

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](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[インストールパッケージ\(PKG\)のアップロード](#)

[設定およびモジュール選択スクリプトの追加](#)

[JAMFポリシーの作成](#)

[システム拡張のサイレントインストールの設定](#)

[コンテンツフィルタのサイレントインストールの設定](#)

[管理対象ログイン項目の設定](#)

[スコープの割り当てとプッシュ展開](#)

[macOSファイアウォール例外の設定](#)

[Cisco Umbrellaルート証明書を展開](#)

[検証](#)

[macOS 14.3の回避策](#)

[自動更新](#)

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。

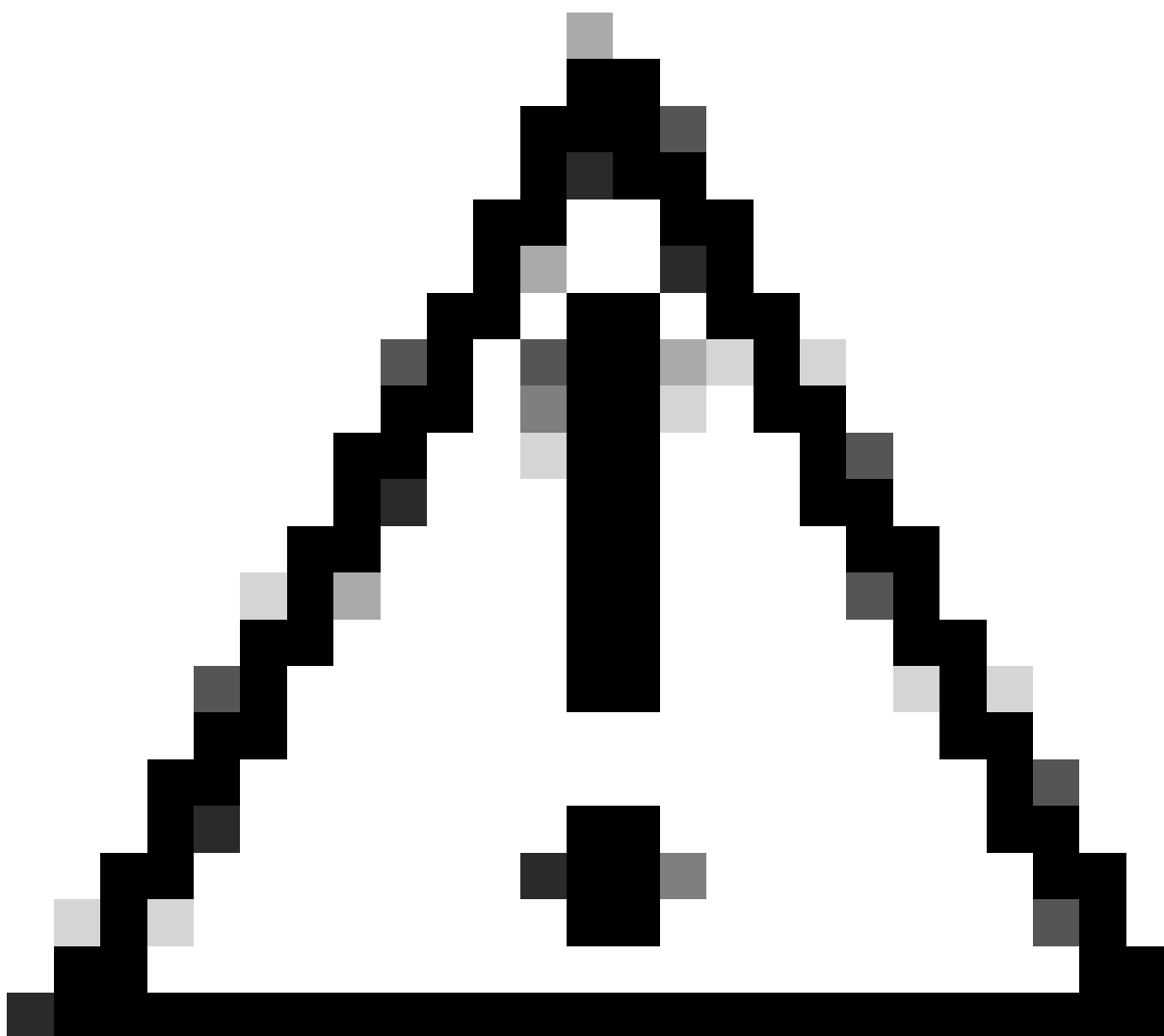
- macOSデバイスはJAMFによって管理される必要があります。
- macOSのMDM登録手順については、[JAMFのドキュメント](#)を参照してください。

