

Bereitstellung von CSC in MacOS mithilfe von JAMF mit Umbrella Module

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Installationspaket hochladen \(PKG\)](#)

[Hinzufügen von Konfigurations- und Modulauswahlskripts](#)

[Erstellen der JAMF-Richtlinie](#)

[Konfigurieren einer automatischen Installation der Systemerweiterung](#)

[Automatische Installation für Content-Filter konfigurieren](#)

[Verwaltete Anmeldeelemente konfigurieren](#)

[Zuweisung von Umfang und Push-Bereitstellung](#)

[macOS-Firewallausnahme konfigurieren](#)

[Bereitstellung des Cisco Umbrella Root-Zertifikats](#)

[Verifizierung](#)

[Problemumgehung für macOS 14.3](#)

[Automatische Updates](#)

Einleitung

In diesem Dokument wird die Bereitstellung von Cisco Secure Client mit dem Umbrella-Modul auf verwalteten MacOS-Geräten mithilfe von JAMF beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

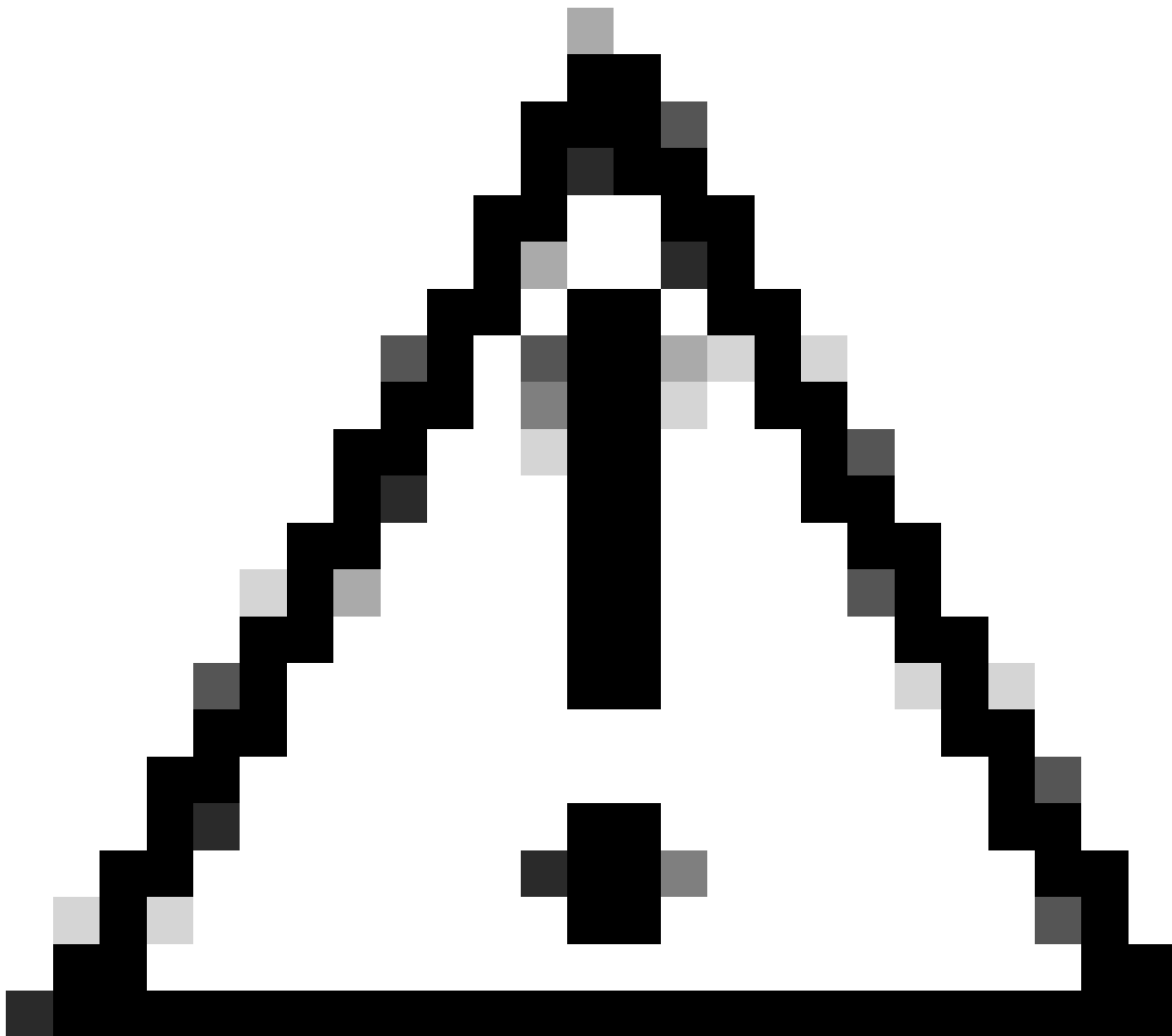
- macOS-Geräte müssen von JAMF verwaltet werden.
- Anweisungen zur MDM-Registrierung für macOS finden Sie in der [JAMF-Dokumentation](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Secure Client.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer

gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

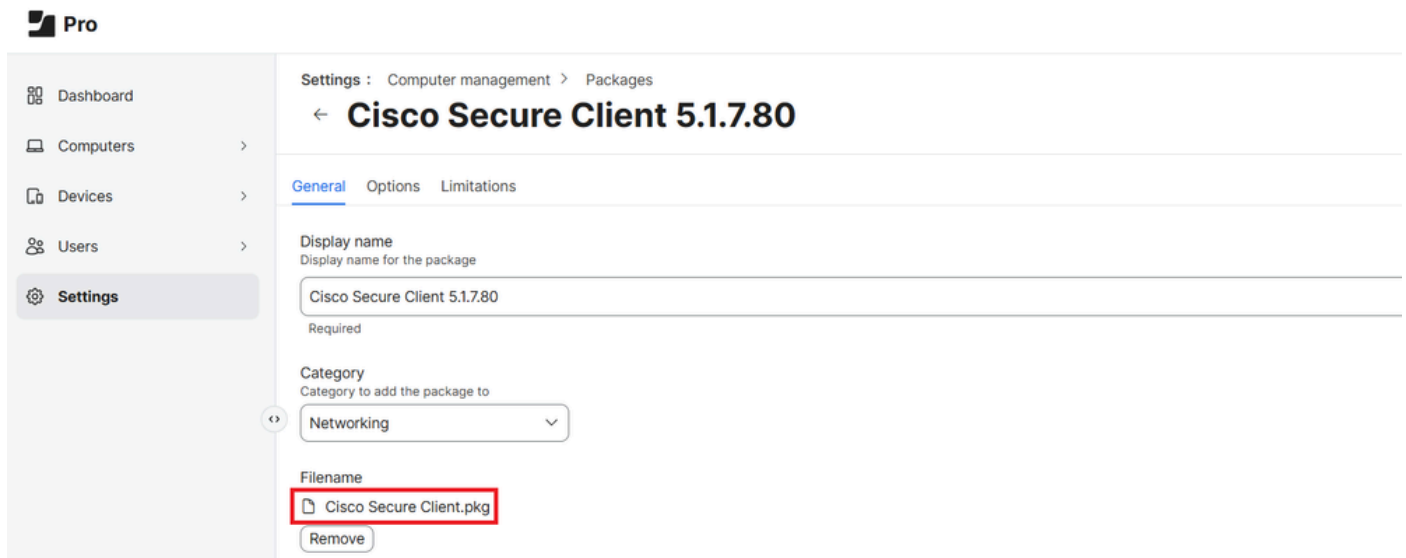


Vorsicht: Dieser Artikel wird mit Stand vom 1. Februar 2025 zur Verfügung gestellt. Cisco Umbrella Support garantiert nicht, dass diese Anweisungen nach diesem Datum gültig sind und sich aufgrund von Updates von JAMF und Apple ändern können.

