Distribuire CSC in macOS utilizzando JAMF con Umbrella Module

Sommario

Introduzione

In questo documento viene descritto come distribuire Cisco Secure Client con il modulo Umbrella ai dispositivi macOS gestiti tramite JAMF.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

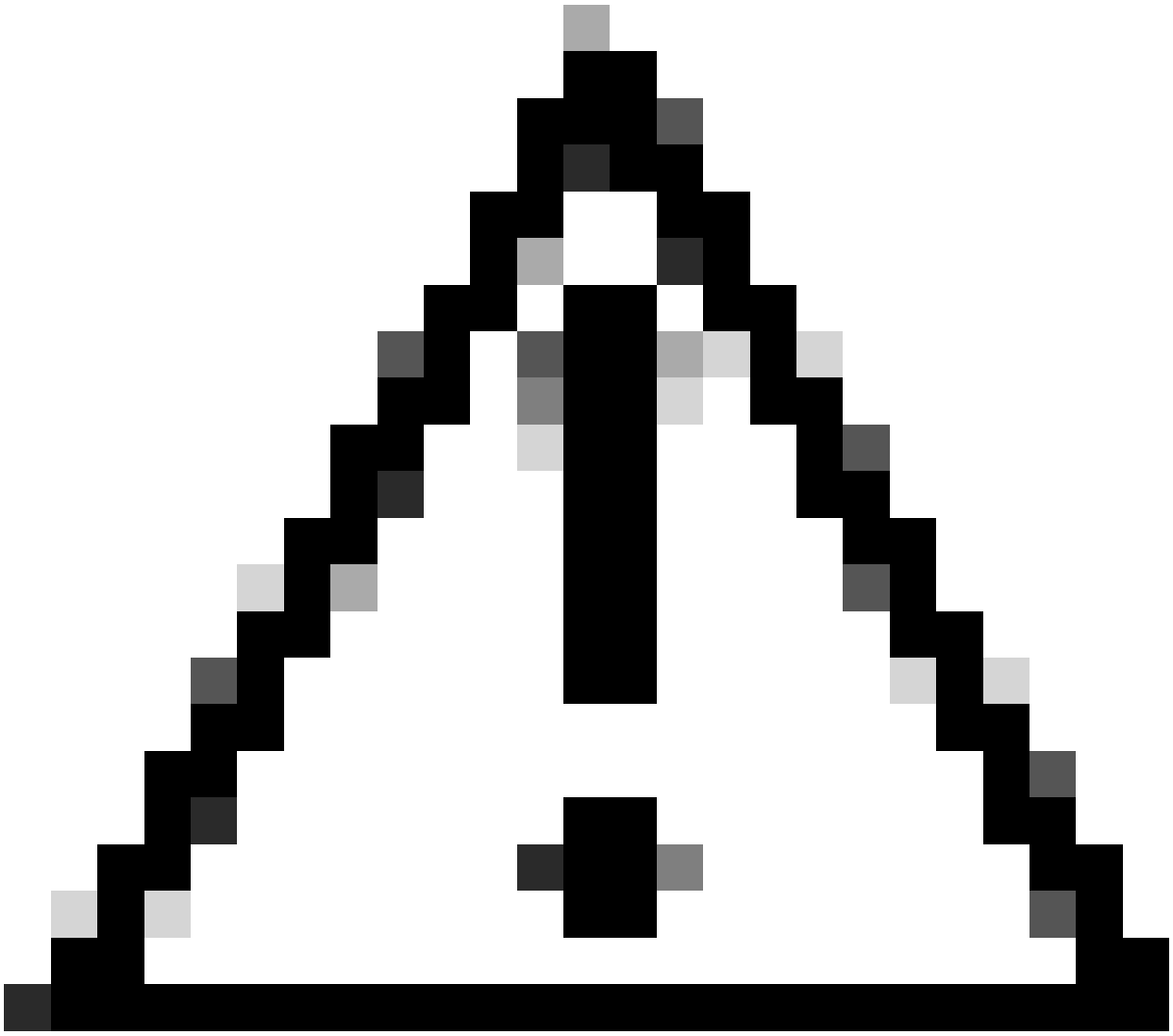
- I dispositivi macOS devono essere gestiti da JAMF.
- Per le istruzioni di registrazione MDM per macOS, consultare la documentazione di JAMF.

Componenti usati

Le informazioni fornite in questo documento si basano su Cisco Secure Client.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata

ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.



Attenzione: Questo articolo viene fornito così com'è il 1 febbraio 2025. Cisco Umbrella Support non garantisce che le presenti istruzioni siano valide dopo questa data e siano soggette a modifica in base agli aggiornamenti di JAMF e Apple.

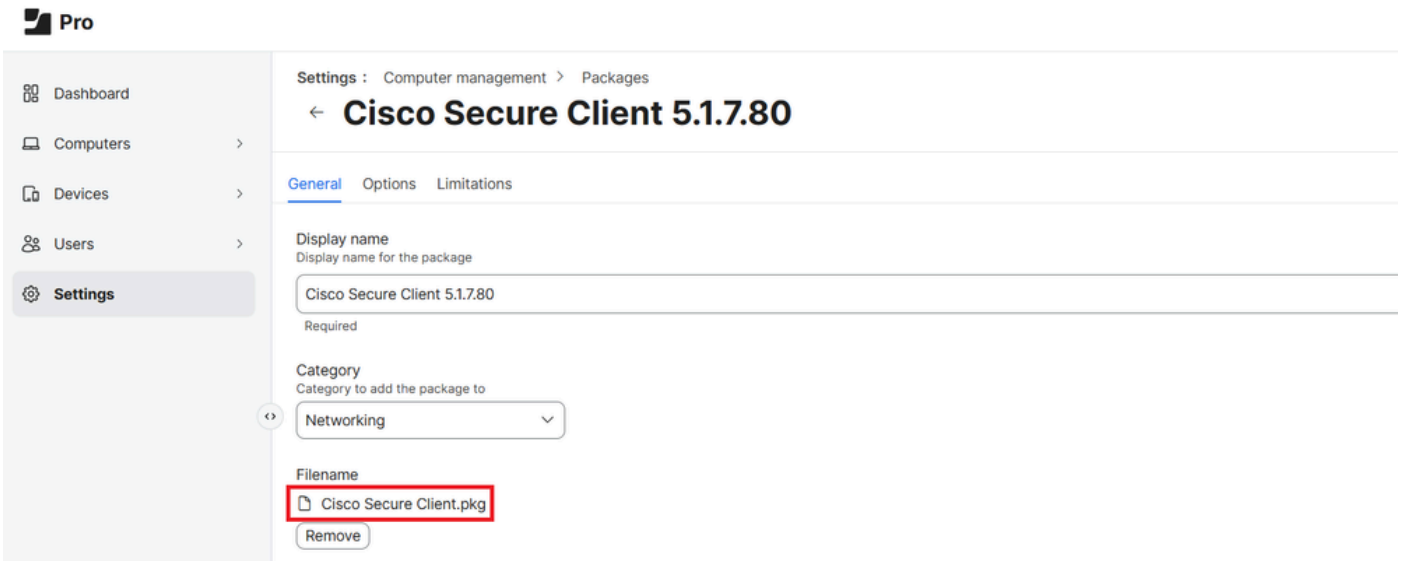
Caricare il pacchetto di installazione (PKG)

1. Scaricare Cisco Secure Client DMG dal dashboard Umbrella in Distribuzioni > Computer mobili > Client mobile > Pacchetto pre-distribuzione > macOS.