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。

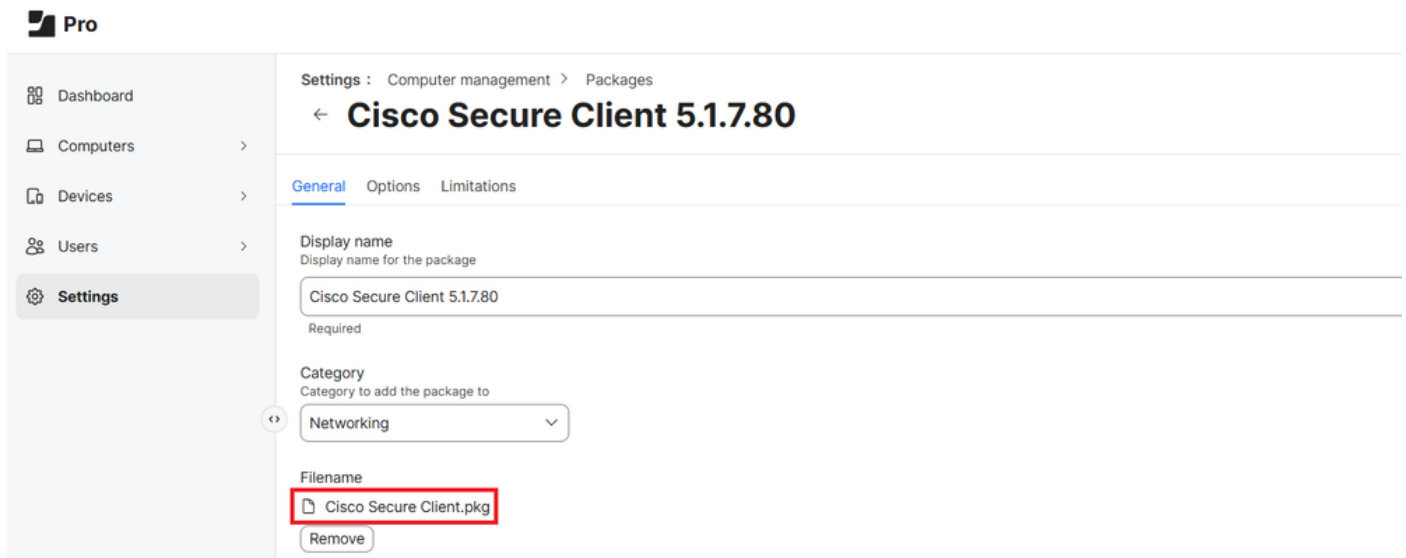


注意：この記事は2025年2月1日の時点でそのまま提供されています。Cisco Umbrellaサポートでは、これらの手順がこの日付以降に有効であることを保証しません。また、JAMFおよびAppleからのアップデートに基づいて手順が変更される場合があります。