Installationspaket hochladen (PKG)

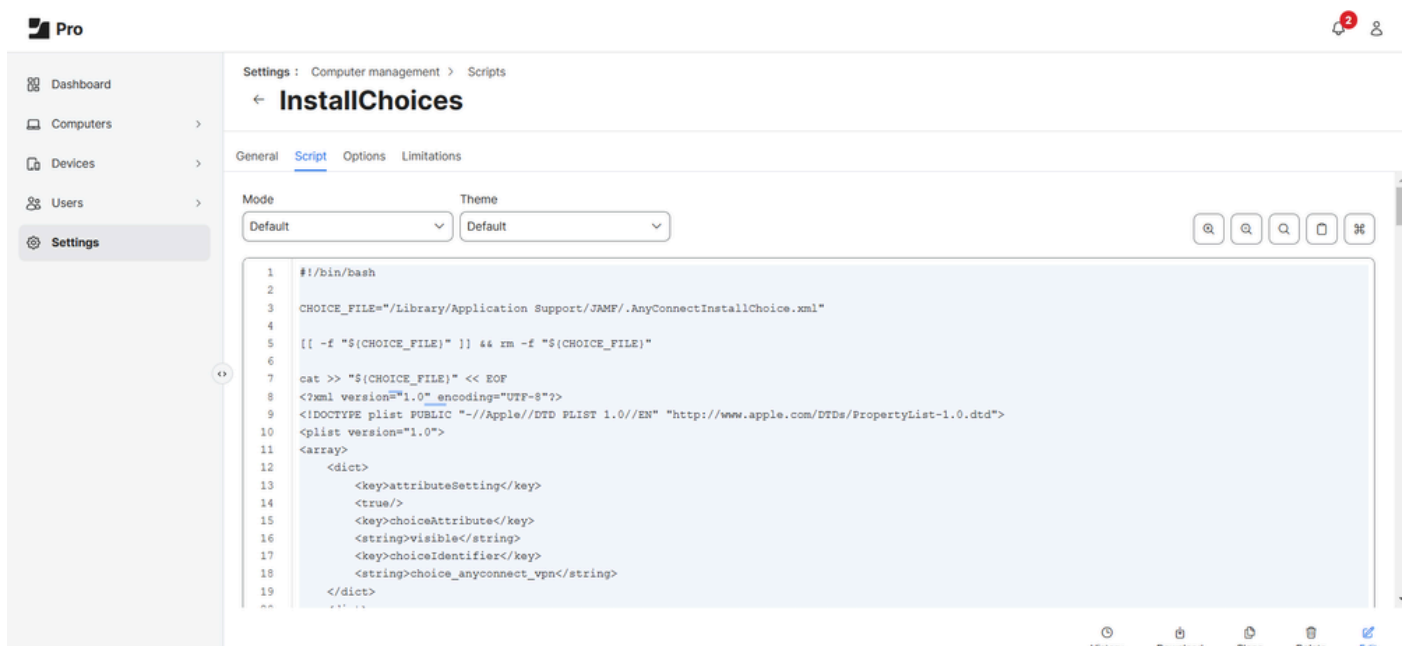
1. Laden Sie Cisco Secure Client DMG vom Umbrella Dashboard unter Bereitstellungen > Roaming-Computer > Roaming-Client > Pre-Deployment-Package > macOS herunter.
2. Melden Sie sich bei Ihrer JAMF Pro Cloud-Instanz an.
3. Navigieren Sie zu Einstellungen > Computerverwaltung > Pakete > Neu.
4. Laden Sie das aus dem DMG-Paket extrahierte PKG hoch, das Sie von Ihrem Umbrella

Dashboard heruntergeladen haben.



Hinzufügen von Konfigurations- und Modulauswahlskripts

1. Gehen Sie zu Einstellungen > Computerverwaltung > Skripte, und fügen Sie dieses Skript hinzu, um zu steuern, welche Module während der Bereitstellung installiert werden.
 2. Sie können die Installation von Secure Client-Modulen steuern, indem Sie ein Modul auf 0 setzen, um es zu überspringen, oder auf 1, um es zu installieren, da die PKG so konfiguriert ist, dass alle Module standardmäßig installiert werden.
- Die XML-Beispieldatei finden Sie in der Umbrella-Dokumentation: [Anpassen der MacOS-Installation von Cisco Secure Client](#)
 - Umbrella hat außerdem das Skript "installchoice" zu diesem [Gigithub-Link](#) hinzugefügt. In diesem Beispiel sind die Core-VPN-, Umbrella- und DART-Module auf 1 festgelegt und können in die Secure Client-Installation integriert werden.



3. Navigieren Sie zu Einstellungen > Computerverwaltung> Skripte, und fügen Sie dieses Skript hinzu, sodass es eine Konfigurationsdatei `orginfo.json` erstellt, die für den Cisco Secure Client erforderlich ist.

- Laden Sie das Modulprofil direkt vom Umbrella Dashboard herunter, und fügen Sie dann die Organisations-ID, den Fingerabdruck und die Benutzer-ID zum Skript hinzu:

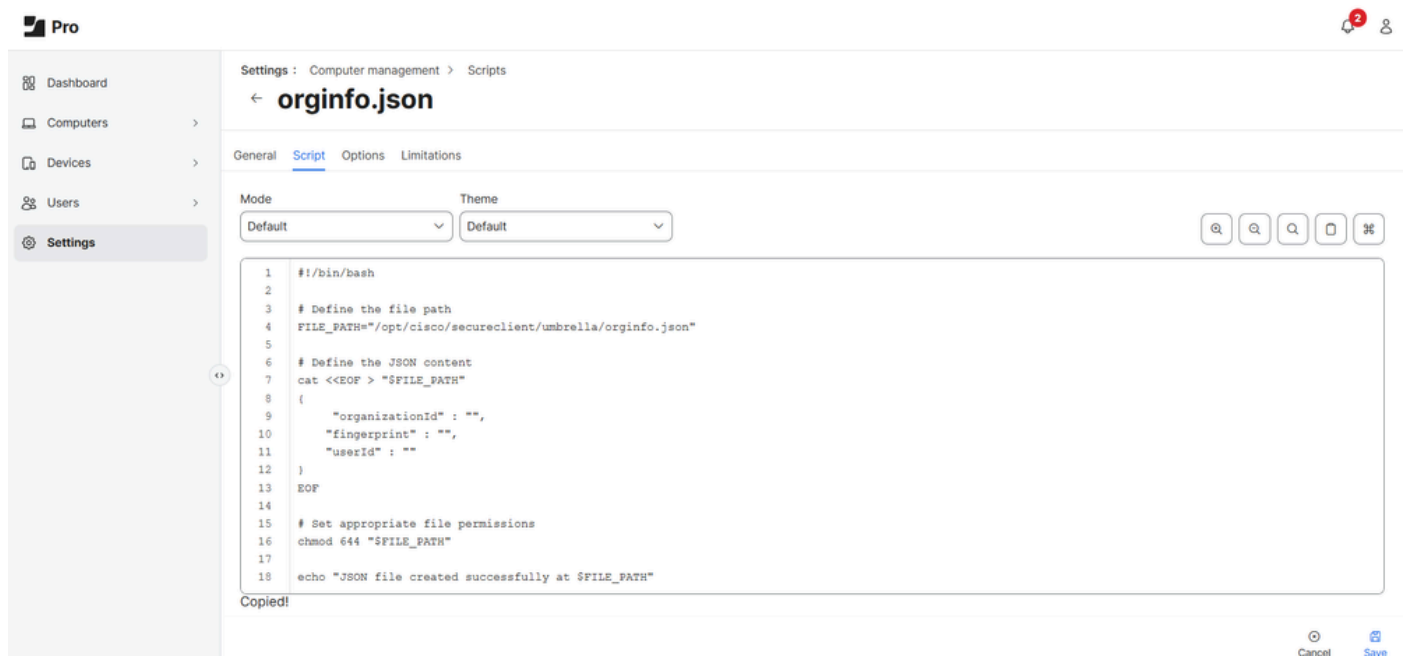
```
#!/bin/bash

# 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"
```



