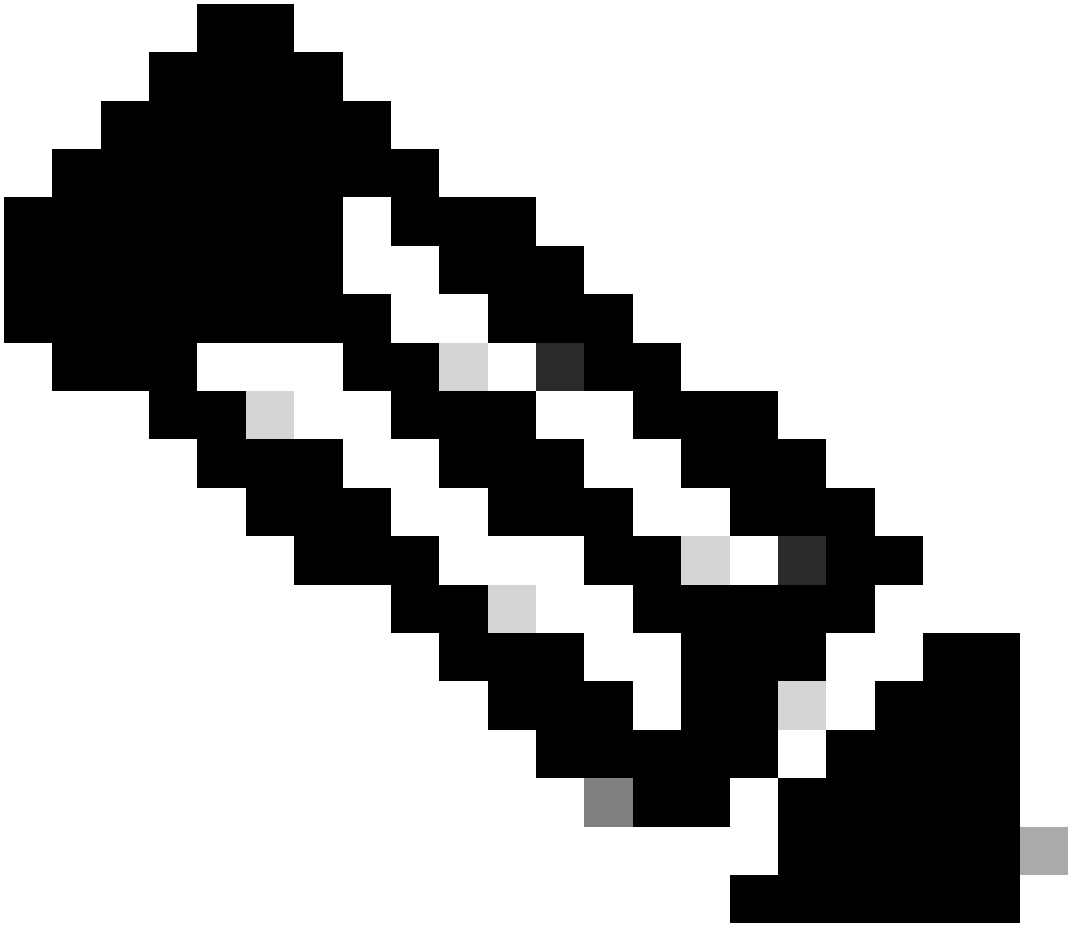
アプリケーション名	バンドルID
Cisco Secure Client – ソケット拡張	com.cisco.anyconnect.macos.acsockext（任意）
Cisco Secure Client	DE8Y96K9QP
Cisco Secure Client – コンテンツフィルタ	com.cisco.anyconnect.macos.acsock（任意のデバイスに接続）



4. Saveを選択します。

5. Redistribution Optionsでプロンプトが表示されたら、Distribute to Allを選択して、変更を目的のmacOSデバイスに即時に適用します。

Cisco Umbrellaルート証明書の展開



注：この手順は、Cisco Secure Clientの新規導入、または以前に導入されたCisco Umbrellaルート証明書がないデバイスにのみ適用されます。 Umbrellaローミングクライアントまたは Cisco AnyConnect 4.10クライアントから移行する場合、または過去にCisco Umbrellaルート証明書を展開した場合は、このセクションを省略できます。