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。

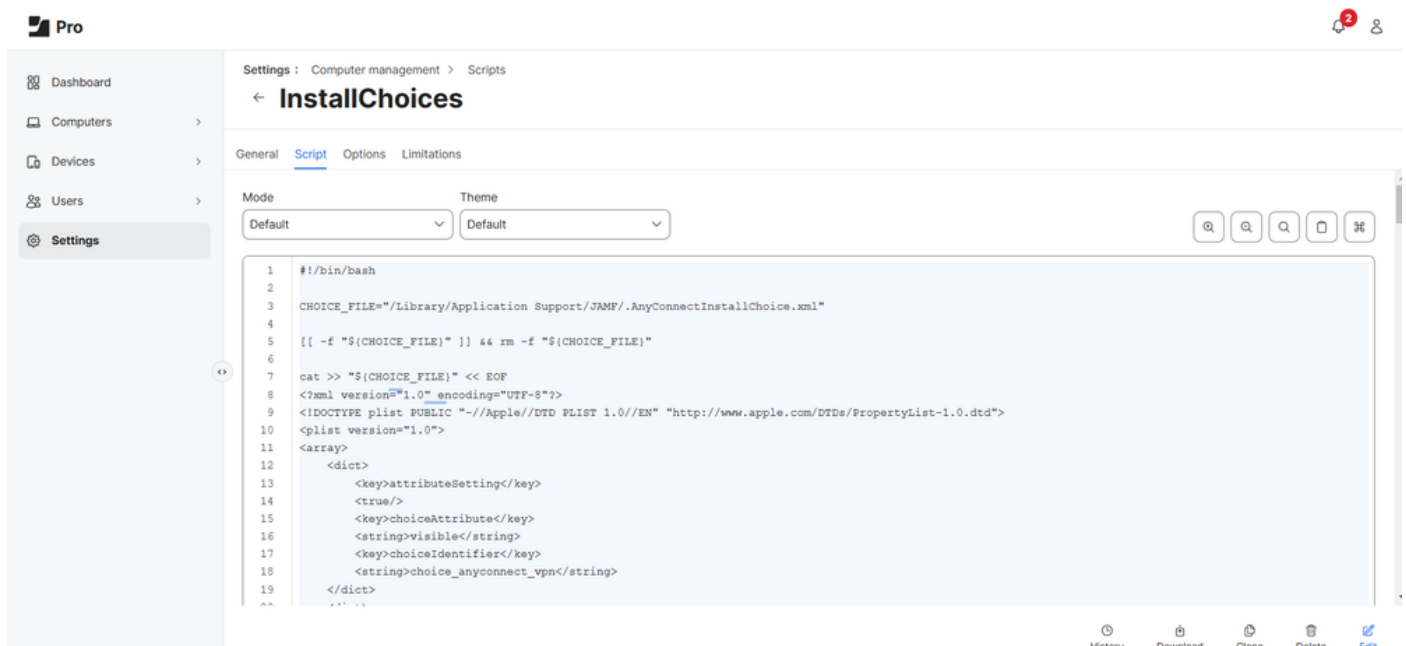


設定およびモジュール選択スクリプトの追加

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。

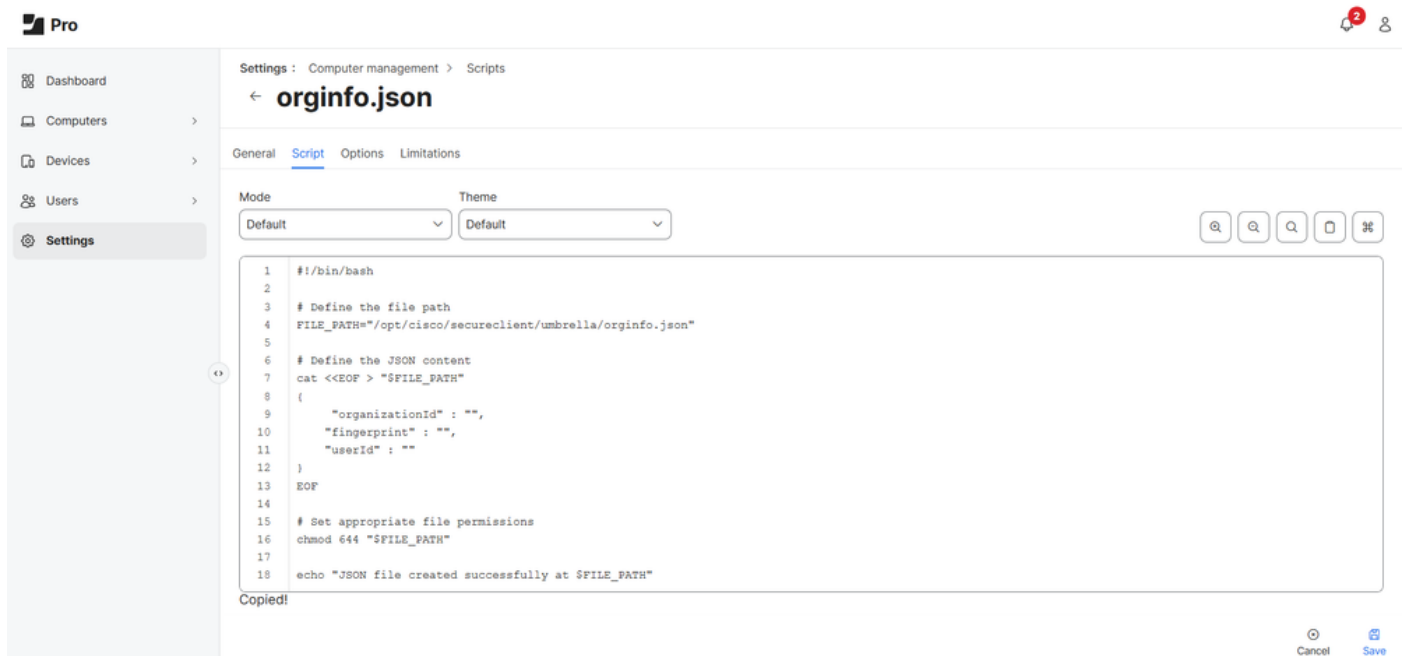
```
#!/bin/bash

# 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"
```



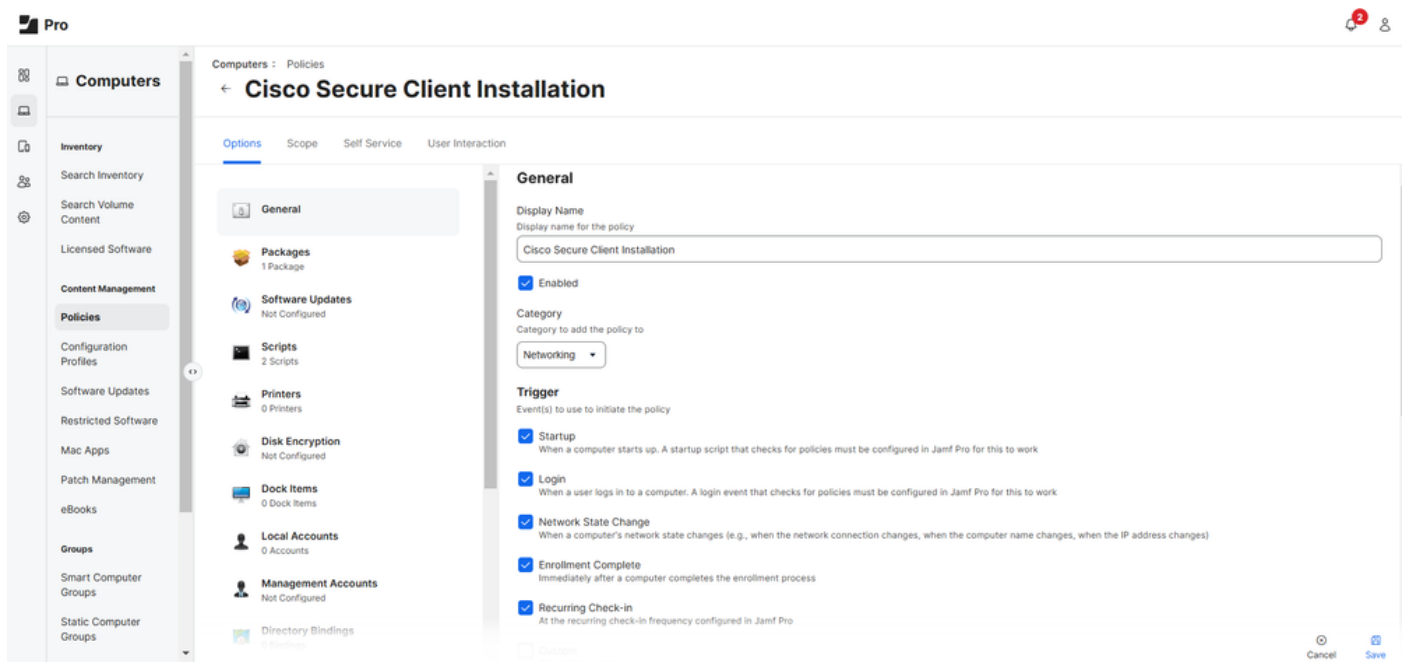
34452906673812

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。

← Cisco Secure Client Installation

Options Scope Self Service User Interaction

General

Packages
1 Package

Software Updates
Not Configured

Scripts
2 Scripts

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Packages

Distribution Point
Distribution point to download the package(s) from
Each computer's default distribution point

Cisco Secure Client 5.1.7.80

Action
Action to take on computers
Cache

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。

← Cisco Secure Client Installation

Options **Scope** Self Service User Interaction

Targets	Limitations	Exclusions
Target Computers Computers to deploy the policy to Specific Computers	Target Users Users to deploy the policy to Specific Users	

