

Deploy CSC to macOS Using JAMF with Umbrella Module

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Upload the Installation Package \(PKG\)](#)

[Add Configuration and Module Selection Scripts](#)

[Create the JAMF Policy](#)

[Configure a Silent Install of System Extension](#)

[Configure Silent Install for Content Filter](#)

[Configure Managed Login Items](#)

[Assign Scope and Push Deployment](#)

[Configure macOS Firewall Exception](#)

[Deploy the Cisco Umbrella Root Certificate](#)

[Verification](#)

[Workaround for macOS 14.3](#)

[Automatic Updates](#)

Introduction

This document describes how to deploy Cisco Secure Client with the Umbrella module to managed macOS devices using JAMF.

Prerequisites

Requirements

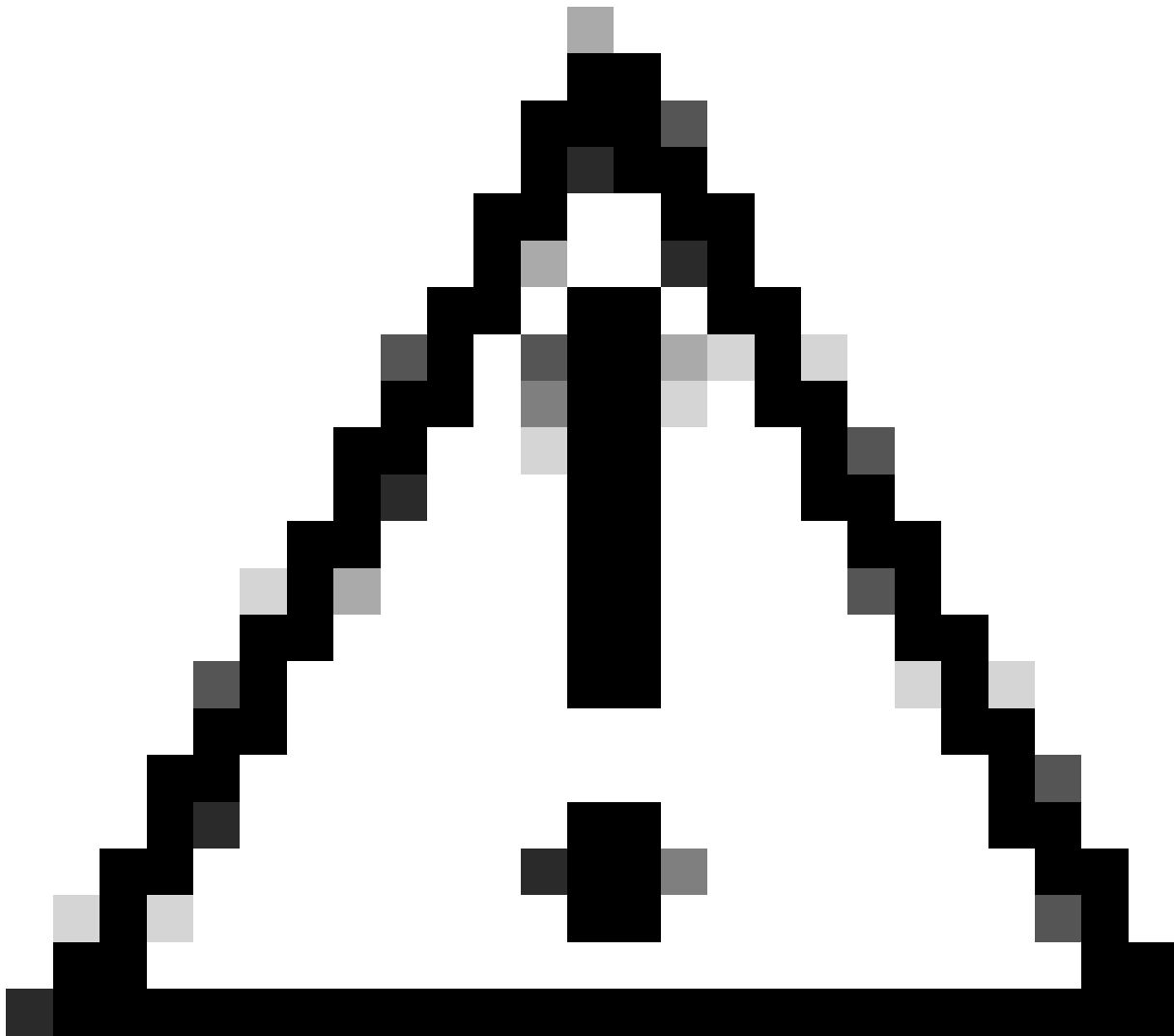
Cisco recommends that you have knowledge of these topics:

- macOS devices must be managed by JAMF.
- For MDM enrollment instructions for macOS, refer to [JAMF documentation](#).

Components Used

The information in this document is based on Cisco Secure Client.