2. Accedere all'istanza del cloud JAMF Pro.

3. Passare a Impostazioni > Gestione computer > Pacchetti > Nuovo.

4. Caricare il PKG estratto dal pacchetto DMG scaricato dal dashboard Umbrella.

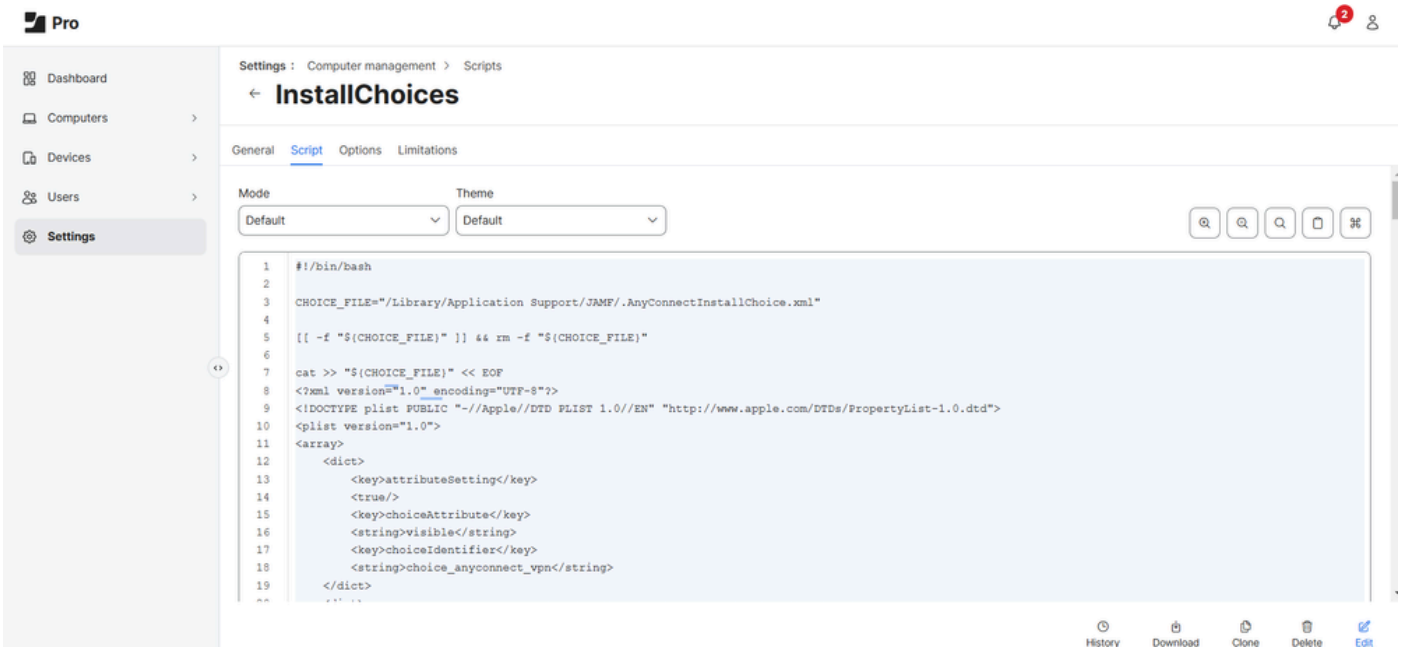


Aggiungi script di configurazione e selezione modulo

1. Selezionare Impostazioni > Gestione computer > Script e aggiungere questo script per controllare quali moduli vengono installati durante la distribuzione.

2. È possibile controllare l'installazione dei moduli Secure Client impostando un modulo su 0 per ignorarlo o su 1 per installarlo, in quanto PKG è configurato per installare tutti i moduli per impostazione predefinita.

- È possibile ottenere il file XML di esempio dalla documentazione di Umbrella: [Customize macOS installation of Cisco Secure Client]
- Umbrella ha anche aggiunto lo script "installchoice" a questo [collegamento github.] In questo esempio, i moduli Core VPN, Umbrella e DART sono impostati su 1 e possono essere inclusi nell'installazione Secure Client.



3. Passare a Impostazioni > Gestione computer> Script e aggiungere questo script in modo che crei un file di configurazione `Orginfo.json` richiesto da Cisco Secure Client.

- Scaricare il profilo del modulo direttamente dal dashboard Umbrella, quindi aggiungere ID organizzazione, impronta digitale e ID utente allo script:

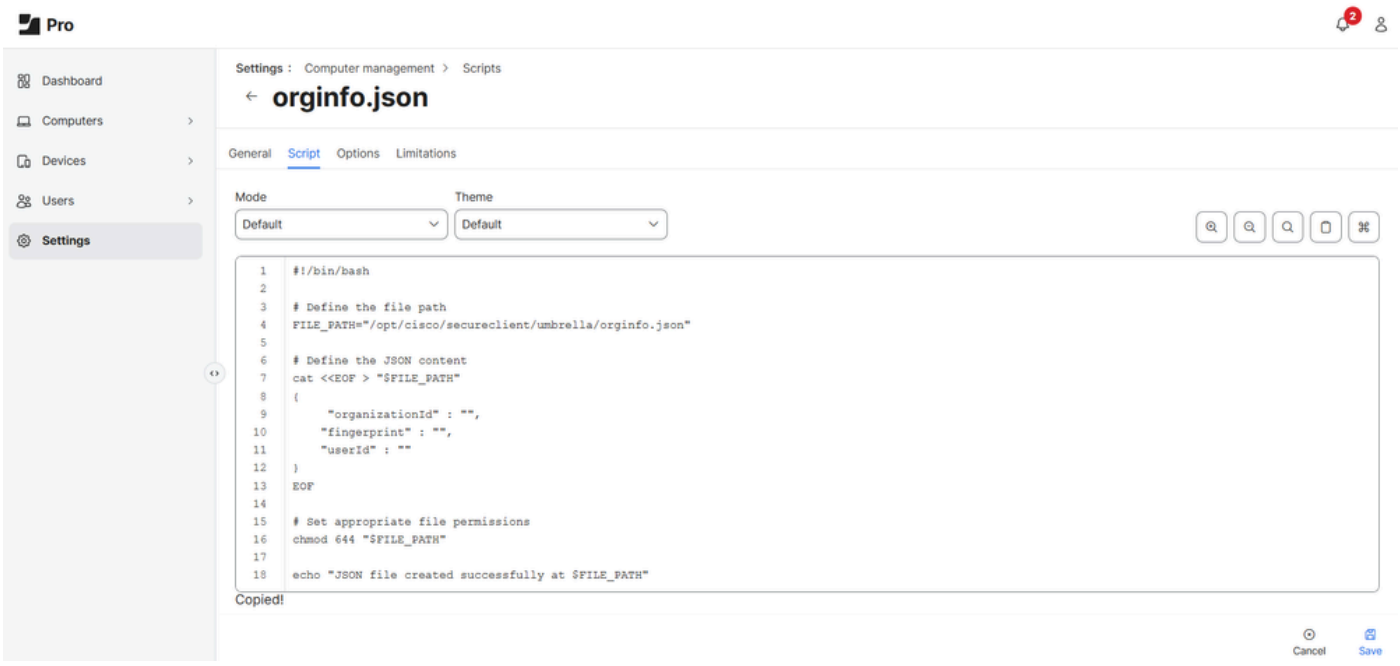
```
#!/bin/bash

# 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

Creare il criterio JAMF

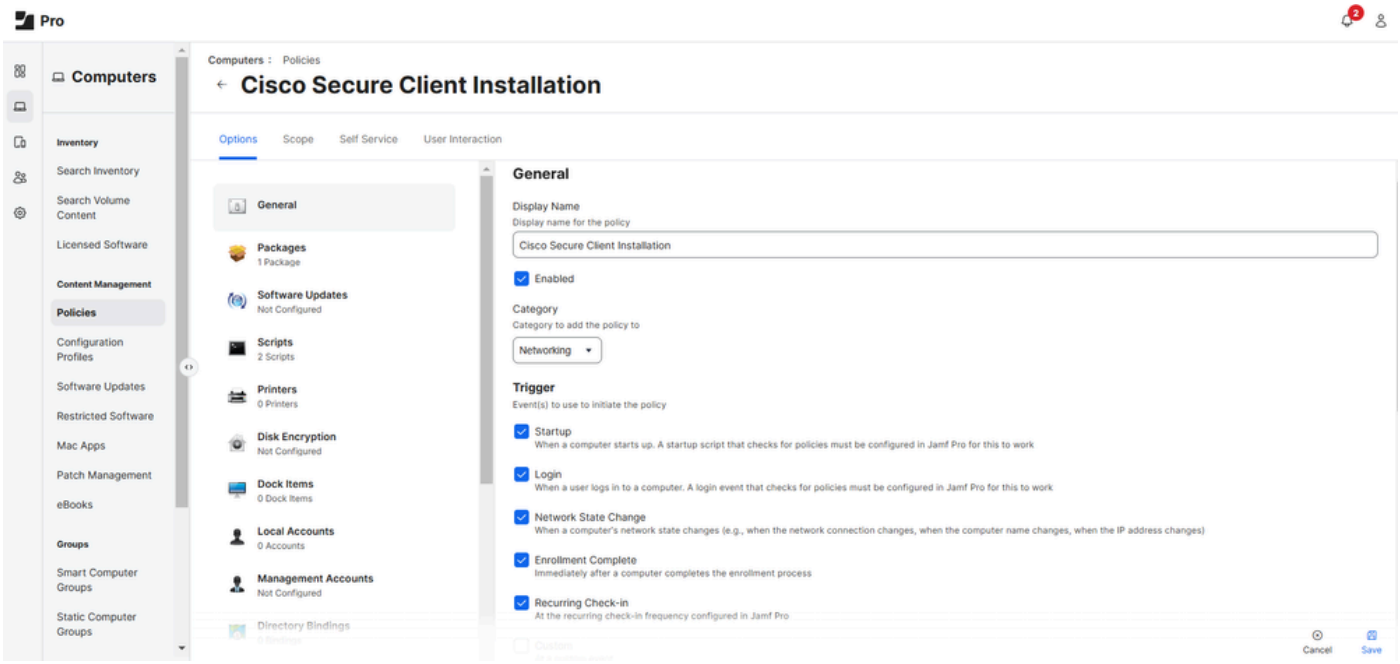
I criteri JAMF vengono utilizzati per determinare come e quando estrarre il modulo Cisco Secure Client con Umbrella.

1. Passare a Computer > Gestione contenuto > Criteri > Nuovo.

2. Assegnare un nome univoco al criterio e selezionare gli eventi categoria e trigger desiderati (ad esempio, quando viene eseguito il criterio).

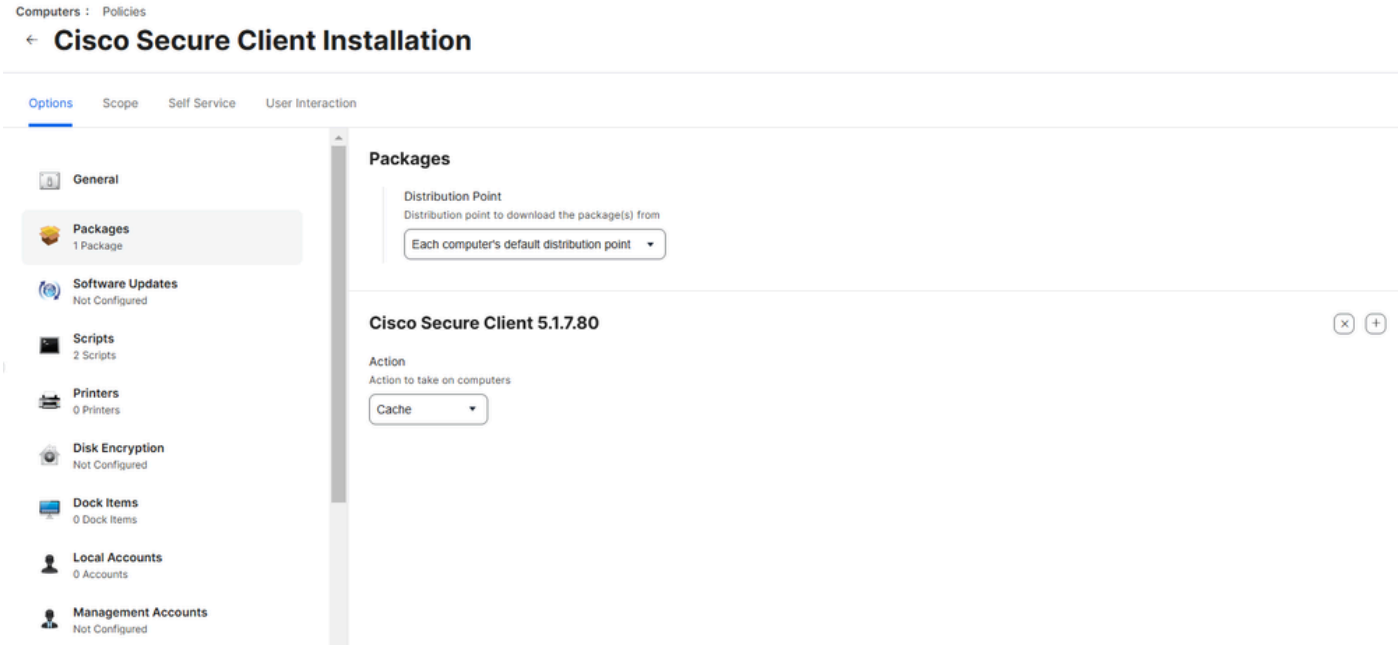
3. Facoltativamente, è possibile anche configurare un comando personalizzato che può essere eseguito in Personalizzato. Il comando per l'esecuzione e l'esecuzione del criterio è simile al seguente:

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

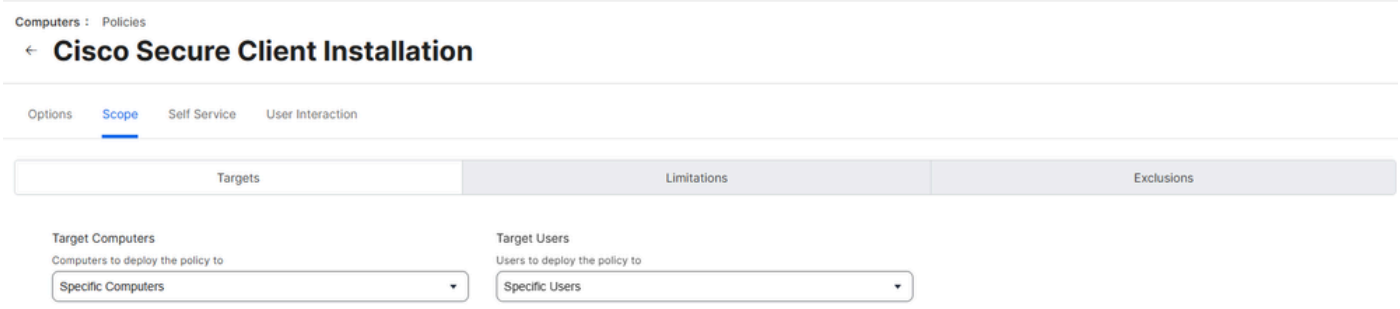


4. Selezionare Packages > Configure, quindi selezionare Add accanto al package Cisco Secure Client.

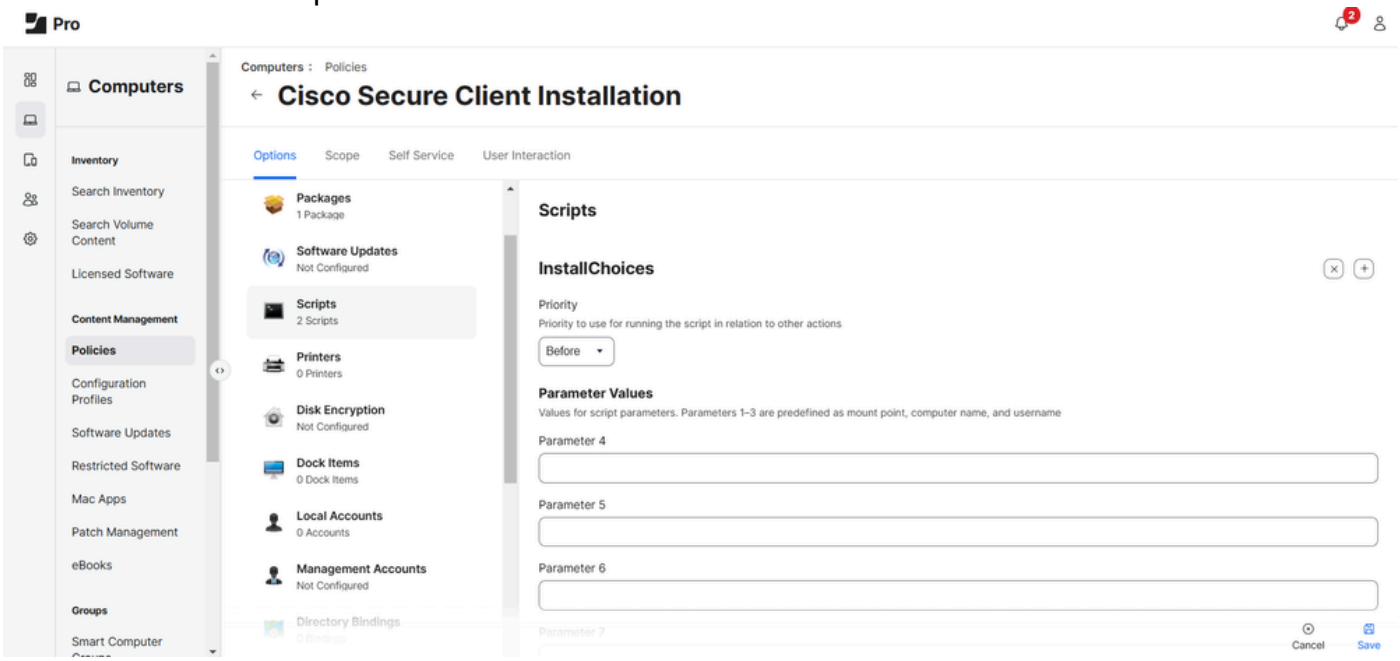
- In Punto di distribuzione, selezionare Il punto di distribuzione predefinito di ogni computer.
- In Azione, selezionare Cache.