UmbrellaダッシュボードのPolicies > Root CertificateからCisco Umbrellaルート証明書をダウンロードします。

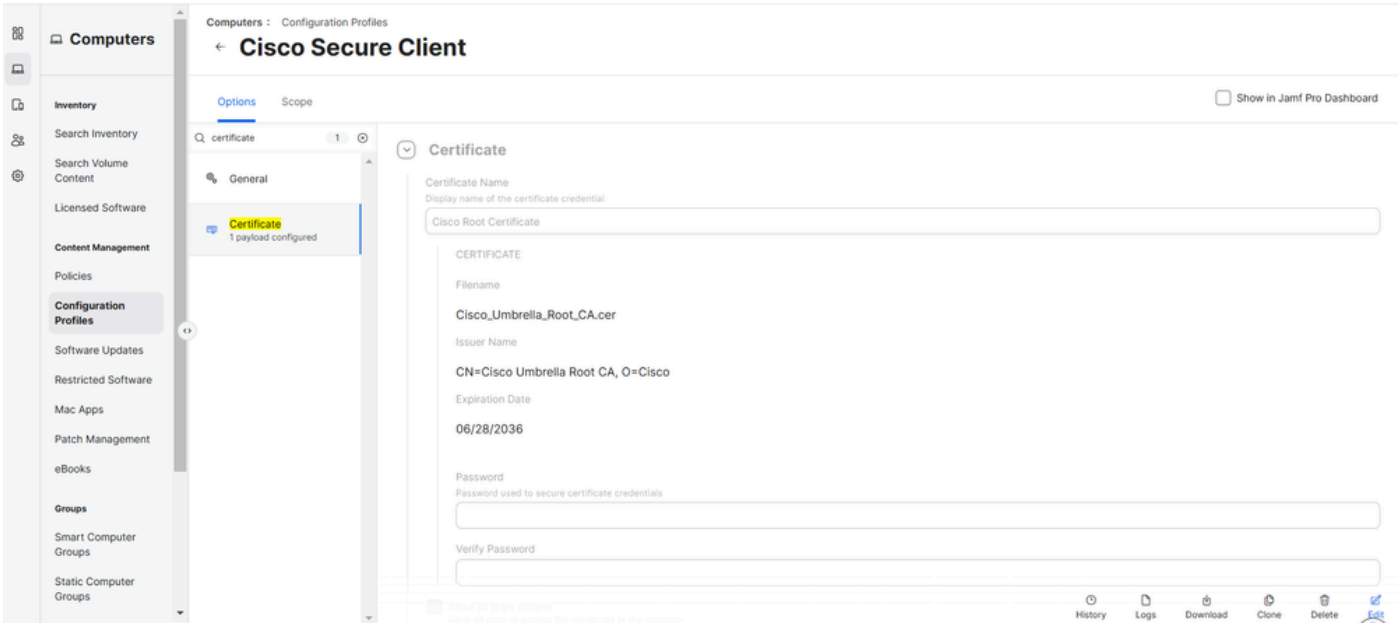
1. UmbrellaダッシュボードのPolicies > Root Certificateで、Cisco Umbrellaルート証明書をダウンロードします。

2. JAMFで、Computers > Configuration Profiles > Cisco Secure Client > Editの順に移動します。

3. Certificate > Configureを検索します。一意の名前を指定します。

4. Select Certificate Optionの下で、Uploadを選択し、ステップ1でダウンロードしたCisco Umbrellaルート証明書をアップロードします。

5. ここでパスワードを設定しないことを確認し、保存を選択します。



6. Redistribution Optionsでプロンプトが表示されたら、Distribute to Allを選択して、変更を目的のmacOSデバイスに即時に適用します。

検証

Cisco Secure Client with Umbrellaモジュールが動作しているかどうかを確認するには、https://policy-debug.checkumbrella.comを参照するか、次のコマンドを実行します。

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

どちらの出力にも、OrgIDなど、Umbrella組織に固有の関連情報が含まれている必要があります。

macOS 14.3の回避策

Cisco Secure Client 5.1.xが稼働するmacOS 14.3（以降）で、「The VPN client agent was unable to create the interprocess communication depot」が表示される場合：

1. JAMFで、「設定」>「コンピュータ管理」>「スクリプト」>「新規」に移動します。

2. 一意の名前を指定し、カテゴリを定義します。

3. 「スクリプト」タブにナビゲートし、次を追加します。

```
#!/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. Optionsで、PriorityがAfterに設定されていることを確認します。このbashスクリプトは、Cisco Secure Client - AnyConnect VPN service.appが実行されているかどうかを、プロセスIDを含む予期される出力を`pgrep -fl`から返すことによって確認します。

- 空の出力が返された場合は、`Cisco Secure Client - AnyConnect VPN service.app`が実行されていないことを確認できます。また、スクリプトを実行して、Umbrellaモジュールが正しく動作するために必要なCisco Secure Clientコアサービスを起動します。

自動更新

シスコは、Umbrellaダッシュボードの自動更新サポートを拡張して、Secure Client 5.1.6.103(MR6)以降のSecure Clientを含めることにしました。 今後、Cisco Secure Client 5.1.6 MR6以降にアップグレードしたお客様は、Umbrellaダッシュボードで自動アップデートが設定されている場合、新しいバージョンに自動アップデートできます。

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。