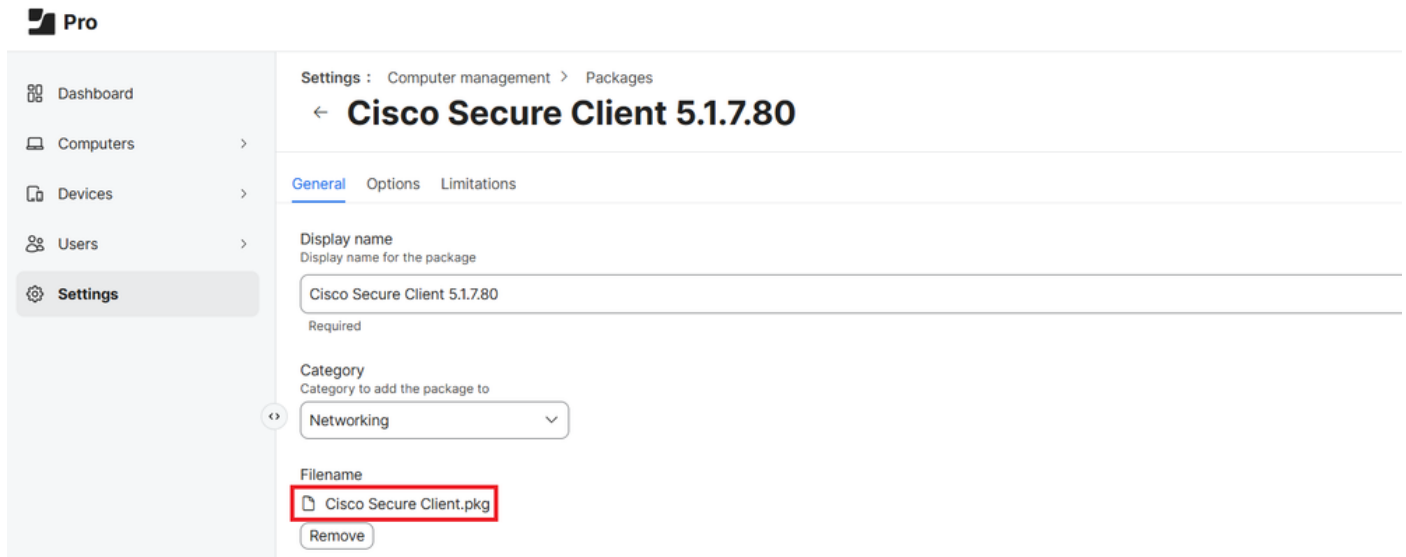
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.



Caution: This article is provided as-is as of February 1, 2025. Cisco Umbrella Support does not guarantee these instructions are valid after this date and are subject to change based on updates from JAMF and Apple.

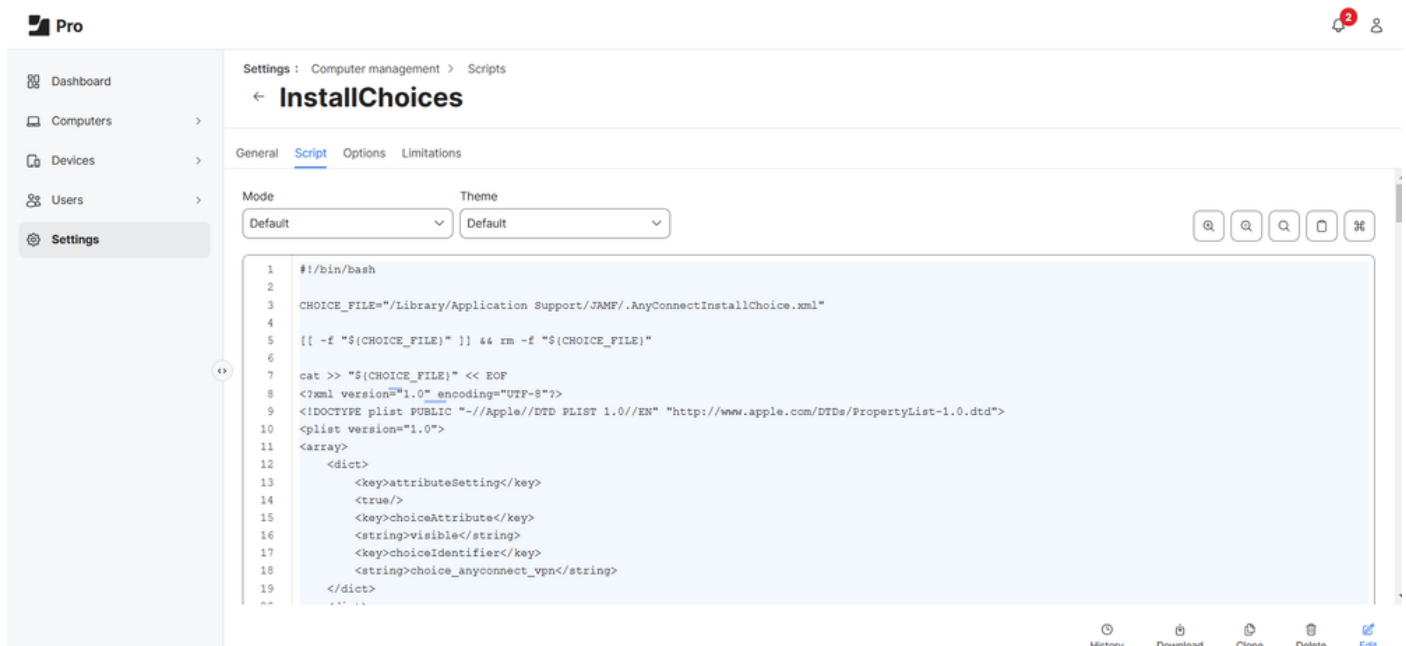
Upload the Installation Package (PKG)

1. Download the Cisco Secure Client DMG from the Umbrella dashboard under **Deployments > Roaming Computers > Roaming Client > Pre-Deployment Package > macOS**.
2. Log in to your JAMF Pro cloud instance.
3. Navigate to **Settings > Computer Management > Packages > New**.
4. Upload the PKG extracted from the DMG package you downloaded from your Umbrella dashboard.



Add Configuration and Module Selection Scripts

1. Go to **Settings > Computer Management > Scripts** and add this script to control which modules are installed during deployment.
2. You can control the installation of Secure Client modules by setting a module to **0** to skip it or **1** to install it as the PKG is configured to install all modules by default.
 - You can get the sample XML file from the Umbrella documentation: [Customize macOS installation of Cisco Secure Client](#)
 - Umbrella also added the "installchoices" script to this [github link](#). In this example, the Core VPN, Umbrella, and DART modules are set to **1** and can be included in the Secure Client installation.