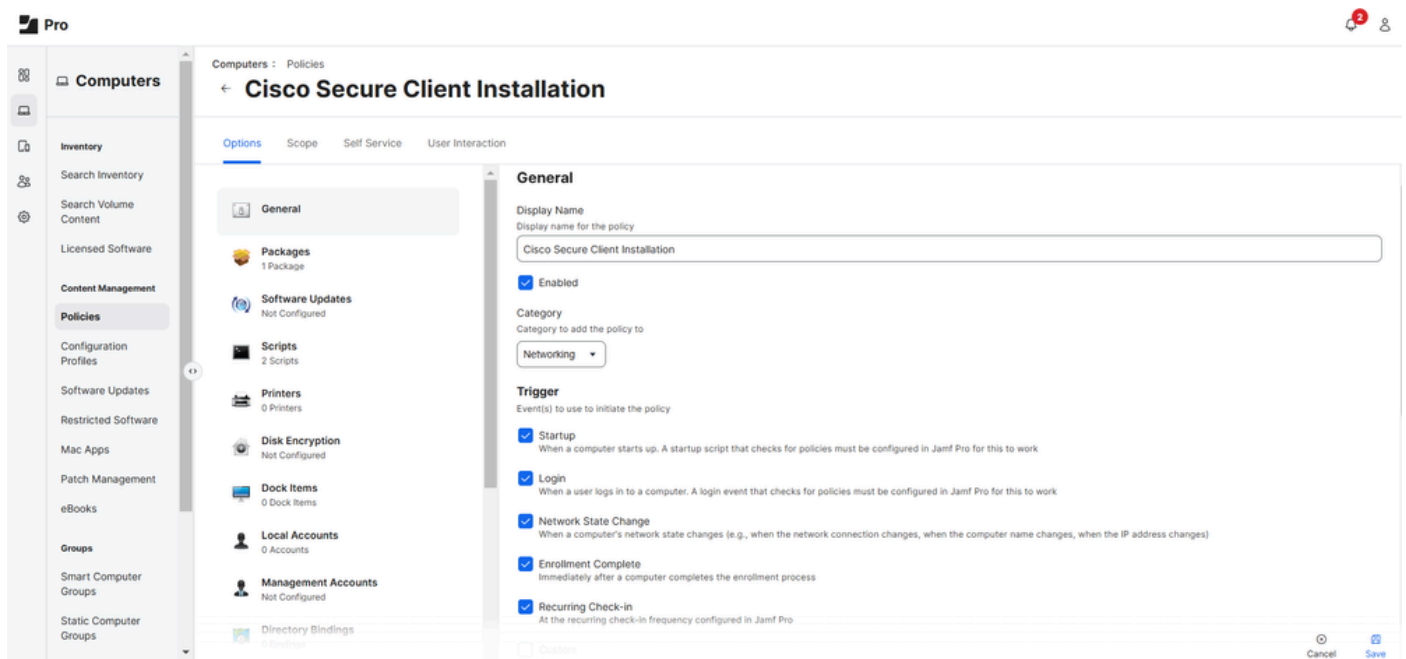
34452906673812

Erstellen der JAMF-Richtlinie

Anhand der JAMF-Richtlinie wird festgelegt, wie und wann das Cisco Secure Client mit Umbrella-Modul ausgeliefert wird.

1. Navigieren Sie zu **Computer > Inhaltsverwaltung > Richtlinien > Neu**.
2. Weisen Sie der Richtlinie einen eindeutigen Namen zu, und wählen Sie die gewünschten Kategorie- und Trigger-Ereignisse aus (z. B. bei der Ausführung dieser Richtlinie).
3. Optional können Sie auch einen benutzerdefinierten Befehl konfigurieren, der unter Benutzerdefiniert ausgeführt werden kann. Der Befehl zum Ausführen dieser Richtlinie sieht in etwa wie folgt aus:

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



4. Wählen Sie **Packages > Configure** und anschließend **Add** neben Ihrem Cisco Secure Client-Paket.

- Wählen Sie unter Verteilungspunkt die Option Standardverteilungspunkt jedes Computers aus.
- Wählen Sie unter Aktion die Option Cache aus.

← 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. Definieren Sie den Umfang der Geräte oder Benutzer für die Bereitstellung, und wählen Sie Speichern aus.

← 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. Fügen Sie sowohl das Skript `InstallChoices` als auch das `orginfo.json` Skript hinzu, und geben Sie ihnen eine Priorität, um das Skript in Bezug auf andere Aktionen auszuführen.