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。

Pro

Computers

Inventory

Search Inventory

Search Volume Content

Licensed Software

Content Management

Policies

Configuration Profiles

Software Updates

Restricted Software

Mac Apps

Patch Management

eBooks

Groups

Smart Computer

Computers : Policies

← Cisco Secure Client Installation

Options Scope Self Service User Interaction

Packages
1 Package

Software Updates
Not Configured

Scripts
2 Scripts

Printers
0 Printers

Disk Encryption
Not Configured

Dock Items
0 Dock Items

Local Accounts
0 Accounts

Management Accounts
Not Configured

Directory Bindings
0 Bindings

Scripts

InstallChoices

Priority
Priority to use for running the script in relation to other actions
Before

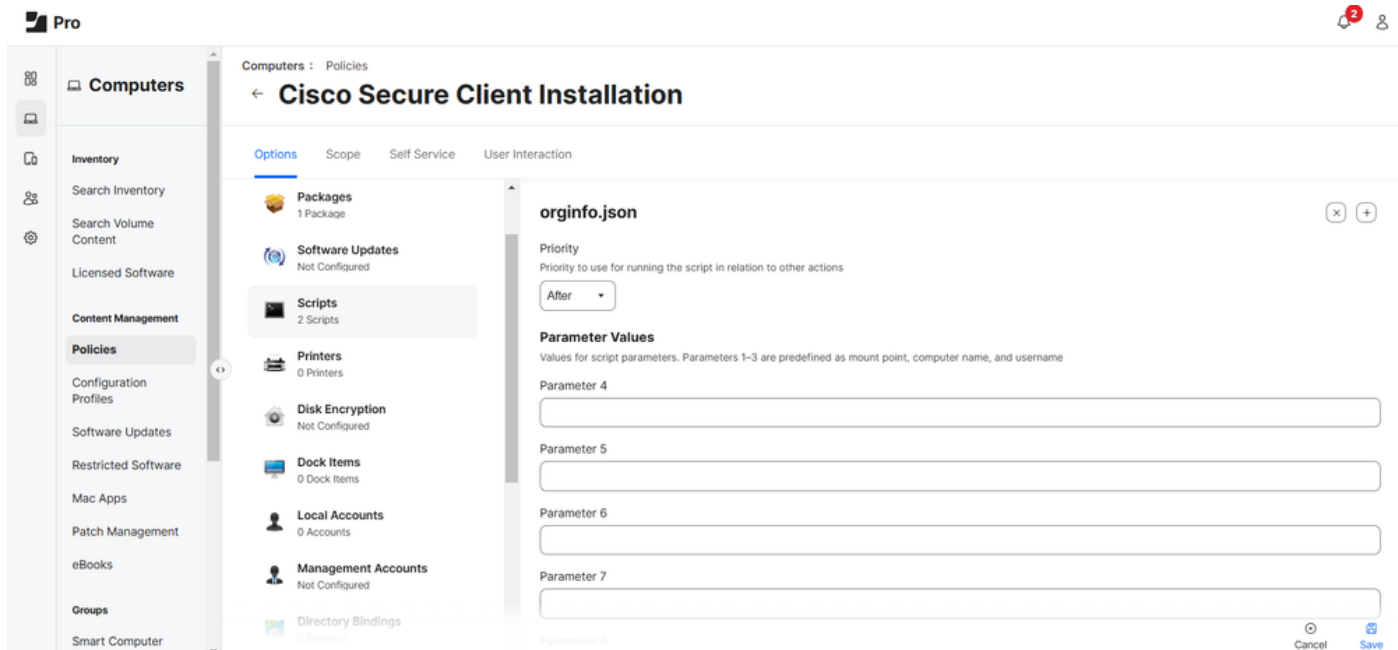
Parameter Values
Values for script parameters. Parameters 1-3 are predefined as mount point, computer name, and username