3. Navigate to **Settings > Computer management > Scripts** and add this script so that it creates a configuration file `Orginfo.json` that is required by Cisco Secure Client.

- Download the module profile directly from the Umbrella dashboard, then add the **Organization ID**,

Fingerprint, and User ID to the script:

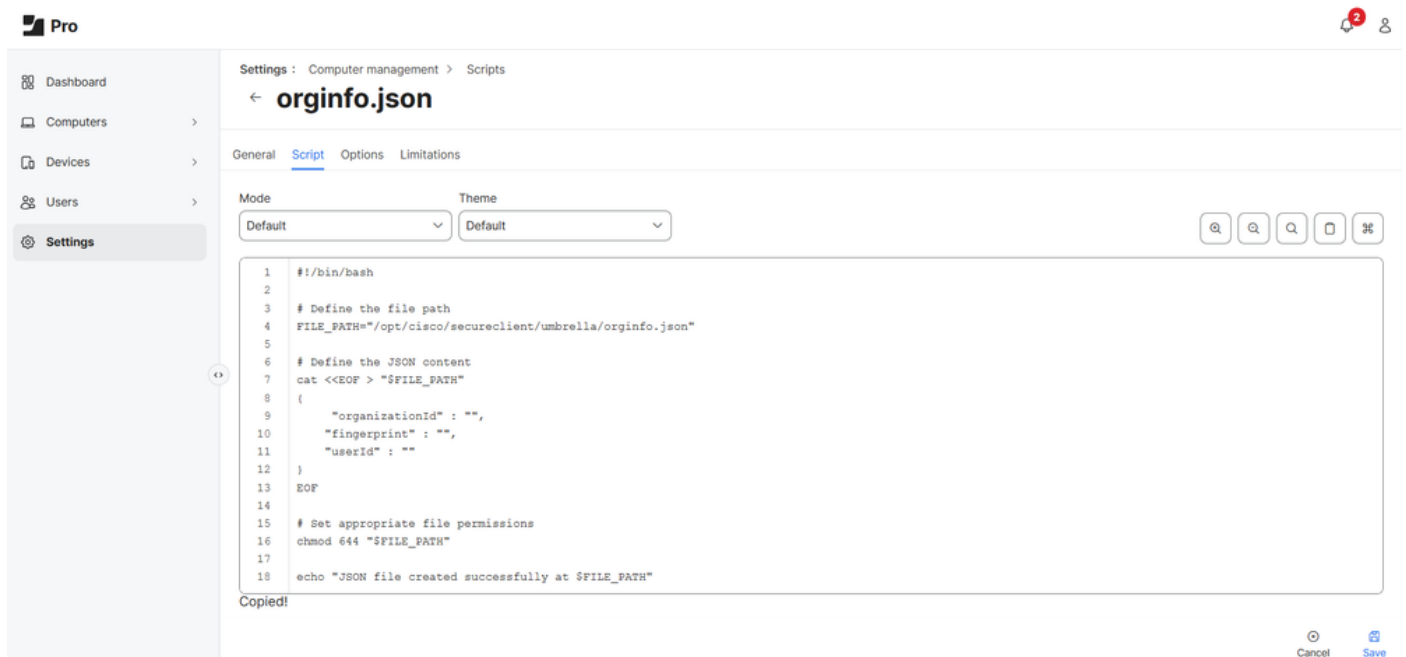
```
#!/bin/bash

# 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

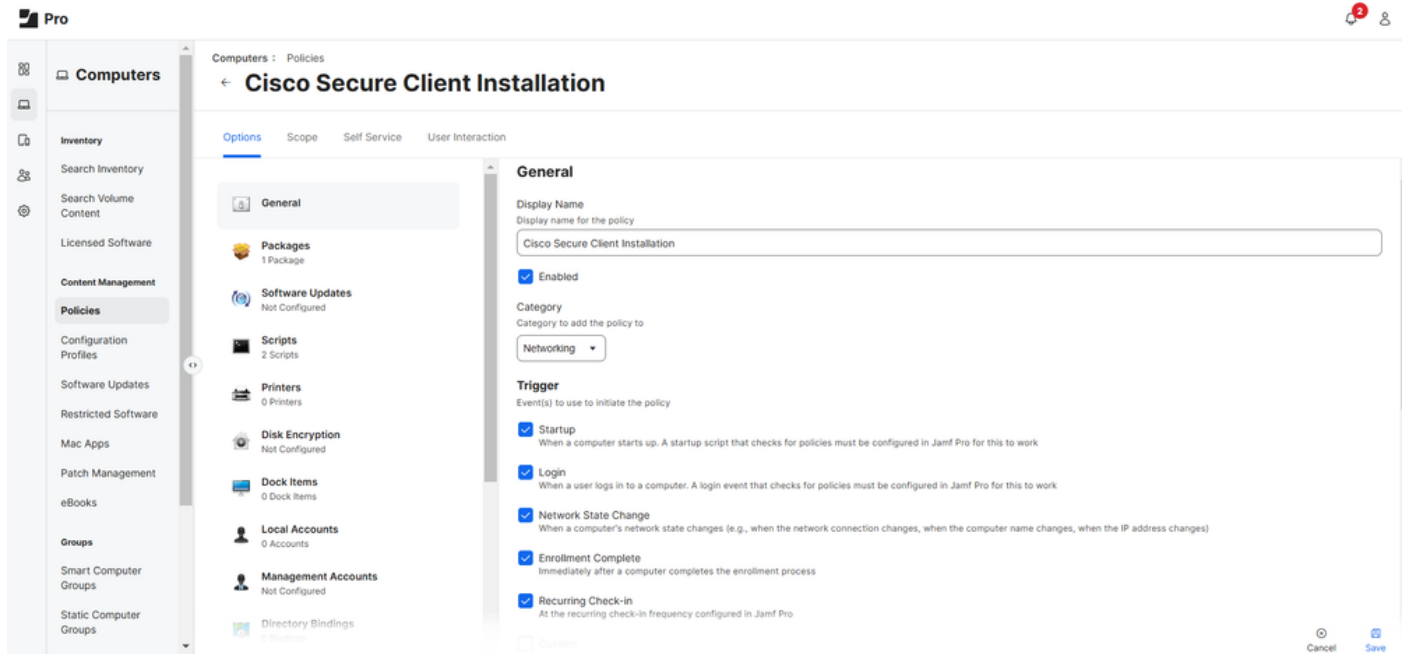
Create the JAMF Policy

The JAMF Policy is used to determine how and when the Cisco Secure Client with Umbrella module is pushed out.

1. Navigate to **Computers > Content Management > Policies > New**.
2. Assign a unique name to the policy and select your desired **Category** and **Trigger** events (for example, when this policy is executed).
3. Optionally, you can also configure a custom command that can be executed under Custom. The command

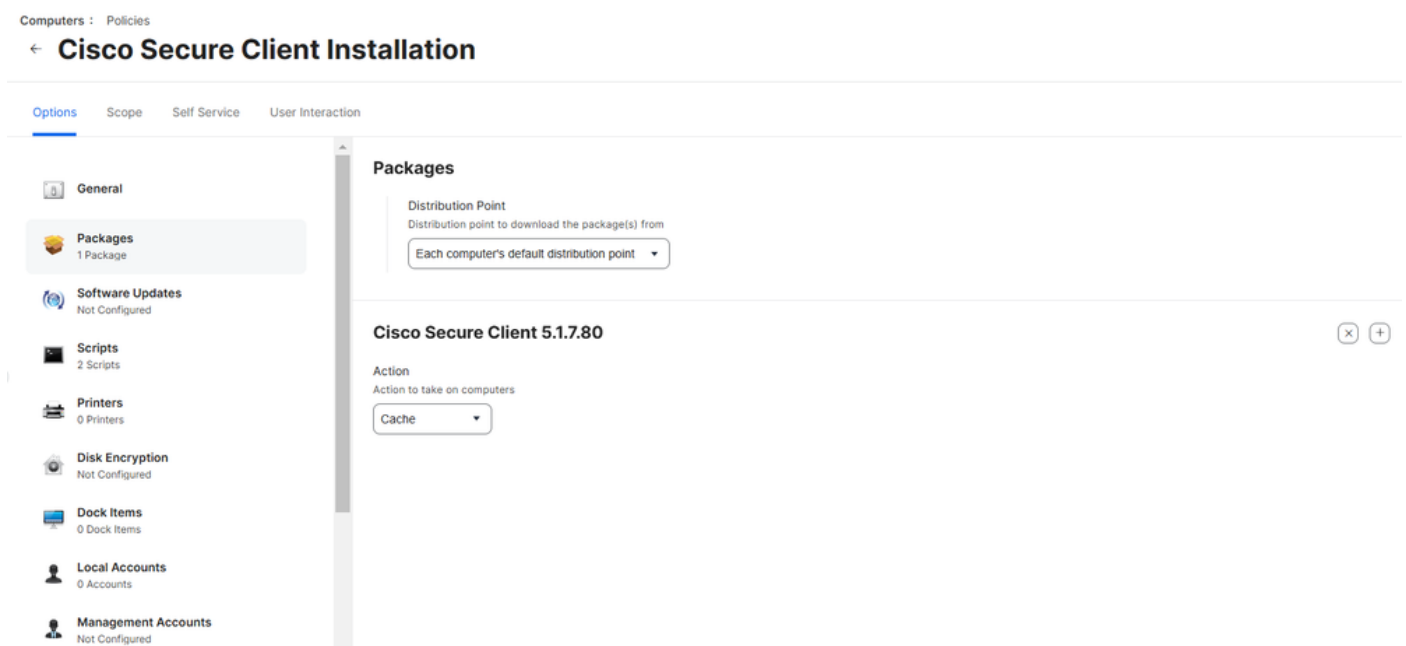
to execute and run this policy would look something like this:

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



4. Select **Packages** > **Configure** and select **Add** next to your Cisco Secure Client package.

- Under **Distribution Point**, select **Each computer's default distribution point**.
- Under **Action**, select **Cache**.



5. Define the scope of devices or users for deployment and select **Save**.

Computers : Policies

← 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. Add both the `InstallChoices` and `orginfo.json` scripts and give them a Priority to use for running the script in relation to other actions.

Pro

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

Cancel Save

Pro

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

orginfo.json

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

After

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

Parameter 4

Parameter 5

Parameter 6

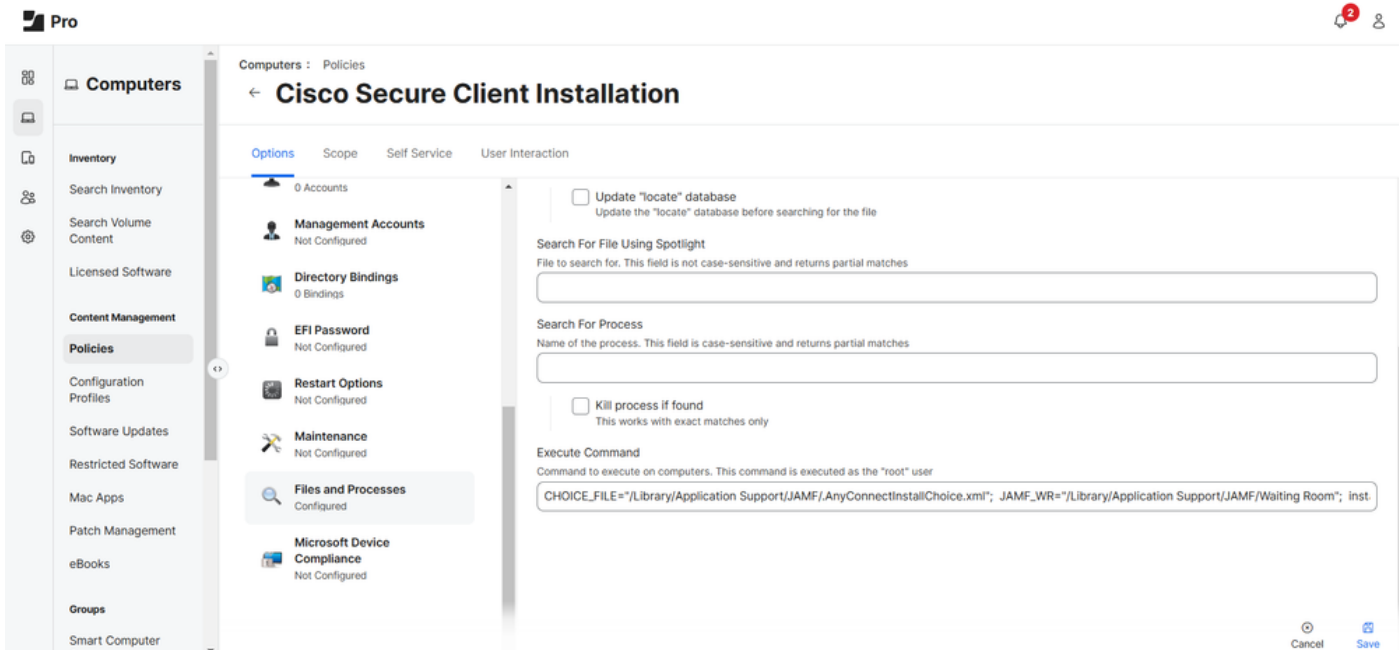
Parameter 7

Parameter 8

Cancel Save