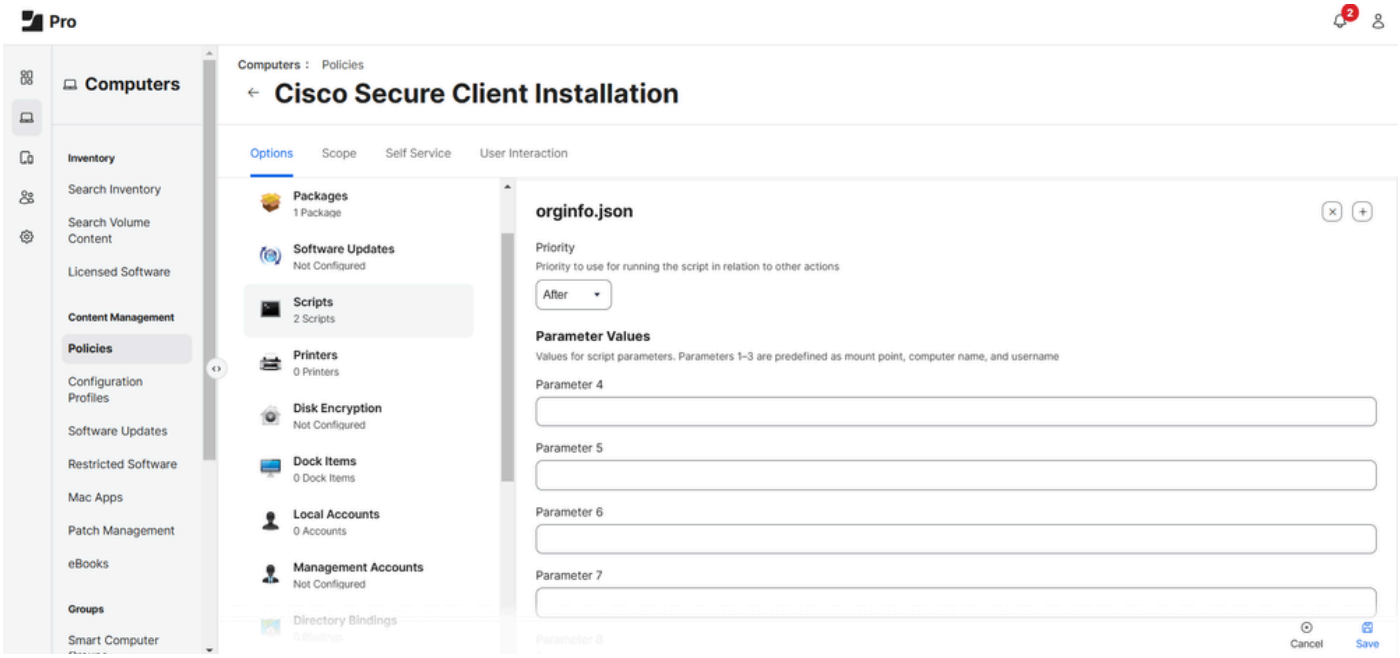


5. Definire l'ambito dei dispositivi o degli utenti per la distribuzione e selezionare Salva.



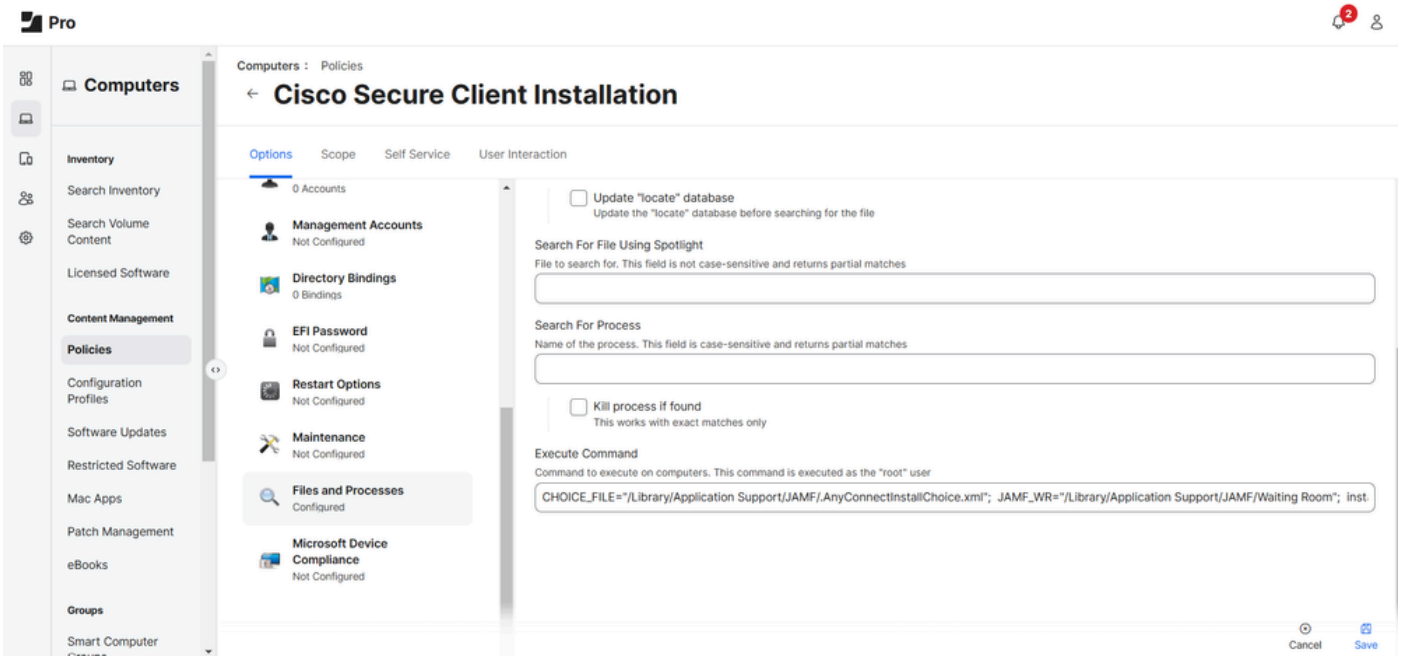
6. Aggiungere gli scriptInstallChoicese **orginfo.json** e assegnargli una priorità da utilizzare per l'esecuzione dello script in relazione ad altre azioni.





7. Eseguire questo comando per installare il pacchetto Cisco Secure Client con i moduli selezionati sui dispositivi:

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



Configurare un'installazione invisibile all'utente dell'estensione di sistema

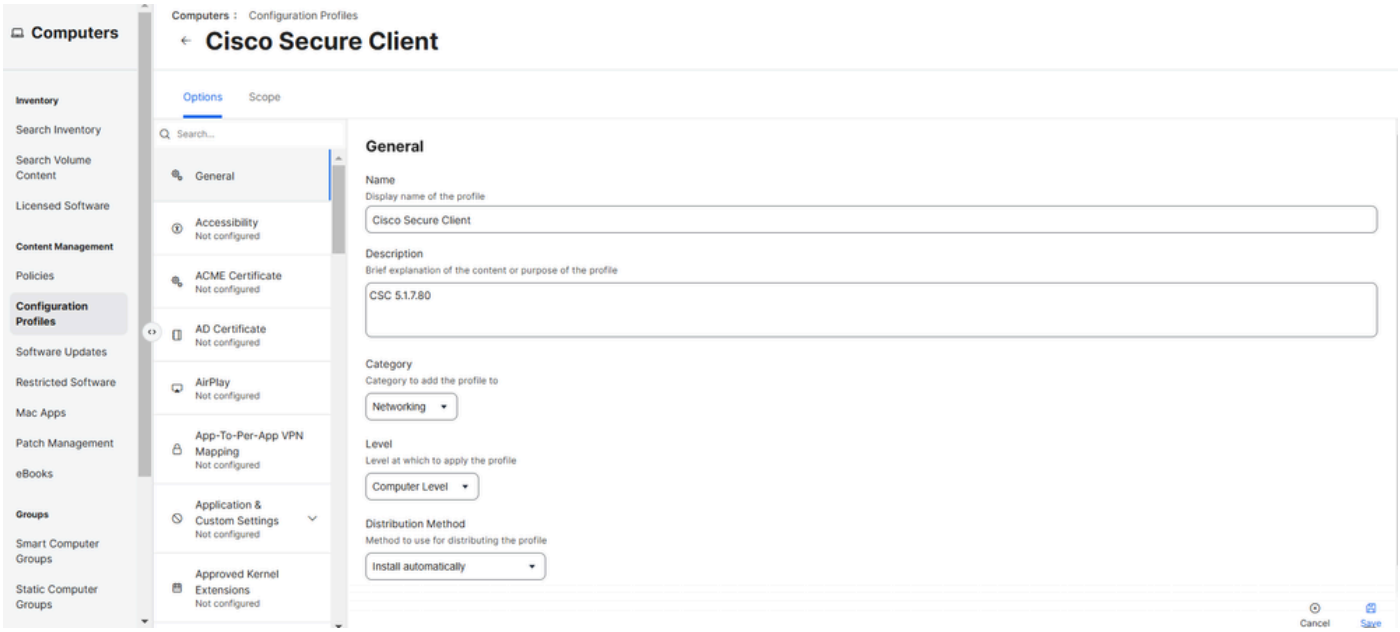
Quindi, usare JAMF per configurare e consentire le estensioni di sistema richieste di Cisco Secure

Client in modo che Cisco Secure Client con modulo Umbrella venga eseguito correttamente senza interazioni con l'utente.

1. Selezionare Computer > Gestione contenuto > Profili di configurazione > Nuovo.

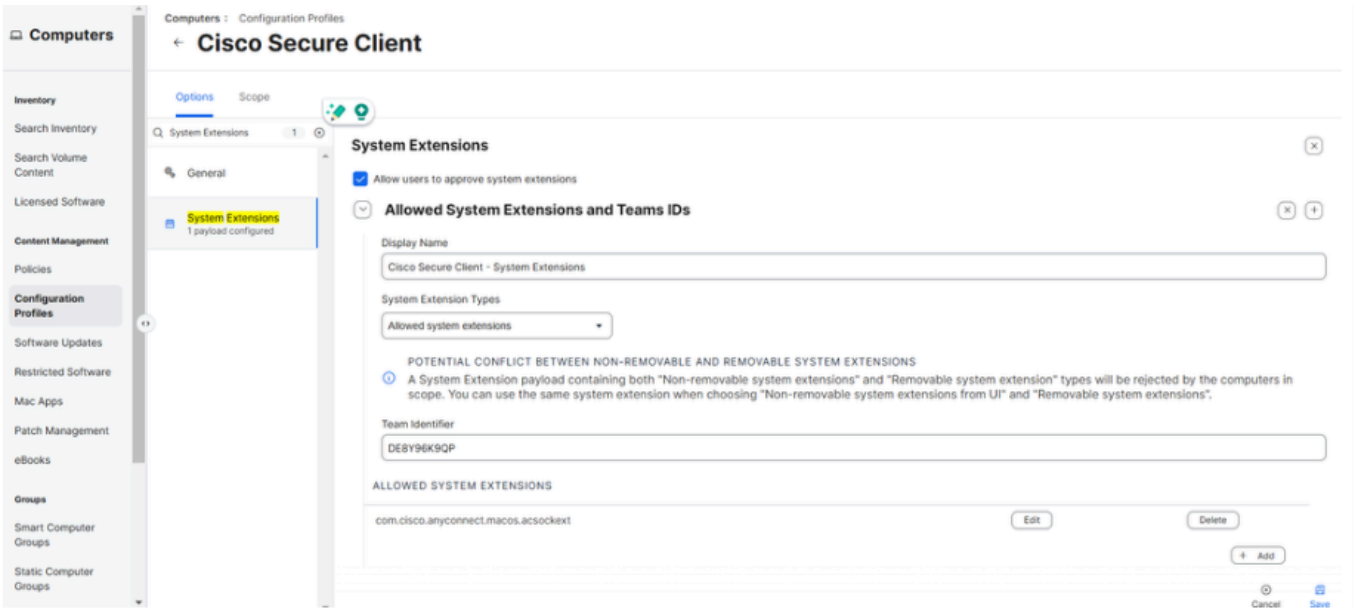
2. Assegnare al profilo un nome univoco e selezionare la categoria e il metodo di distribuzione.

3. EnsureLevel è impostato su Computer Level.