Computers

← 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

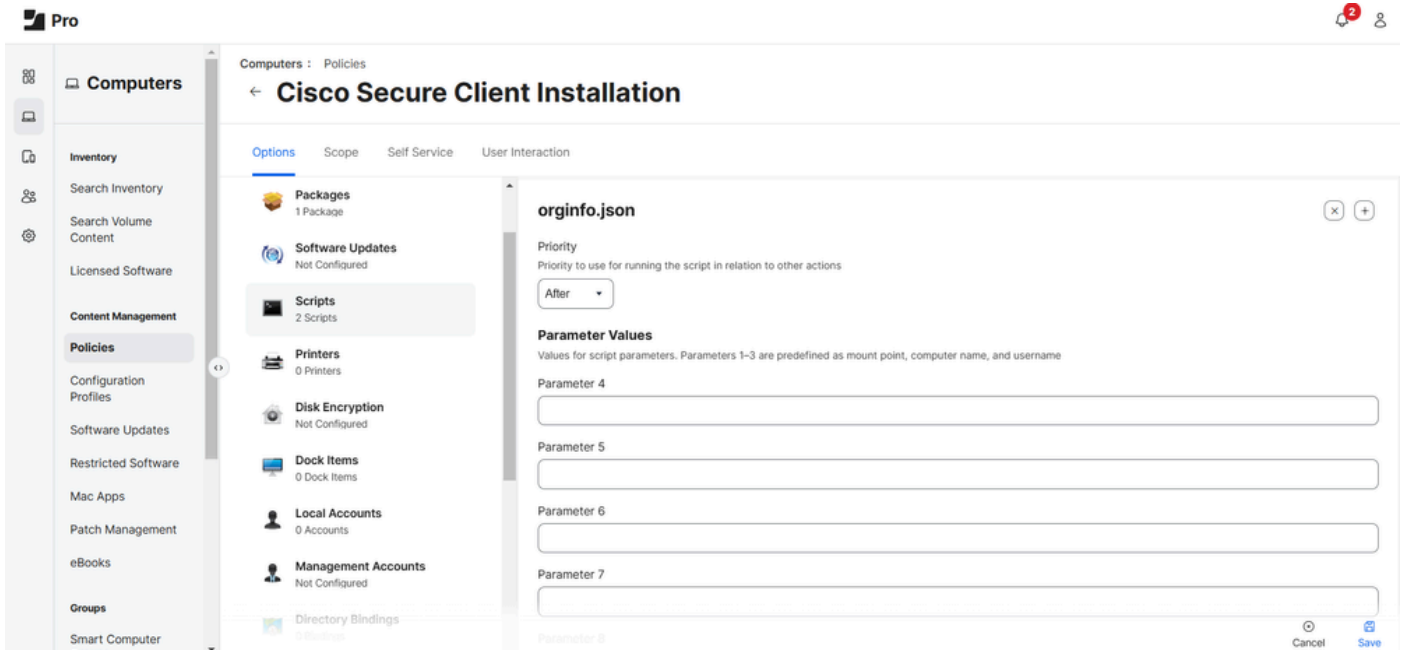
Parameter 4

Parameter 5

Parameter 6

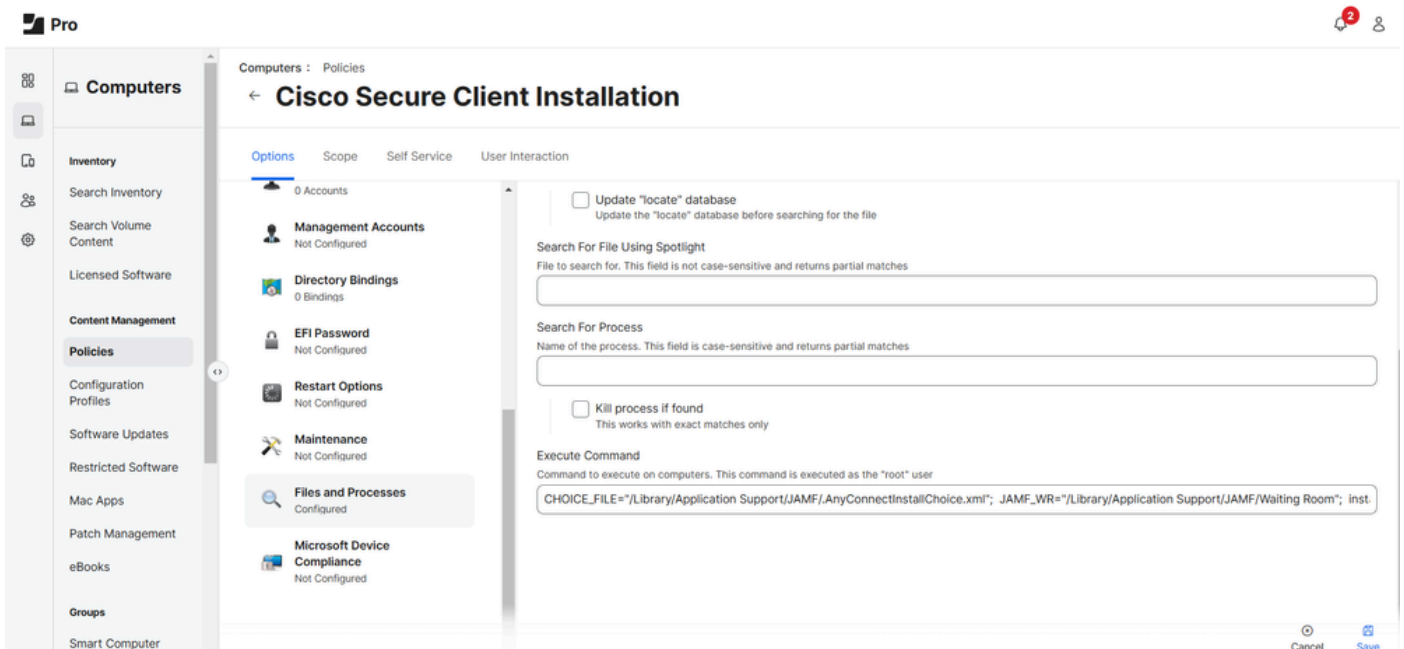
Parameter 7

Cancel Save



7. Führen Sie diesen Befehl aus, um das Cisco Secure Client-Paket mit den ausgewählten Modulen auf den Geräten zu installieren:

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



Konfigurieren einer automatischen Installation der Systemerweiterung

Verwenden Sie anschließend JAMF, um die erforderlichen Systemerweiterungen des Cisco

Secure Client zu konfigurieren und zuzulassen, damit der Cisco Secure Client mit Umbrella-Modul ohne Benutzerinteraktionen ordnungsgemäß ausgeführt wird.

1. Gehen Sie zu **Computer > Content Management > Configuration Profiles > New**.
2. Geben Sie dem Profil einen eindeutigen Namen, und wählen Sie Kategorie und Verteilungsmethode aus.
3. Stellen Sie sicher, dass **Level** auf Computerebene festgelegt ist.

The screenshot shows the 'Cisco Secure Client' configuration page in the 'General' tab. The left sidebar lists various management categories, with 'Configuration Profiles' selected. The main area contains the following fields:

- Name:** Cisco Secure Client
- Description:** CSC 5.17.80
- Category:** Networking
- Level:** Computer Level
- Distribution Method:** Install automatically

At the bottom right, there are 'Cancel' and 'Save' buttons.

4. Suchen Sie nach **Systemerweiterungen > Konfigurieren**. Geben Sie folgende Werte ein:

- Anzeigename: Cisco Secure Client - Systemerweiterungen
- Systemerweiterungstypen: Zulässige Systemerweiterungen
- Team-ID: DE8Y96K9QP
- Zulässige Systemerweiterungen: com.cisco.anyconnect.macos.acsockext, und wählen Sie dann **Speichern**.