7. Execute this command to install the Cisco Secure Client package with the selected modules on devices:

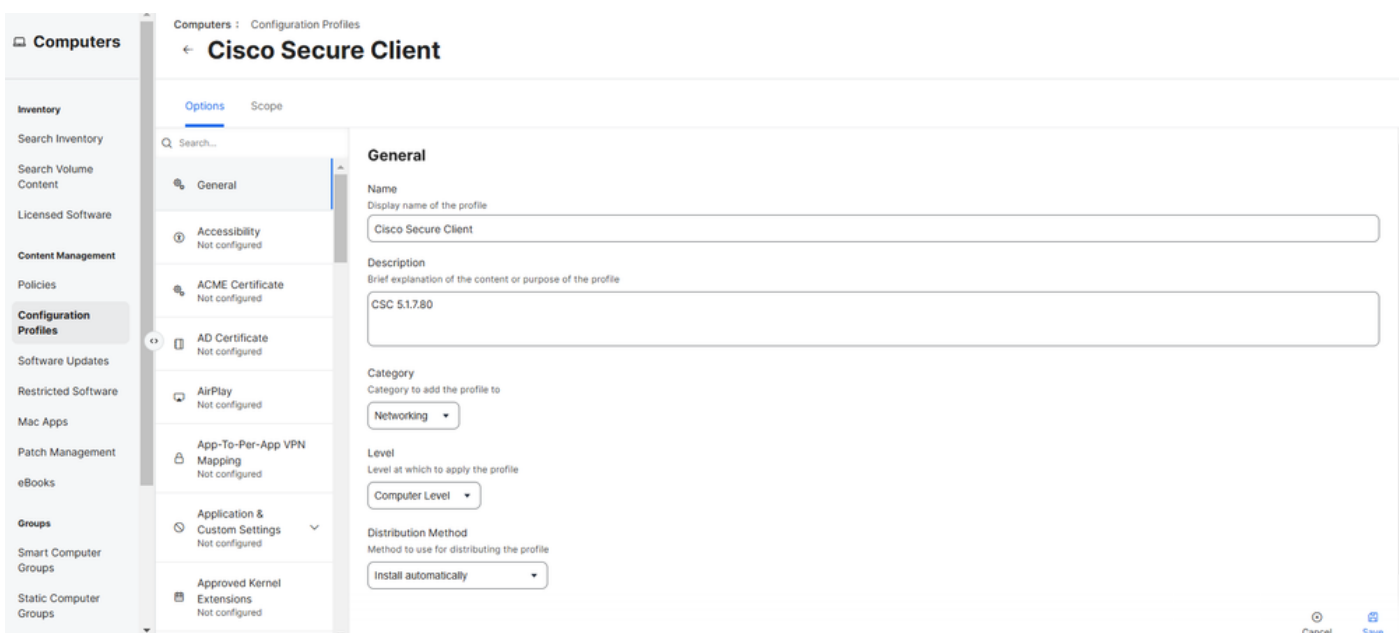
```
CHOICE_FILE="/Library/Application Support/JAMF/.AnyConnectInstallChoice.xml"; JAMF_WR="/Library/Applica
```



Configure a Silent Install of System Extension

Next, use JAMF to configure and allow Cisco Secure Client's required System Extensions in order for Cisco Secure Client with Umbrella module to run correctly without user interactions.

1. Go to **Computers > Content Management > Configuration Profiles > New**.
2. Give the profile a unique name and select your **Category** and **Distribution Method**.
3. Ensure **Level** is set to **Computer Level**.



4. Search for **System Extensions > Configure**. Enter these values:

- **Display Name:** Cisco Secure Client - System Extensions
- **System Extension Types:** Allowed System Extensions
- **Team Identifier:** DE8Y96K9QP

- **Allowed System Extensions:** com.cisco.anyconnect.macos.acsockext, then select **Save**.

The screenshot shows the 'Cisco Secure Client' configuration page under 'System Extensions'. The 'Allowed System Extensions and Teams IDs' section is active. The 'Display Name' is 'Cisco Secure Client - System Extensions'. The 'System Extension Types' dropdown is set to 'Allowed system extensions'. 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".' The 'Team Identifier' is 'DE8Y96K9QP'. Below, the 'ALLOWED SYSTEM EXTENSIONS' list contains 'com.cisco.anyconnect.macos.acsockext' with 'Edit' and 'Delete' buttons. An '+ Add' button is at the bottom right.

5. Select the + icon next to **Allowed Team IDs and System Extensions** to add another System Extension. Then, enter these values:

- **Display Name:** Cisco Secure Client - System Extensions
- **System Extension Types:** Allow System Extension Types
- **Team Identifier:** DE8Y96K9QP
- **Allow System Extension Types:** Network Extension