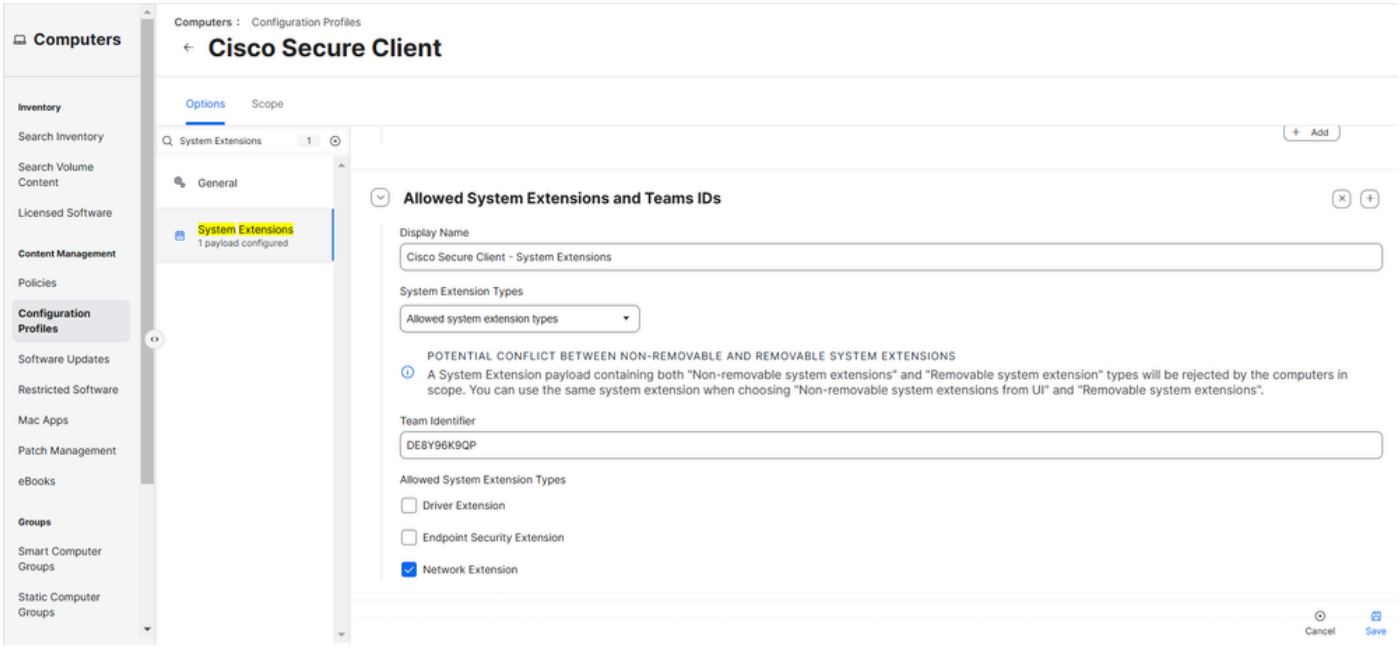
4. Cercare Estensioni di sistema > Configura. Immettere i seguenti valori:

- Nome visualizzato: Cisco Secure Client - Estensioni di sistema
- Tipi di estensione di sistema: Estensioni di sistema consentite
- Identificatore team: DE8Y96K9QP
- Estensioni di sistema consentite: com.cisco.anyconnect.macos.acsockext, quindi selezionare Save (Salva).



5. Selezionare l'icona + accanto a ID team autorizzati ed estensioni di sistema per aggiungere un'altra estensione di sistema. Immettere quindi i valori seguenti:

- Nome visualizzato: Cisco Secure Client - Estensioni di sistema
- Tipi di estensione di sistema: Consenti tipi di estensione di sistema
- Identificatore team: DE8Y96K9QP
- Consenti tipi di estensione di sistema: Estensione di rete

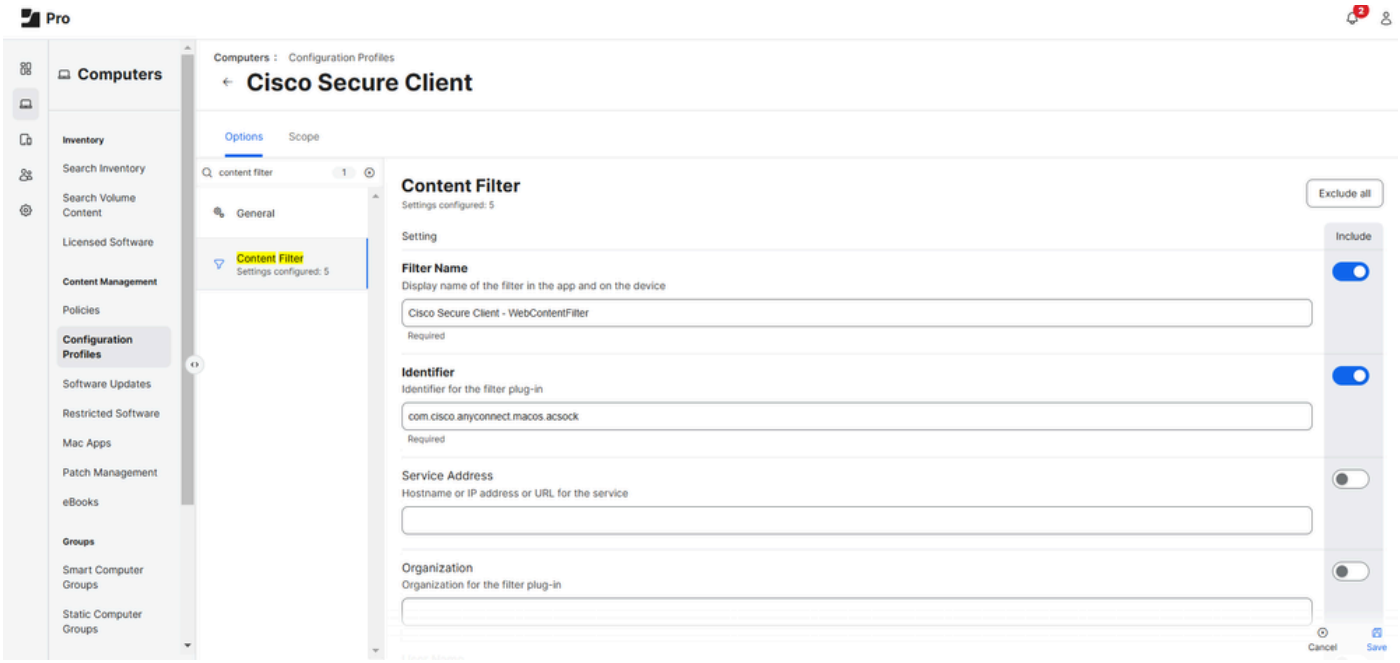


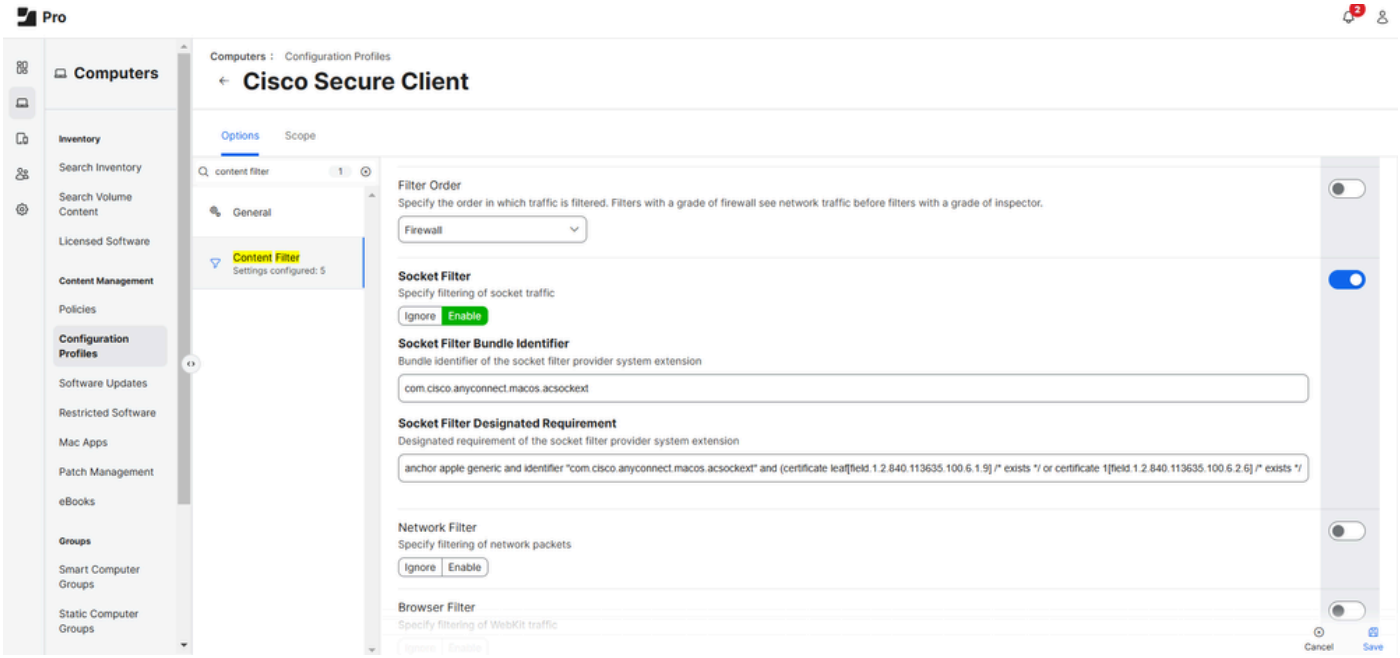
Configura installazione invisibile all'utente per filtro contenuto

Configurare quindi un'installazione invisibile all'utente per il filtro contenuti, correlato al Cisco Secure Client con il filtro socket del modulo Umbrella:

1. Cercare Filtro contenuti. Abilitare e completare questi campi con i rispettivi valori:

- Nome filtro: Cisco Secure Client - FiltroContenutiWeb
- Identificativo: com.cisco.anyconnect.macos.acsock
- Filtro socket: Attivato
- Identificatore pacchetto filtro socket: com.cisco.anyconnect.macos.acsockext
- Requisito designato dal filtro socket:
  `l'identificatore generico "com.cisco.anyconnect.macos.acsockext" e (certificate leaf[field.1.2.840.113635.100.6.1.9] /* esiste */ o il certificato 1[field.1.2.840.113635.100.6.2.6] /* esiste */ e il certificato leaf[field.1.2.840.113635.100.6.1.13] /* esiste */ e certificate leaf[subject.OU] = DE8Y96K9QP)`





2. In Dati personalizzati, selezionare Aggiungi cinque volte e immettere i seguenti valori:

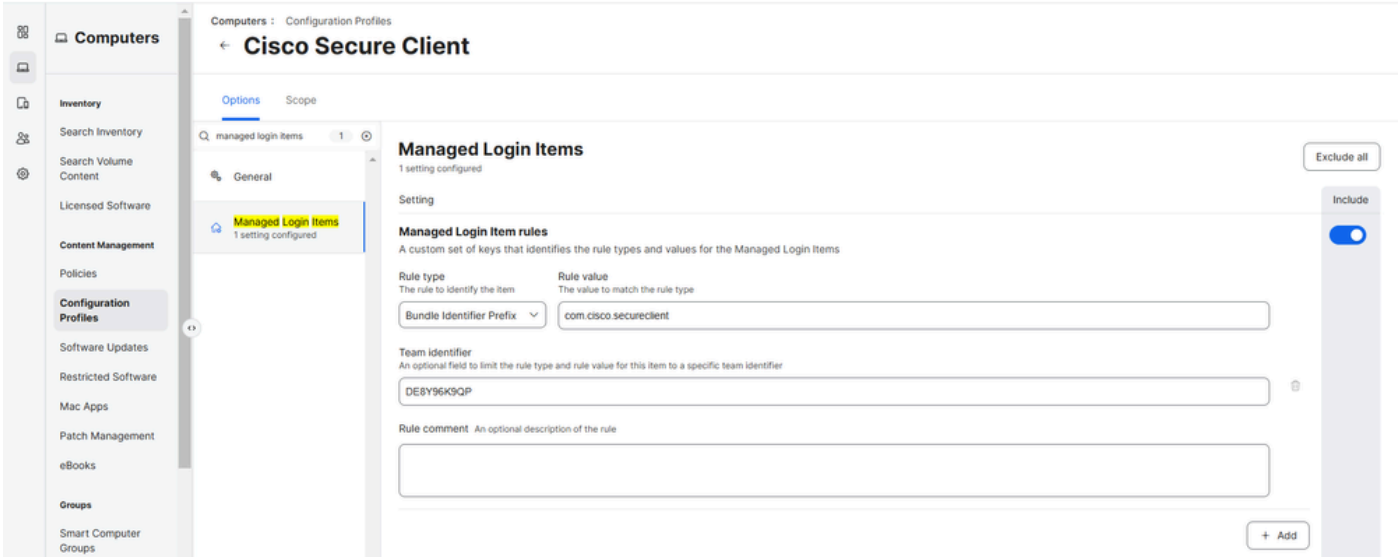
Chiave	Valore
Filtro automatico abilitato	falso
FiltraBrowser	falso
FiltraSocket	vero
FiltraPacchetti	falso
.LivelloFiltro	firewall

Configura elementi di login gestiti

La configurazione degli elementi di login gestiti per Cisco Secure Client con il modulo Umbrella garantisce che Cisco Secure Client venga avviato all'avvio del dispositivo.