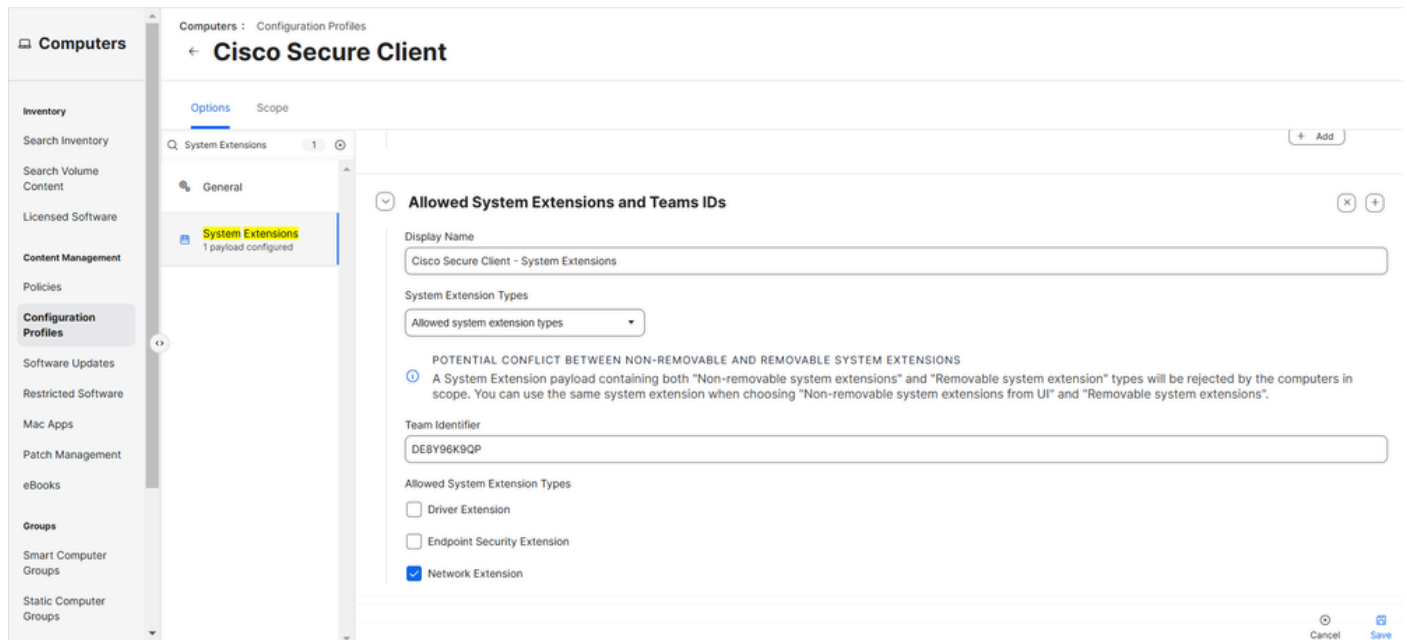
The screenshot shows the 'Cisco Secure Client' configuration page in the 'System Extensions' tab. The left sidebar is the same, but 'System Extensions' is now selected. The main area contains the following fields and sections:

- System Extensions:** A checkbox 'Allow users to approve system extensions' is checked.
- Allowed System Extensions and Teams IDs:** A section with a dropdown menu.
- Display Name:** Cisco Secure Client - System Extensions
- System Extension Types:** Allowed system extensions
- POTENTIAL CONFLICT BETWEEN NON-REMOVABLE AND REMOVABLE SYSTEM EXTENSIONS:** A warning message: '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".'
- Team Identifier:** DE8Y96K9QP
- ALLOWED SYSTEM EXTENSIONS:** A table with one entry: com.cisco.anyconnect.macos.acsockext. There are 'Edit' and 'Delete' buttons for this entry.

At the bottom right, there are 'Cancel' and 'Save' buttons.

5. Wählen Sie das Symbol + neben Zugelassene Team-IDs und Systemerweiterungen aus, um eine weitere Systemerweiterung hinzuzufügen. Geben Sie anschließend die folgenden Werte ein:

- Anzeigename: Cisco Secure Client - Systemerweiterungen
- Systemerweiterungstypen: Systemerweiterungstypen zulassen
- Team-ID: DE8Y96K9QP
- Systemerweiterungstypen zulassen: Netzwerkerweiterung



Automatische Installation für Content-Filter konfigurieren

Konfigurieren Sie anschließend eine automatische Installation für den Content-Filter, der mit dem Socket-Filter des Cisco Secure Client mit Umbrella-Moduls korreliert:

1. Suchen Sie nach Content-Filter. Aktivieren und vervollständigen Sie diese Felder mit den entsprechenden Werten:

- Filtername: Cisco Secure Client - WebContentFilter
- Identifikator: com.cisco.anyconnect.macos.acsock
- Socket-Filter: Aktiviert
- Kennung des Socket-Filterpakets: com.cisco.anyconnect.macos.acsockext
- Für Socketfilter festgelegte Anforderung:

Ankerapple generisch und Kennung "com.cisco.anyconnect.macos.acsockext" und (Zertifikatblatt[Feld.1.2.840.113635.100.6.1.9] /* existiert */ oder Zertifikat 1[Feld.1.2.840.113635.100.6.2.6] /* existiert */ und Zertifikat leaf[field.1.2.840.113635.100.6.1.13] /* existiert */ und certificate leaf[subject.OU] = DE8Y96K9QP)

Computers : Configuration Profiles

Cisco Secure Client

Options Scope

Search content filter 1

General

Content Filter
Settings configured: 5

Exclude all

Include

Setting

Filter Name
Display name of the filter in the app and on the device

Cisco Secure Client - WebContentFilter

Required

Identifier
Identifier for the filter plug-in

com.cisco.anyconnect.macos.acsock

Required

Service Address
Hostname or IP address or URL for the service

Organization
Organization for the filter plug-in

Cancel Save

Computers : Configuration Profiles

Cisco Secure Client

Options Scope

Search content filter 1

General

Content Filter
Settings configured: 5

Filter Order
Specify the order in which traffic is filtered. Filters with a grade of firewall see network traffic before filters with a grade of inspector.

Firewall

Socket Filter
Specify filtering of socket traffic

Ignore Enable

Socket Filter Bundle Identifier
Bundle identifier of the socket filter provider system extension

com.cisco.anyconnect.macos.acsockext

Socket Filter Designated Requirement
Designated requirement of the socket filter provider system extension

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 */)

Network Filter
Specify filtering of network packets

Ignore Enable

Browser Filter
Specify filtering of WebKit traffic

Ignore Enable

Cancel Save

2. Wählen Sie unter Benutzerdefinierte Daten die Option Hinzufügen fünfmal aus, und geben Sie die folgenden Werte ein:

Wichtigste	Wert
AutoFilter aktiviert	falsch
FilterBrowser	falsch
FilterSockets	wahr
FilterPakete	falsch
Filtergrad	Firewall

Verwaltete Anmeldeelemente konfigurieren

Durch die Konfiguration der verwalteten Anmeldeelemente für den Cisco Secure Client mit

Umbrella-Modul wird sichergestellt, dass der Cisco Secure Client beim Starten des Geräts gestartet wird.