This screenshot shows the same configuration page as before, but with the 'Allowed System Extension Types' dropdown set to 'Allowed system extension types'. Under the 'Allowed System Extension Types' section, three checkboxes are visible: 'Driver Extension' (unchecked), 'Endpoint Security Extension' (unchecked), and 'Network Extension' (checked). The '+ Add' button is now visible at the top right of the configuration area.

Configure Silent Install for Content Filter

Next, configure a silent install for the Content Filter, which correlates to the Cisco Secure Client with Umbrella module's Socket Filter:

1. Search for **Content Filter**. Enable and complete these fields with their respective values:

- **Filter Name:** Cisco Secure Client - WebContentFilter
- **Identifier:** com.cisco.anyconnect.macos.acsock
- **Socket Filter:** Enabled
- **Socket Filter Bundle Identifier:** com.cisco.anyconnect.macos.acsockext
- **Socket Filter Designated Requirement:**
 anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and
 (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate
 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate
 leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] =
 DE8Y96K9QP)

The screenshot shows the 'Cisco Secure Client' configuration page in the 'Options' tab. The 'Content Filter' section is active, showing settings for a filter named 'Cisco Secure Client - WebContentFilter'. The 'Identifier' is set to 'com.cisco.anyconnect.macos.acsock'. The 'Service Address' and 'Organization' fields are empty. The 'Filter Name' is 'Cisco Secure Client - WebContentFilter'. The 'Include' toggle is turned on.

The screenshot shows the 'Cisco Secure Client' configuration page in the 'Options' tab. The 'Socket Filter' section is active, showing settings for a filter named 'Cisco Secure Client - WebContentFilter'. The 'Socket Filter' is set to 'Enabled'. The 'Socket Filter Bundle Identifier' is set to 'com.cisco.anyconnect.macos.acsockext'. The 'Socket Filter Designated Requirement' is set to 'anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext" and (certificate leaf[field.1.2.840.113635.100.6.1.9] /* exists */ or certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */'. The 'Network Filter' and 'Browser Filter' are set to 'Ignore'.