Per configurare, cercare Elementi di login gestiti e configurare i campi con questi valori:

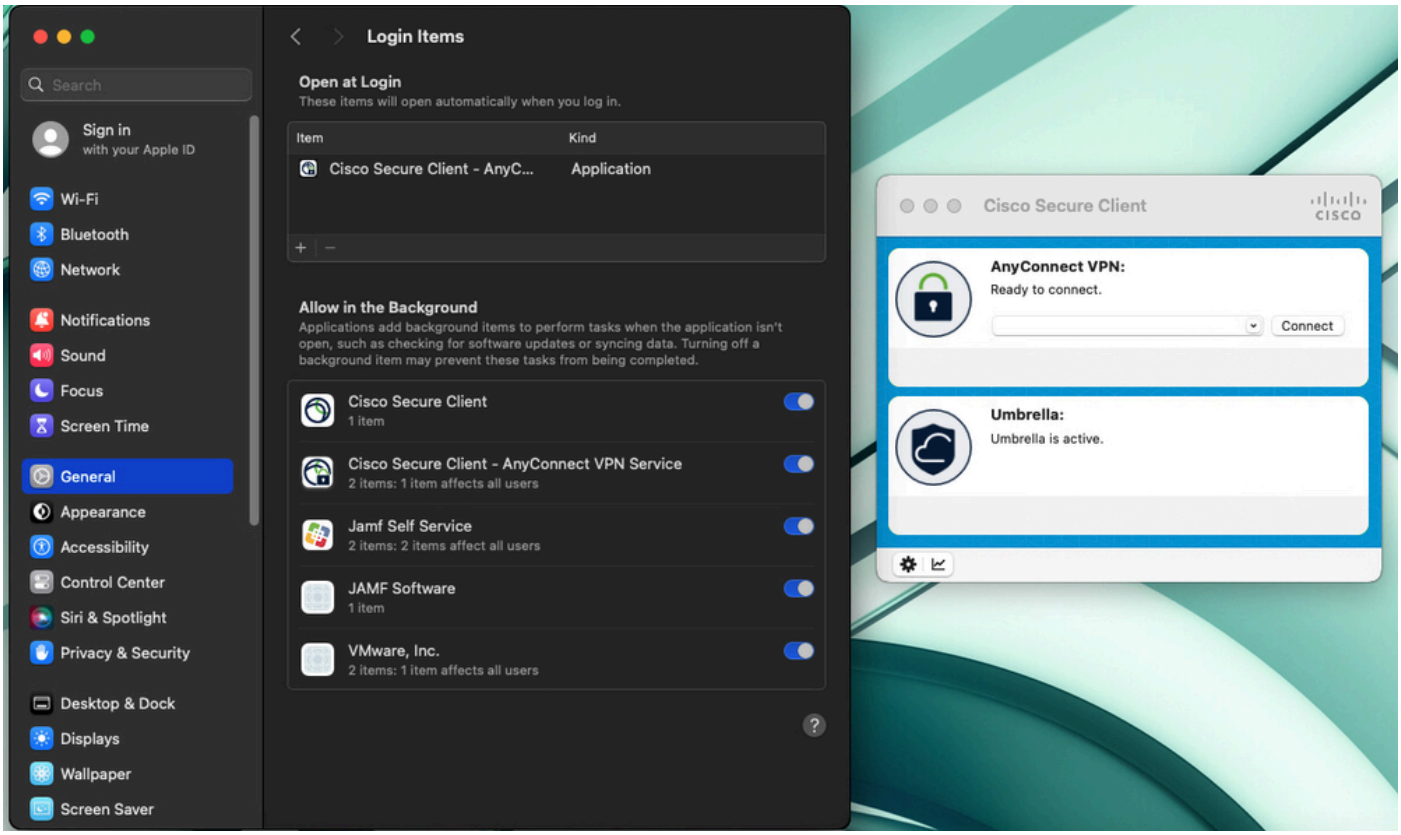
- Tipo di regola: Prefisso identificatore bundle
- Valore regola: com.cisco.secureclient
- Identificatore team: DE8Y96K9QP

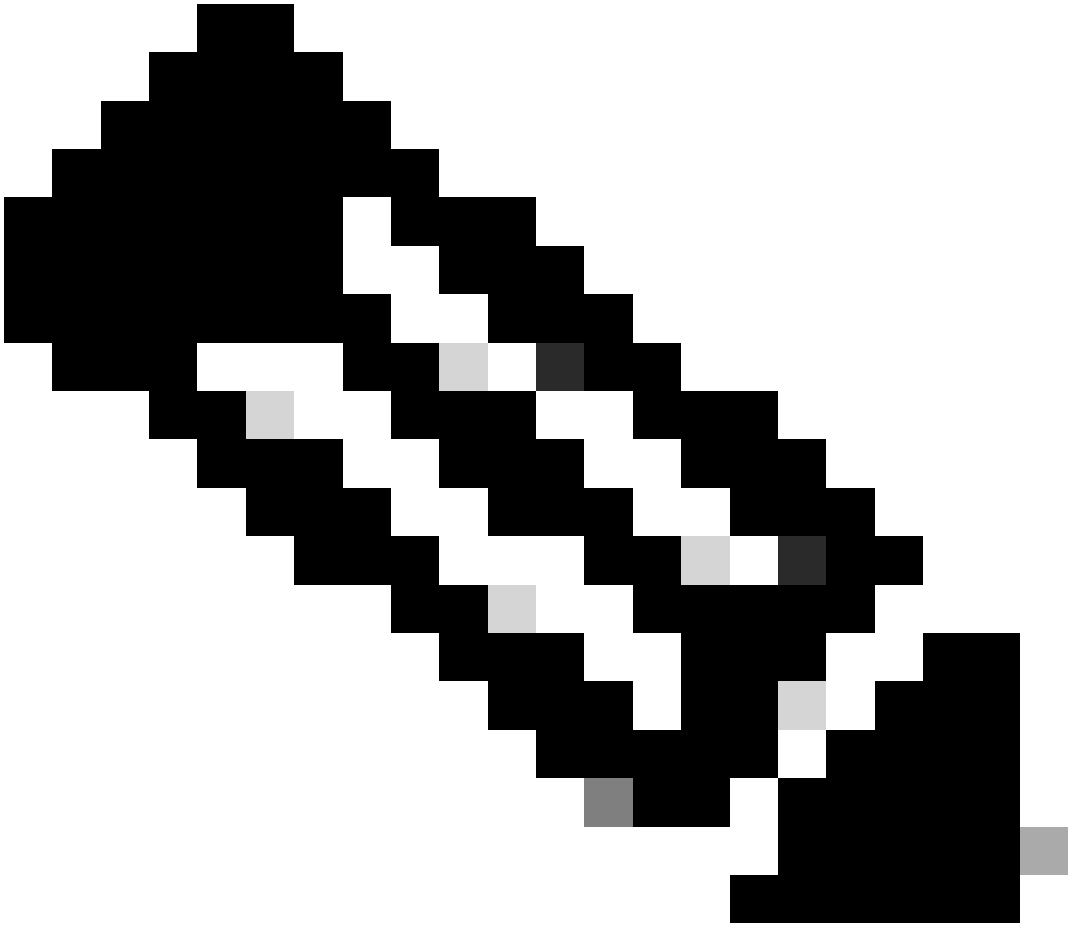


Assegna ambito e distribuzione push

1. Passare a Ambito e definire l'ambito per dispositivi o utenti.

2. È possibile eseguire il push di Cisco Secure Client con modulo Umbrella nei dispositivi macOS desiderati quando viene attivato uno dei trigger configurati nel passaggio 2 di Creazione di criteri JAMF. In alternativa, è possibile distribuire il file tramite il portale Self Service di 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.



Nota: Anche se un utente tenta di disabilitare il proxy DNS o il proxy trasparente in Impostazioni di sistema (Rete > Filtro), viene automaticamente riabilitato per impostazione predefinita poiché il filtro contenuti è abilitato tramite JAMF come descritto in questo articolo e non può essere disabilitato.

Configura eccezione firewall macOS