Parameter 4

Parameter 5

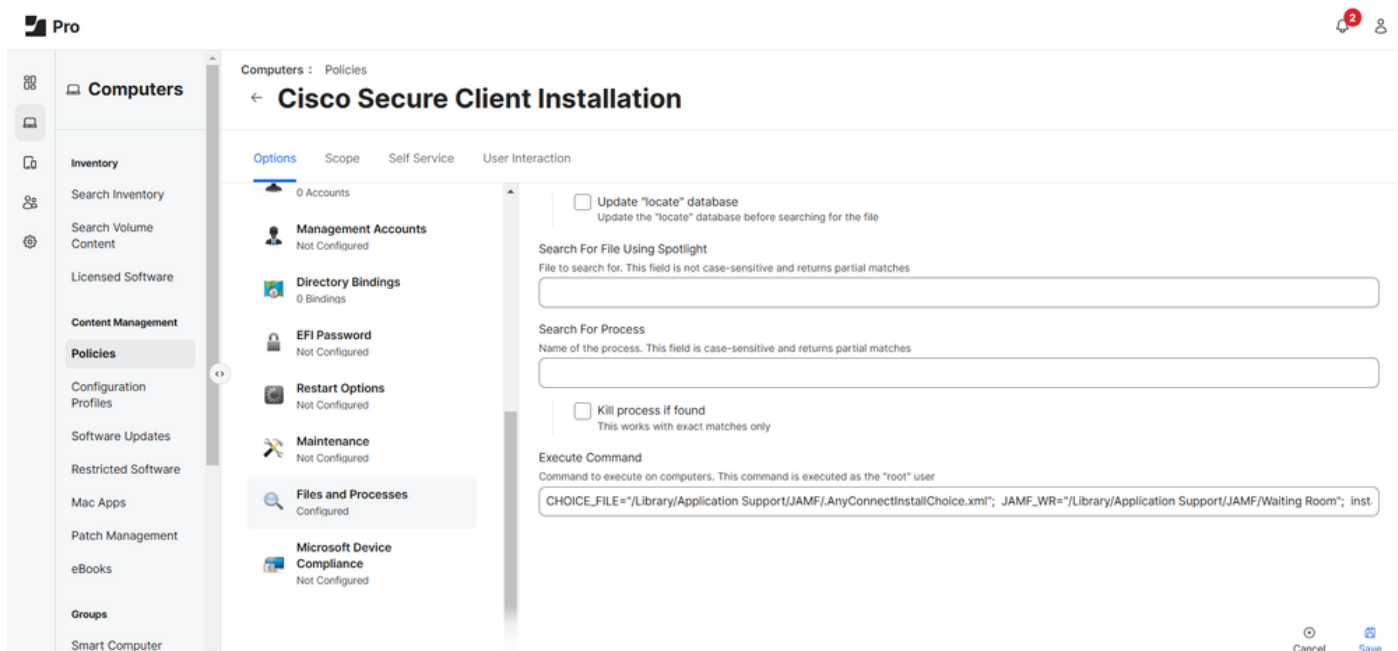
Parameter 6

Parameter 7



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。

The screenshot shows the 'Cisco Secure Client' configuration page under 'Configuration Profiles'. The left sidebar lists various management categories, with 'Configuration Profiles' selected. The main area has two tabs: 'Options' (active) and 'Scope'. Under 'Options', there's a list of settings like General, Accessibility, ACME Certificate, AD Certificate, AirPlay, App-To-Per-App VPN Mapping, Application & Custom Settings, and Approved Kernel Extensions. The 'General' tab is active, showing fields for Name (Cisco Secure Client), Description (CSC 5.17.80), Category (Networking), Level (Computer Level), and Distribution Method (Install automatically). Buttons for 'Cancel' and 'Save' are at the bottom right.

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。

The screenshot shows the 'Cisco Secure Client' configuration page with the 'System Extensions' tab selected. The left sidebar shows 'System Extensions' under 'Configuration Profiles' with a note '1 payload configured'. The