2. Under **Custom Data**, select **Add** five times and enter these values:

Key	Value
AutoFilterEnabled	false
FilterBrowsers	false

FilterSockets	true
FilterPackets	false
FilterGrade	firewall

Configure Managed Login Items

Configuring the Managed Login Items for the Cisco Secure Client with Umbrella module ensures that the Cisco Secure Client launches upon device startup.

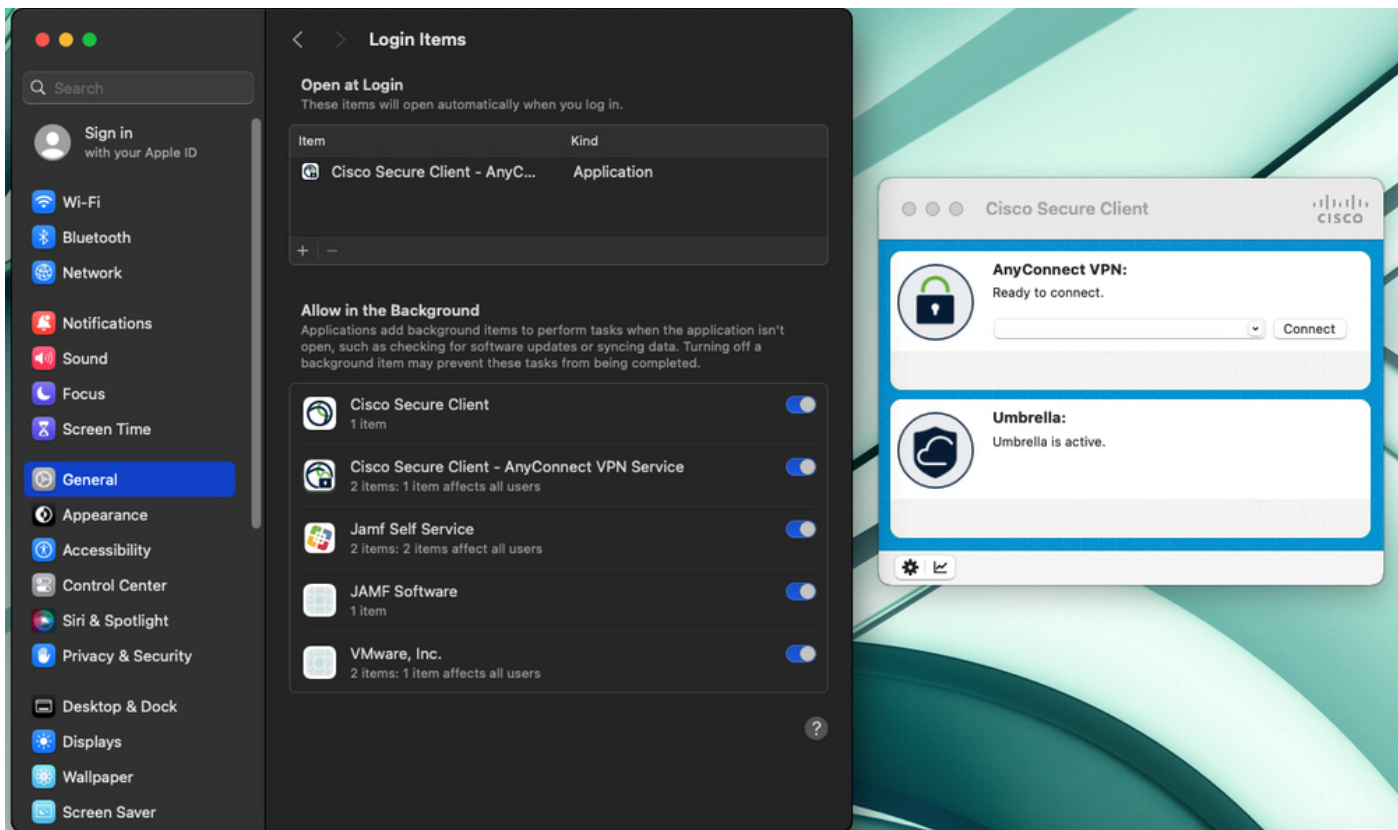
To configure, search for **Managed Login Items** and configure the fields with these values:

- **Rule Type:** Bundle Identifier Prefix
- **Rule Value:** com.cisco.secureclient
- **Team Identifier:** DE8Y96K9QP

The screenshot shows the Cisco Secure Client configuration interface. On the left is a sidebar with a navigation menu including 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, and Groups. The main panel is titled 'Computers : Configuration Profiles' and 'Cisco Secure Client'. It has two tabs: 'Options' and 'Scope'. Under 'Options', there is a search bar with 'managed login items' and a result count of '1'. Below the search bar is a list of items, with 'Managed Login Items' selected and showing '1 setting configured'. The 'Managed Login Items' section has a 'Setting' tab and a 'Managed Login item rules' section. The 'Managed Login item rules' section has a description: '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 'Managed Login item rules' section, there are two buttons: 'Exclude all' and 'Include', with the 'Include' button being active (blue toggle).

Assign Scope and Push Deployment

1. Navigate to **Scope** and define the scope for devices or users.
2. The Cisco Secure Client with Umbrella module can be pushed out to your desired macOS devices when one of the Triggers that you configured in step 2 of **Create a JAMF Policy** is activated. Alternatively, you can push this out through [JAMF's Self Service portal](#).