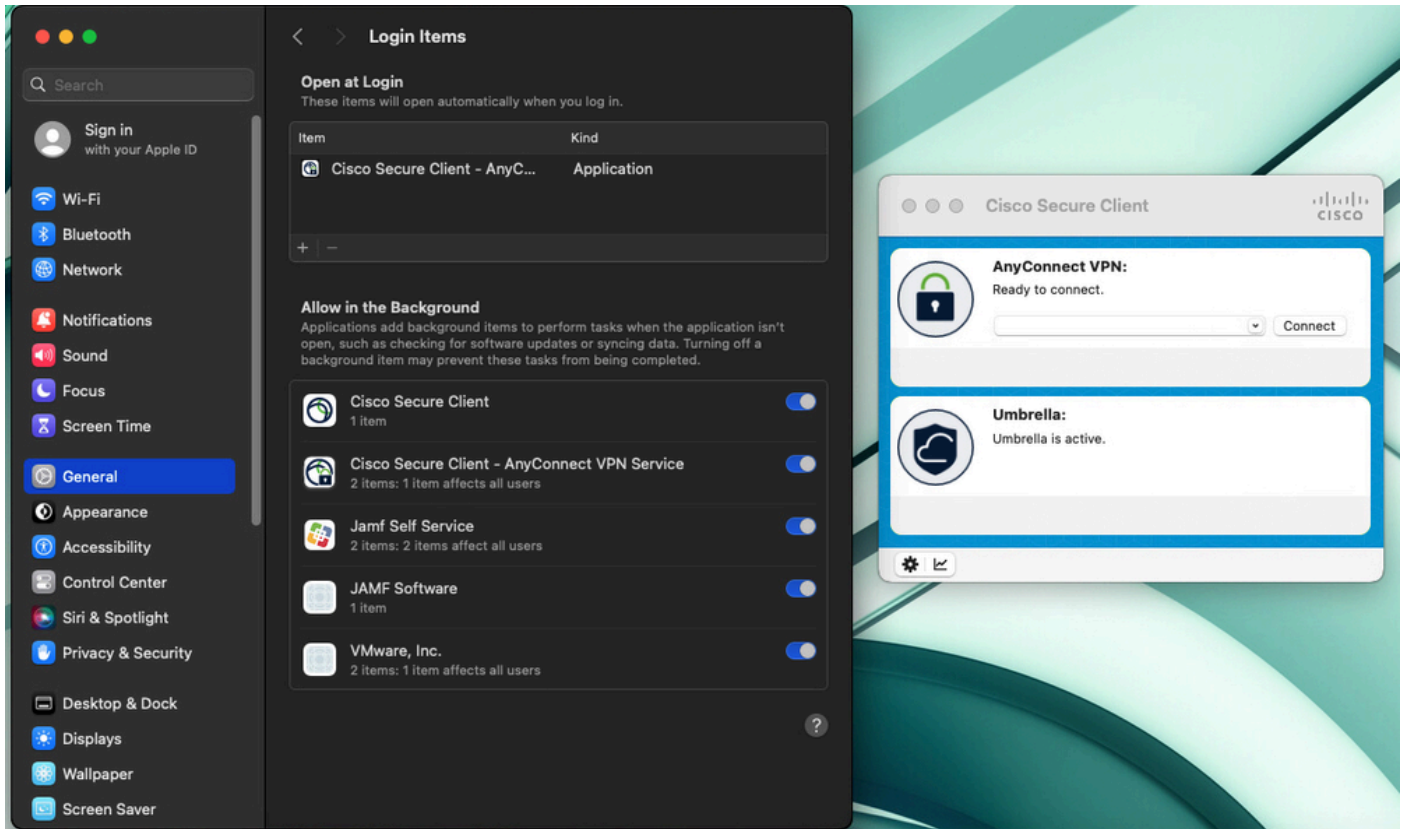
Suchen Sie zum Konfigurieren nach verwalteten Anmeldeelementen, und konfigurieren Sie die Felder mit folgenden Werten:

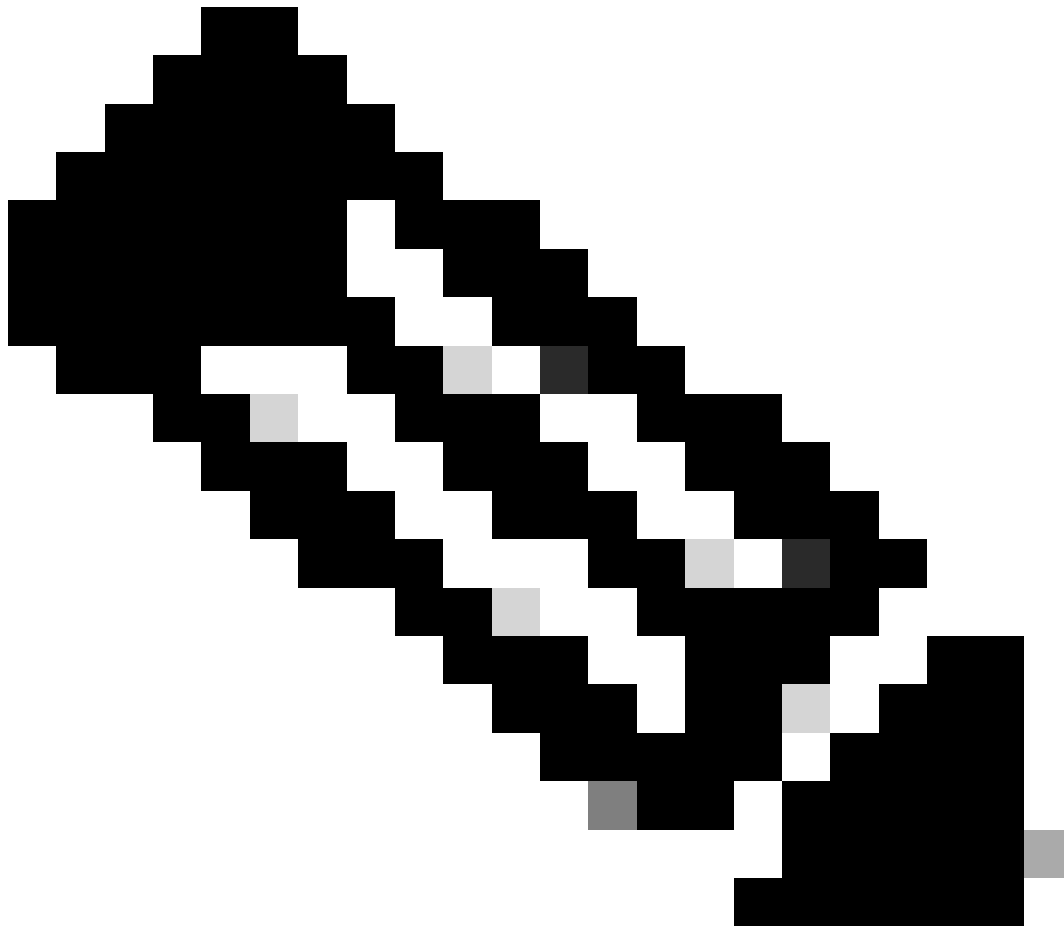
- Regeltyp: Paket-ID-Präfix
- Regelwert: com.cisco.secureclient
- Team-ID: DE8Y96K9QP

The screenshot shows the 'Cisco Secure Client' configuration page in the Jamf Pro console. The left sidebar contains a navigation menu with categories like 'Computers', 'Inventory', 'Content Management', 'Policies', 'Configuration Profiles', 'Software Updates', 'Restricted Software', 'Mac Apps', 'Patch Management', 'eBooks', 'Groups', and 'Smart Computer Groups'. The 'Configuration Profiles' section is expanded, showing 'Managed Login Items' with '1 setting configured'. The main content area is titled 'Managed Login Items' and includes a search bar, tabs for 'Options' and 'Scope', and a 'General' tab. The 'Managed Login Item rules' section is active, showing a table with columns for 'Rule type' and 'Rule value'. The 'Rule type' is set to 'Bundle Identifier Prefix' and the 'Rule value' is 'com.cisco.secureclient'. Below this, the 'Team identifier' is 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', and '+ Add'.