main area shows the 'System Extensions' configuration. It includes a checkbox for 'Allow users to approve system extensions' (checked), a section for 'Allowed System Extensions and Teams IDs' with a 'Display Name' field (Cisco Secure Client - System Extensions), a 'System Extension Types' dropdown (Allowed system extensions), and a 'Team Identifier' field (DE8Y96K9QP). A warning message states: 'POTENTIAL CONFLICT BETWEEN NON-REMOVABLE AND REMOVABLE SYSTEM EXTENSIONS. A System Extension payload containing both "Non-removable system extensions" and "Removable system extension" types will be rejected by the computers in scope. You can use the same system extension when choosing "Non-removable system extensions from UI" and "Removable system extensions".' Below this, there's a table for 'ALLOWED SYSTEM EXTENSIONS' with one entry: 'com.cisco.anyconnect.macos.acsockext'. Buttons for 'Edit', 'Delete', and '+ Add' are present. 'Cancel' and 'Save' buttons are at the bottom right.

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

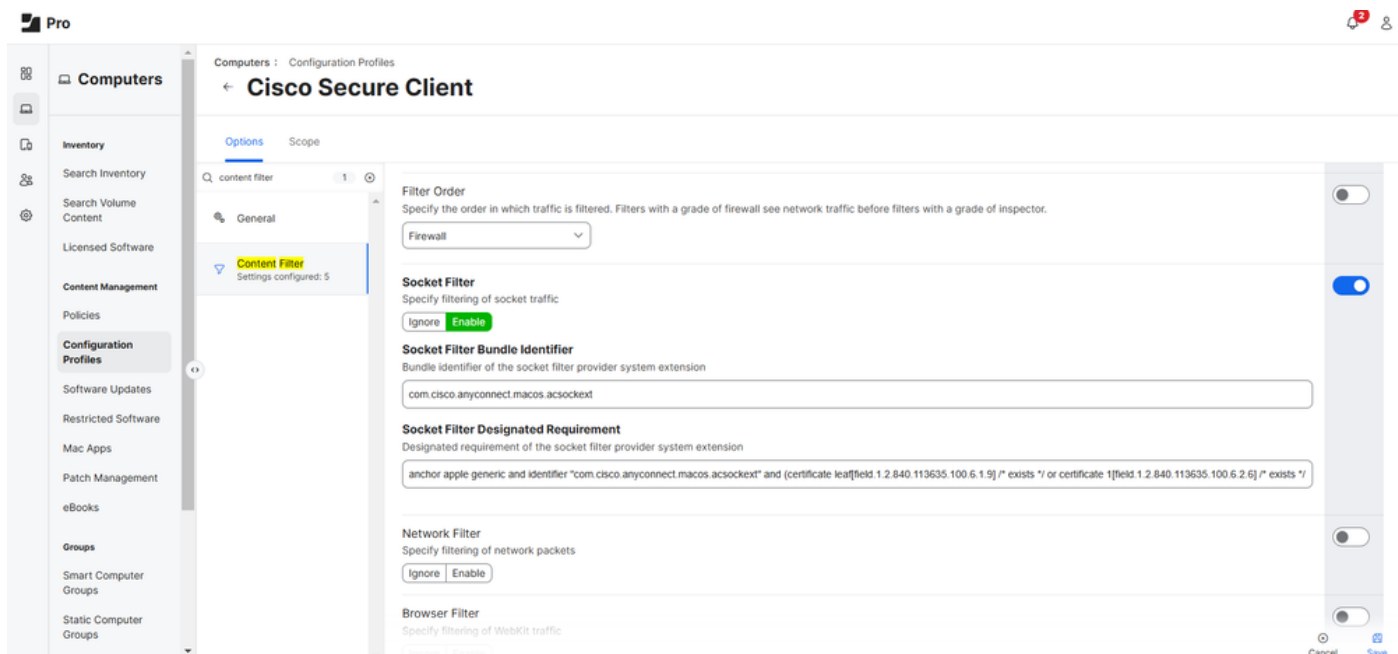
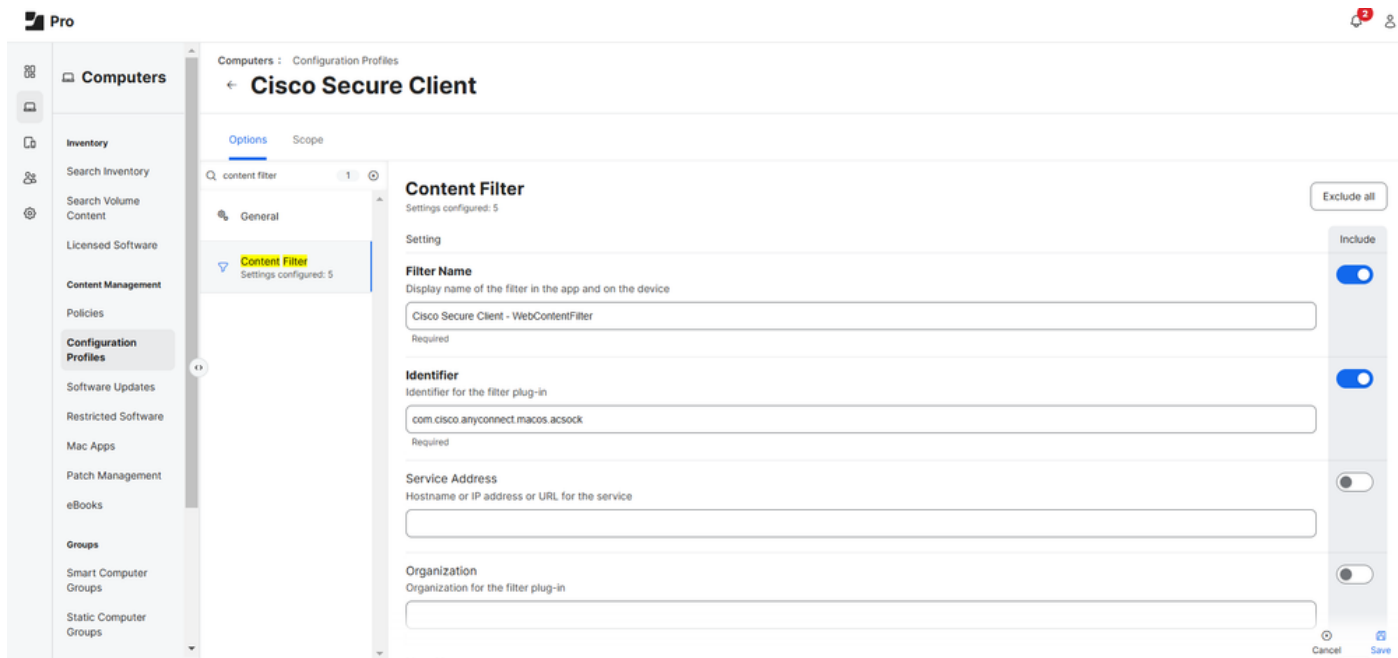
コンテンツフィルタのサイレントインストールの設定