Note: Even if a user tries to disable the DNS Proxy or Transparent Proxy in System Settings (Network > Filter), it automatically is re-enabled by default as the Content Filter is enabled via JAMF as described in this article and cannot be disabled.

Configure macOS Firewall Exception

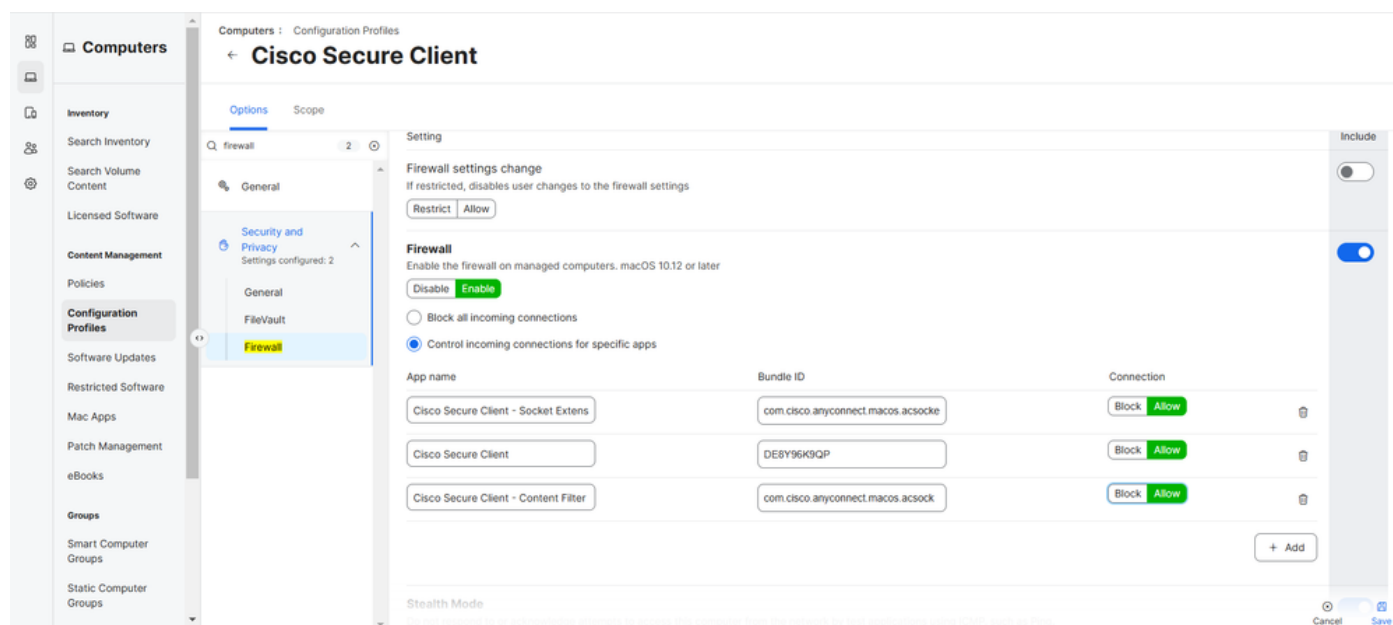
If the macOS firewall is set to [Block all incoming connections](#), you must also add the Cisco Secure Client and its components to its exceptions list:

1. Navigate to **Computers > Content Management > Configuration Profiles**.
2. Select your Cisco Secure Client configuration profile and locate **Security and Privacy**.
3. Configure it with these settings:
 - Firewall: **Enable - Control incoming connections for specific apps**

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

Cisco Secure Client - Content Filter

com.cisco.anyconnect.macos.acsock



4. Select **Save**.

5. If you are prompted with **Redistribution Options**, select **Distribute to All** to immediately push out the changes to your desired macOS devices.

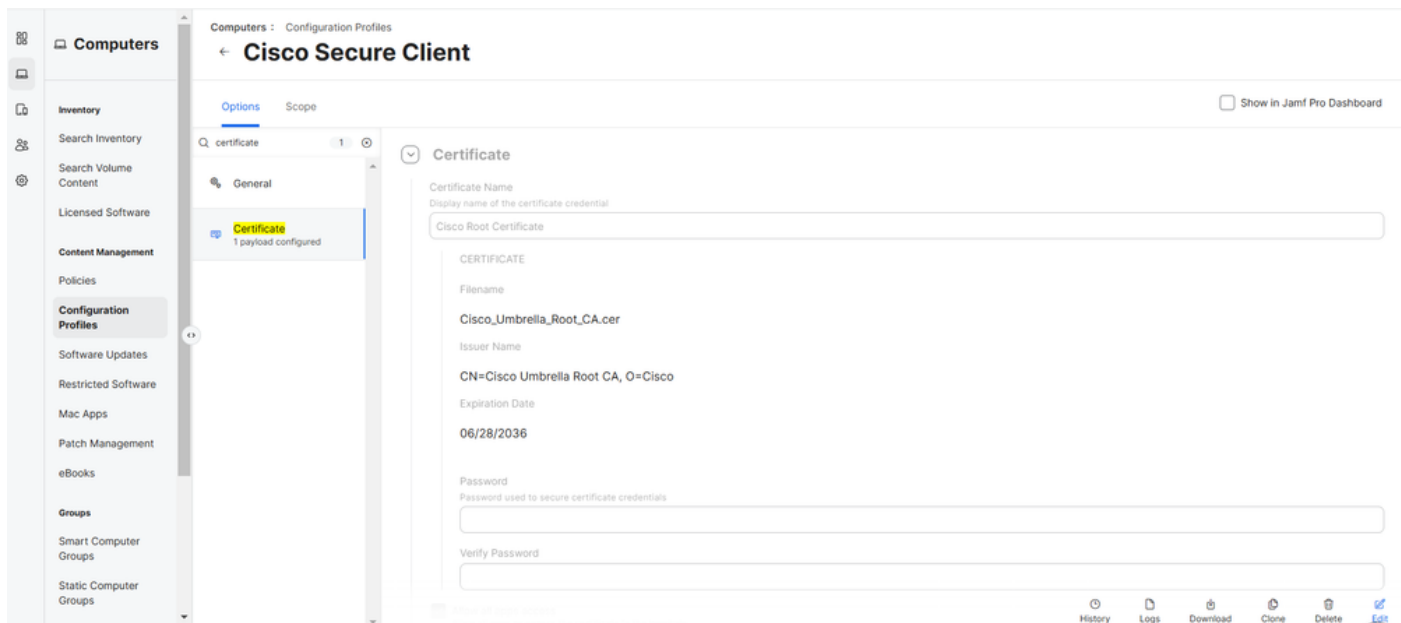
Deploy the Cisco Umbrella Root Certificate



Note: This step only applies to new deployments of Cisco Secure Client or devices that does not have the Cisco Umbrella Root Certificate deployed previously. If you are migrating over from the Umbrella Roaming Client or Cisco AnyConnect 4.10 client, and/or have deployed the Cisco Umbrella Root Certificate already in the past, you can skip this section.

Download the Cisco Umbrella Root Certificate from **Policies > Root Certificate** in the Umbrella dashboard.

1. In the Umbrella dashboard under **Policies > Root Certificate**, download the **Cisco Umbrella Root Certificate**.
2. In JAMF, navigate to **Computers > Configuration Profiles > Cisco Secure Client > Edit**.
3. Search for **Certificate > Configure**. Give it a unique name.