Zuweisung von Umfang und Push-Bereitstellung

1. Navigieren Sie zu Bereich, und definieren Sie den Bereich für Geräte oder Benutzer.
2. Das Modul "Cisco Secure Client mit Umbrella" kann auf die gewünschten MacOS-Geräte ausgelagert werden, wenn einer der Trigger, die Sie in Schritt 2 von "Erstellen einer JAMF-Richtlinie" konfiguriert haben, aktiviert ist. Alternativ können Sie dies auch über das [JAMF Self Service Portal](#) bereitstellen.





Anmerkung: Selbst wenn ein Benutzer versucht, den DNS-Proxy oder transparenten Proxy in den Systemeinstellungen (Netzwerk > Filter) zu deaktivieren, wird er standardmäßig wieder aktiviert, da der Content-Filter wie in diesem Artikel beschrieben über JAMF aktiviert ist und nicht deaktiviert werden kann.

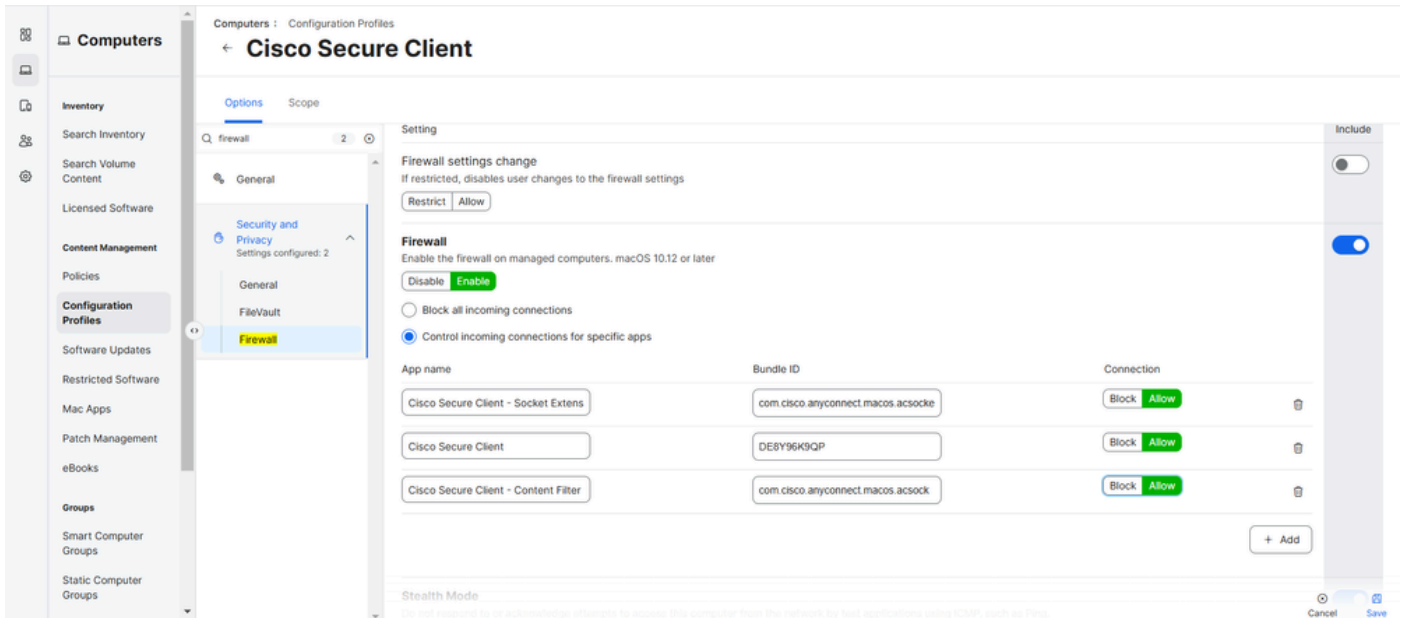
macOS-Firewallausnahme konfigurieren

Wenn die macOS-Firewall auf [Alle eingehenden Verbindungen blockieren](#) eingestellt ist, müssen Sie auch den Cisco Secure Client und seine Komponenten zur Ausnahmeliste hinzufügen:

1. Navigieren Sie zu Computer > Inhaltsverwaltung > Konfigurationsprofile.
2. Wählen Sie Ihr Cisco Secure Client-Konfigurationsprofil aus, und suchen Sie nach Security and Privacy.
3. Konfigurieren Sie es mit den folgenden Einstellungen:

- Firewall: Aktivieren - Steuerung eingehender Verbindungen für bestimmte Anwendungen

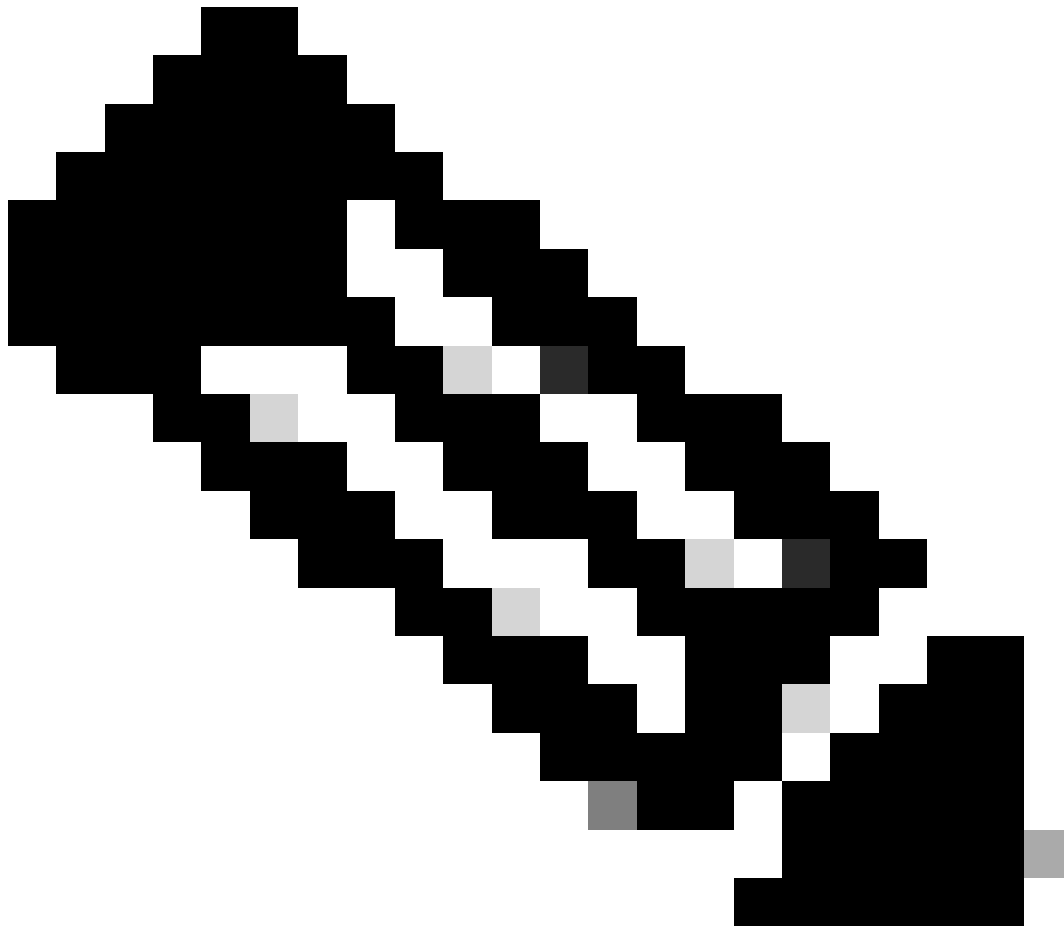
Anwendungsname	Paket-ID
Cisco Secure Client - Socket-Erweiterungen	com.cisco.anyconnect.macos.acsockext
Cisco Secure Client	DE8Y96K9QP
Cisco Secure Client - Content-Filter	com.cisco.anyconnect.macos.acsock



4. Wählen Sie Speichern.

5. Wenn Sie nach den Weiterverteilungsoptionen gefragt werden, wählen Sie An alle verteilen, um die Änderungen sofort an die gewünschten macOS-Geräte weiterzuleiten.