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。

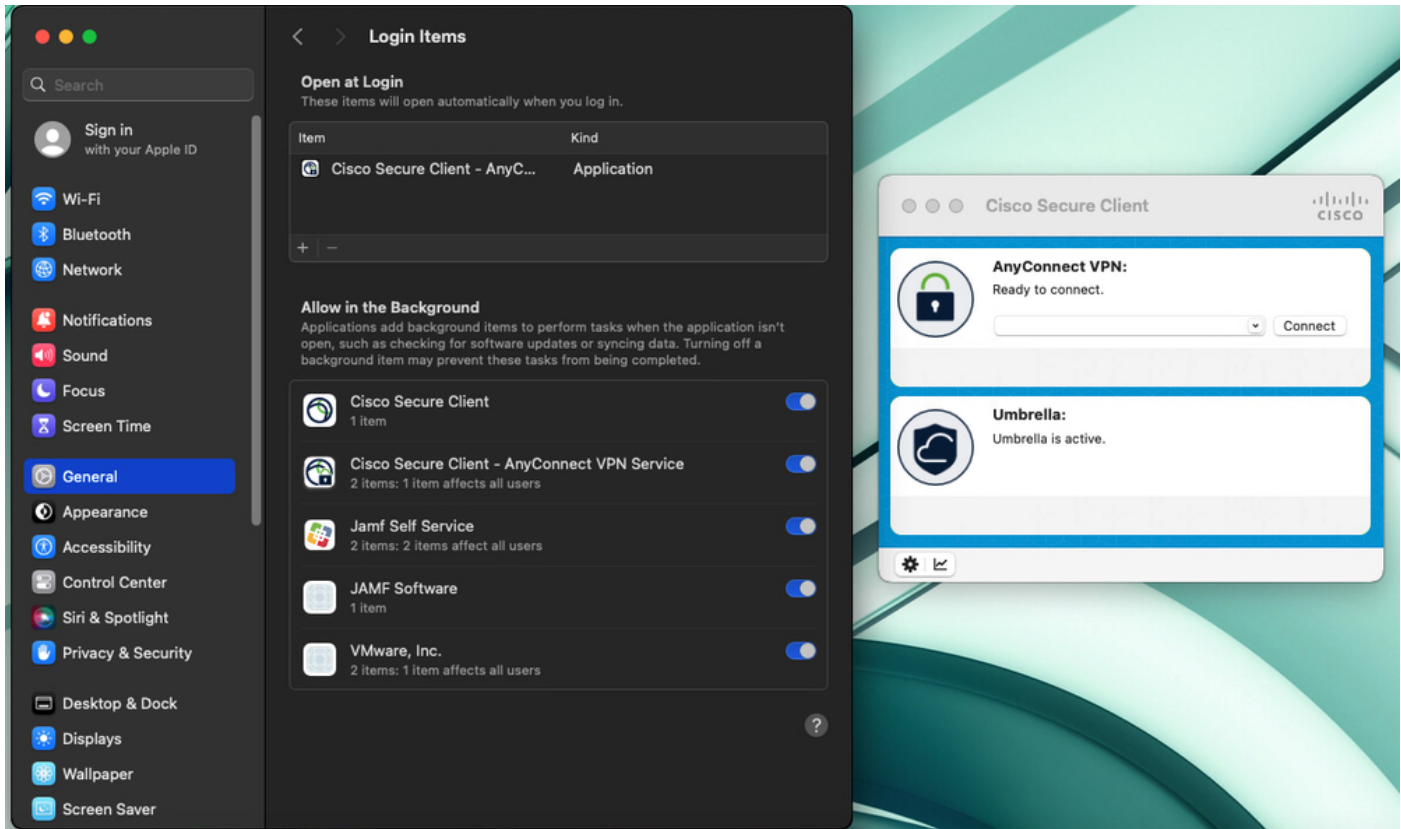
設定するには、管理対象ログイン項目を検索し、次の値でフィールドを設定します。

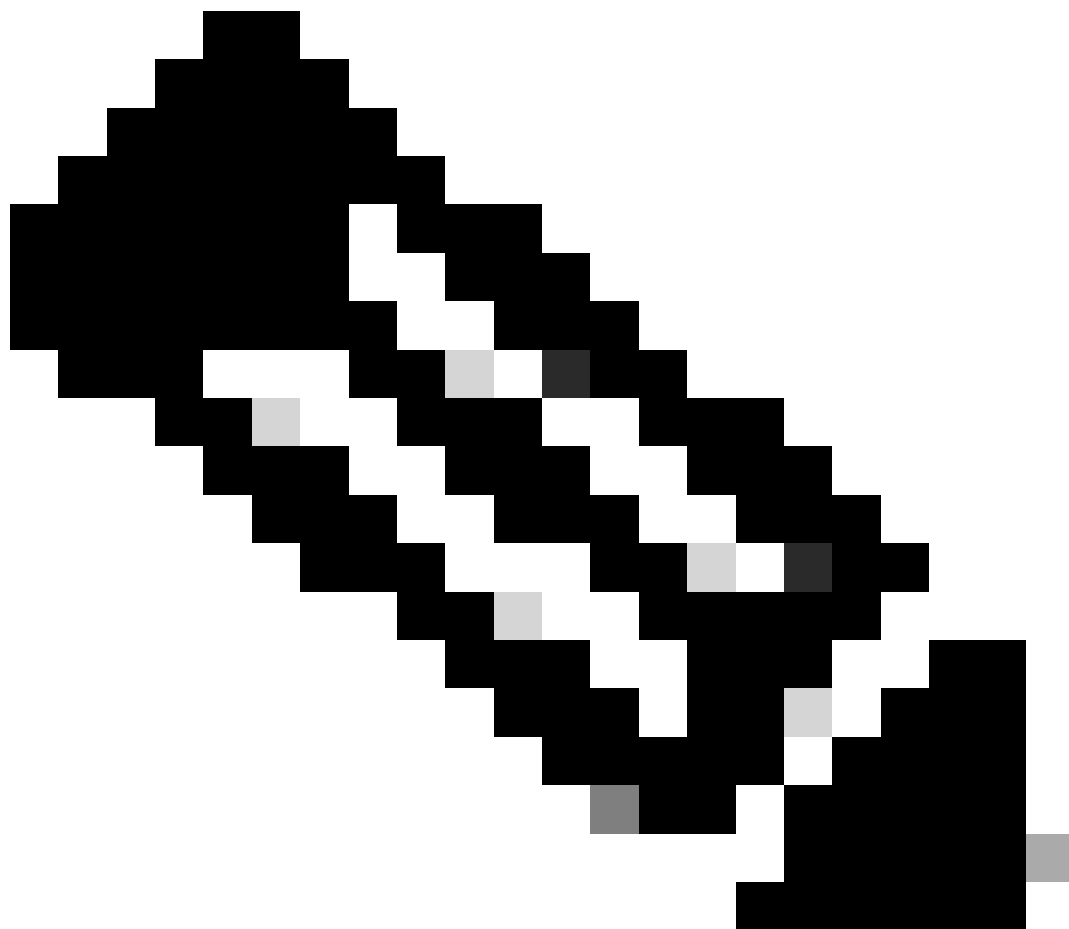
- ルールタイプ：バンドルIDプレフィクス
- ルール値：com.cisco.secureclient
- チームID: DE8Y96K9QP

The screenshot shows the 'Cisco Secure Client' configuration page. On the left is a sidebar with navigation options: Computers, Inventory, Search Inventory, Search Volume Content, Licensed Software, Content Management, Policies, Configuration Profiles (selected), Software Updates, Restricted Software, Mac Apps, Patch Management, eBooks, Groups, Smart Computer Groups. The main area is titled 'Configuration Profiles' and 'Cisco Secure Client'. It has tabs for 'Options' and 'Scope'. Under 'Options', there's a search bar with 'managed login items' and a result count of '1'. Below this is a 'General' tab and a 'Managed Login Items' section with '1 setting configured'. The 'Managed Login Item rules' section describes it as 'A custom set of keys that identifies the rule types and values for the Managed Login Items'. It contains three fields: 'Rule type' (set to 'Bundle Identifier Prefix'), 'Rule value' (set to 'com.cisco.secureclient'), and 'Team identifier' (set to 'DE8Y96K9QP'). There is also a 'Rule comment' field. On the right side of the configuration area, there are buttons for 'Exclude all', 'Include' (with a toggle switch), and '+ Add'.