4. Under **Select Certificate Option**, select **Upload** and upload the Cisco Umbrella Root Certificate that you downloaded previously in Step 1.
5. Ensure you that you **do not** configure a password here and select **Save**.



6. If you are prompted with **Redistribution Options**, select **Distribute to All** to immediately push out the changes to your desired macOS devices.

Verification

To verify if Cisco Secure Client with Umbrella module is working, browse to <https://policy-debug.checkumbrella.com> or run this command:

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

Either output must contain unique and relevant information to your Umbrella organization, such as your OrgID.

Workaround for macOS 14.3

For macOS 14.3 (or later) with Cisco Secure Client 5.1.x, if you encounter "The VPN client agent was unable to create the interprocess communication depot":

1. In JAMF, navigate to **Settings > Computer Management > Scripts > New**.
2. Give it a unique name and define your category.
3. Navigate to the **Script** tab and add this:

```
#!/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. Under **Options**, ensure the **Priority** is set to **After**. This bash script checks if the Cisco Secure Client - AnyConnect VPN service.app is running via returning an expected output with the Process ID from pgrep - fl.

- If it returns an empty output, then you can confirm the Cisco Secure Client - AnyConnect VPN service.app is not running and the script executes to launch the Cisco Secure Client core services that are required in order for the Umbrella module to run correctly.

Automatic Updates

Cisco has decided to extend [auto-update support](#) from the Umbrella dashboard to include Secure Client starting with Secure Client 5.1.6.103 (MR6). Going forward, customers who have upgraded to at least Cisco Secure Client 5.1.6 MR6 are able to auto update to newer versions if auto-update has been configured in the Umbrella dashboard.