Bereitstellung des Cisco Umbrella Root-Zertifikats

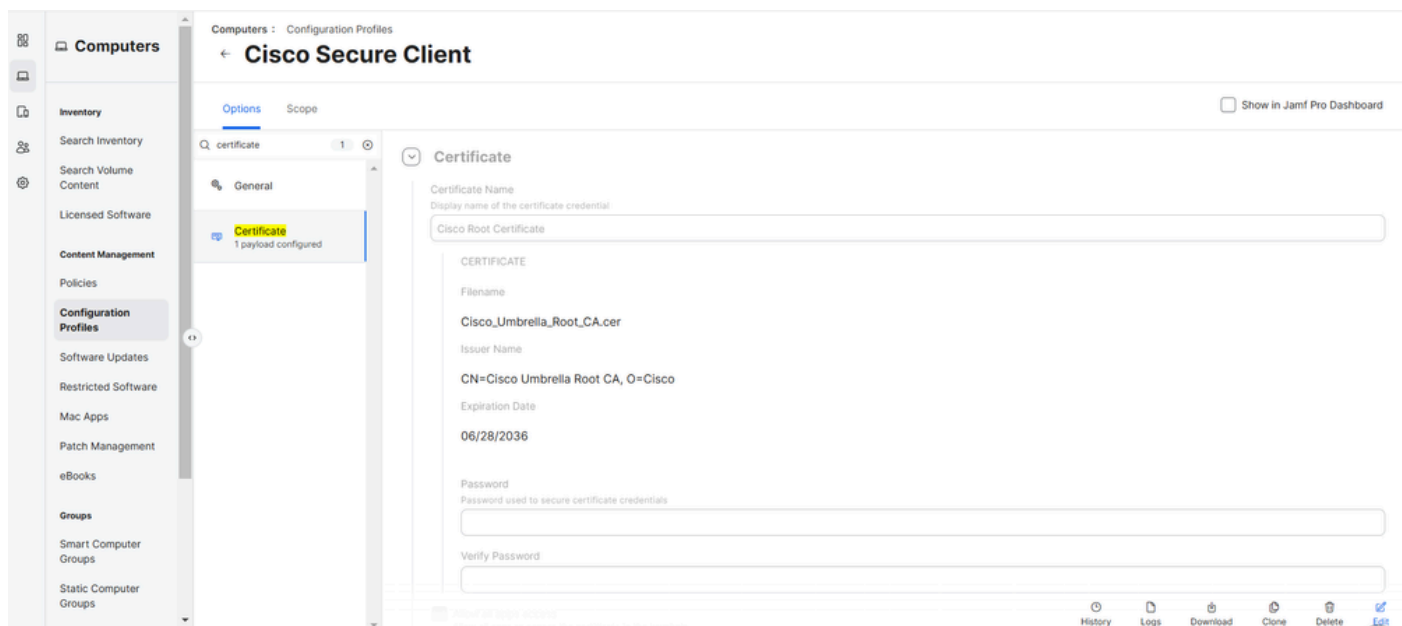


Anmerkung: Dieser Schritt gilt nur für neue Bereitstellungen von Cisco Secure Client oder Geräten, auf denen zuvor kein Cisco Umbrella Root Certificate bereitgestellt wurde. Wenn Sie vom Umbrella Roaming Client oder vom Cisco AnyConnect 4.10 Client migrieren und/oder das Cisco Umbrella Root Certificate bereits in der Vergangenheit bereitgestellt haben, können Sie diesen Abschnitt überspringen.

Laden Sie das Cisco Umbrella Root-Zertifikat von Policies > Root Certificate in das Umbrella Dashboard herunter.

1. Laden Sie im Umbrella Dashboard unter Policies > Root Certificate das Cisco Umbrella Root Certificate herunter.
2. Navigieren Sie in JAMF zu Computer > Configuration Profiles > Cisco Secure Client > Edit.
3. Suchen Sie nach Zertifikat > Konfigurieren. Geben Sie ihm einen eindeutigen Namen.
4. Wählen Sie unter Select Certificate Option die Option Upload and upload the Cisco Umbrella Root Certificate, das Sie zuvor in Schritt 1 heruntergeladen haben.

5. Stellen Sie sicher, dass Sie hier kein Kennwort konfigurieren, und wählen Sie Speichern.



6. Wenn Sie nach den Weiterverteilungsoptionen gefragt werden, wählen Sie An alle verteilen, um die Änderungen sofort an die gewünschten macOS-Geräte weiterzuleiten.

Verifizierung

Um zu überprüfen, ob das Modul "Cisco Secure Client mit Umbrella" funktioniert, rufen Sie <https://policy-debug.checkumbrella.com> auf, oder führen Sie den folgenden Befehl aus:

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

Beide Ausgaben müssen eindeutige und relevante Informationen für Ihre Umbrella-Organisation enthalten, z. B. Ihre OrgID.

Problemumgehung für macOS 14.3

Für macOS 14.3 (oder höher) mit Cisco Secure Client 5.1.x, wenn Sie "Der VPN-Client-Agent konnte das Interprocess Communication Depot nicht erstellen" feststellen:

1. Navigieren Sie in JAMF zu Einstellungen > Computerverwaltung > Skripte > Neu.
2. Geben Sie ihm einen eindeutigen Namen und definieren Sie Ihre Kategorie.
3. Navigieren Sie zur Registerkarte Skript, und fügen Sie Folgendes hinzu:

```
#!/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. Stellen Sie unter Optionen sicher, dass die Priorität auf Nachher festgelegt ist. Dieses Bash-Skript überprüft, ob Cisco Secure Client - AnyConnect VPN service.app ausgeführt wird. Hierzu wird eine erwartete Ausgabe mit der Prozess-ID von `pgrep -fl` zurückgegeben.

- Wenn eine leere Ausgabe zurückgegeben wird, können Sie bestätigen, dass der Cisco Secure Client - AnyConnect VPN-Dienst nicht ausgeführt wird und das Skript zum Starten der Cisco Secure Client-Kerndienste ausgeführt wird, die erforderlich sind, damit das Umbrella-Modul ordnungsgemäß ausgeführt wird.

Automatische Updates

Cisco hat beschlossen, die [automatische Update-Unterstützung](#) vom Umbrella Dashboard auf Secure Client ab Secure Client 5.1.6.103 (MR6) zu erweitern. Für die Zukunft können Kunden, die mindestens auf Cisco Secure Client 5.1.6 MR6 aktualisiert haben, automatisch auf neuere Versionen aktualisieren, wenn im Umbrella Dashboard eine automatische Aktualisierung konfiguriert wurde.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.