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。





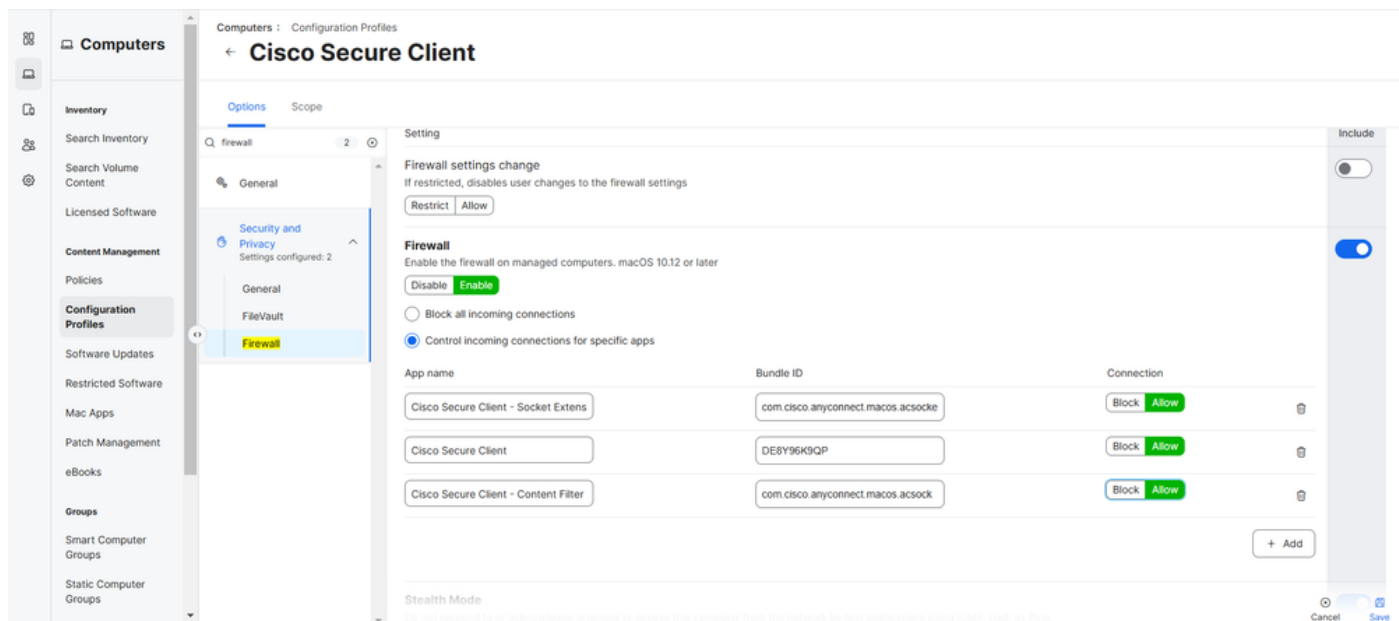
注：ユーザがシステム設定（ネットワーク>フィルタ）でDNSプロキシまたはトランスペアレントプロキシを無効にしようとしても、この記事で説明されているように、コンテンツフィルタがJAMFを介して有効になっており、無効にすることができないため、デフォルトで自動的に再度有効になります。

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

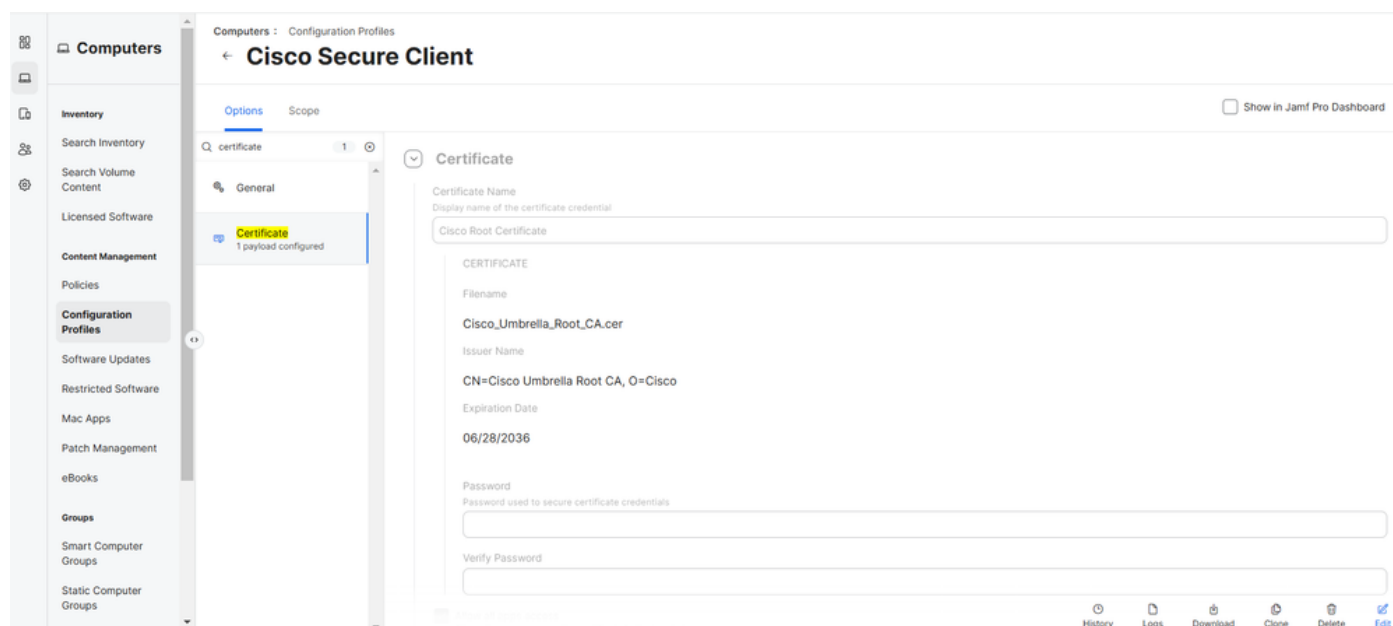


注：この手順は、Cisco Secure Clientの新規導入、または以前に導入されたCisco Umbrellaルート証明書がないデバイスにのみ適用されます。UmbrellaローミングクライアントまたはCisco AnyConnect 4.10クライアントから移行する場合、または過去にCisco Umbrellaルート証明書を展開した場合は、このセクションを省略できます。

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。