Se il firewall macOS è impostato su Blocca tutte le connessioni in ingresso, è necessario aggiungere anche il Cisco Secure Client e i relativi componenti all'elenco delle eccezioni:

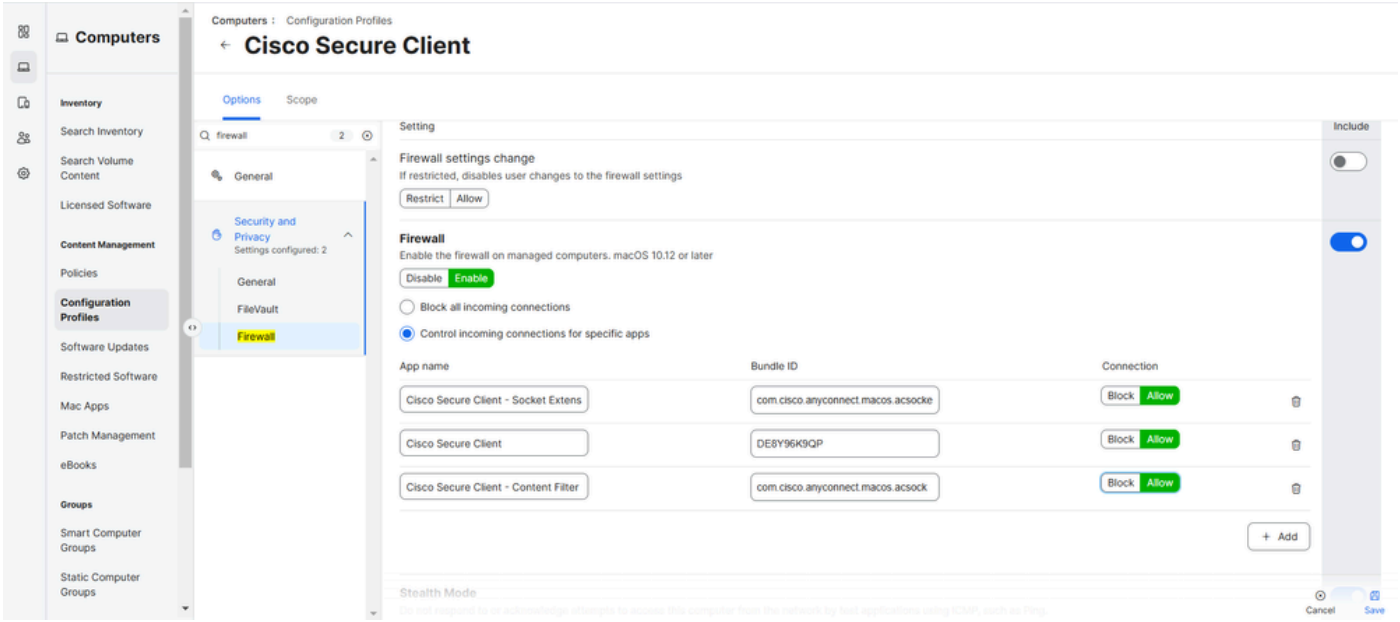
1. Passare a Computer > Gestione contenuto > Profili di configurazione.

2. Selezionare il profilo di configurazione di Cisco Secure Client e individuare Security and Privacy.

3. Configurarlo con queste impostazioni:

- Firewall: abilita - Controlla le connessioni in ingresso per app specifiche

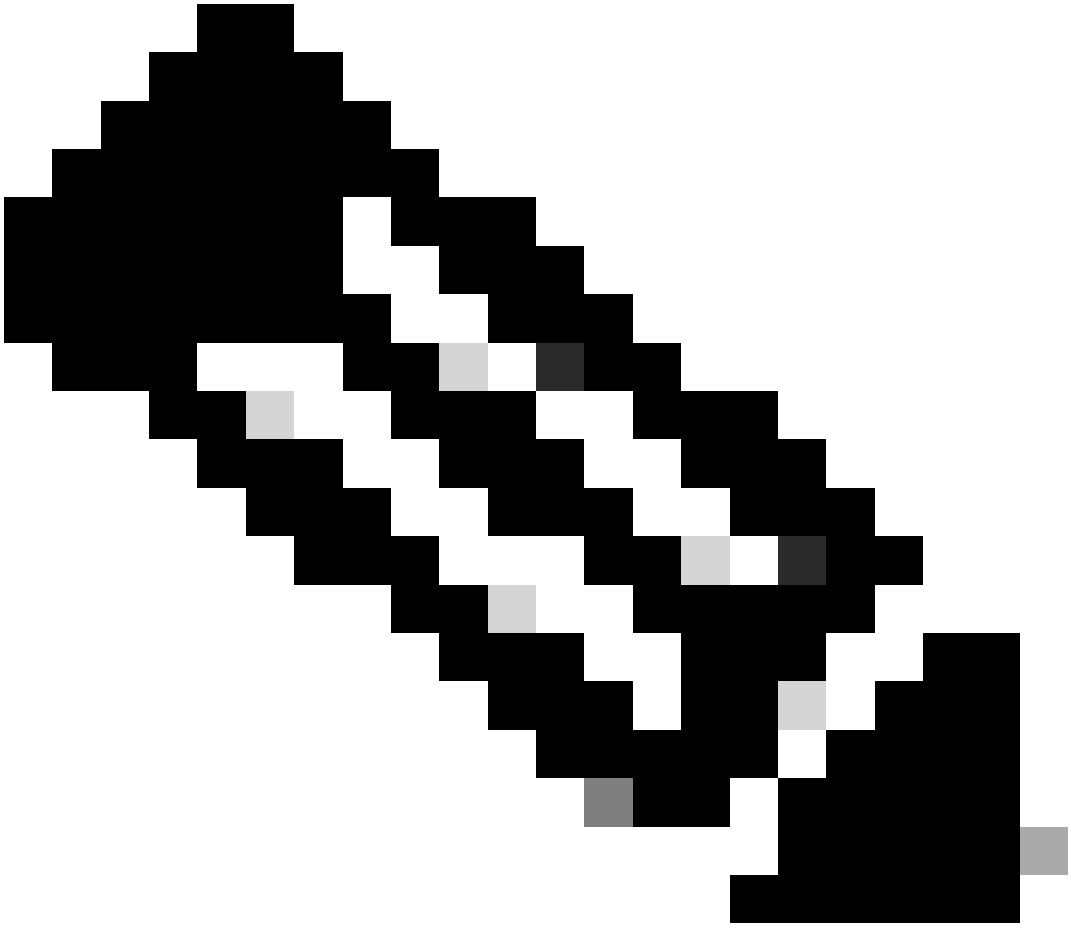
Nome app	ID bundle
Cisco Secure Client - Estensioni socket	com.cisco.anyconnect.macos.acsockext
Cisco Secure Client	DE8Y96K9QP
Cisco Secure Client - Filtro contenuti	com.cisco.anyconnect.macos.acsock



4. Selezionare Salva.

5. Se viene visualizzato il messaggio Redistribution Options (Opzioni di ridistribuzione), selezionare Distribute to All (Distribuisci su tutti) per annullare immediatamente le modifiche apportate ai dispositivi macOS desiderati.

Distribuire il certificato radice Cisco Umbrella



Nota: Questo passaggio è valido solo per le nuove distribuzioni di Cisco Secure Client o dei dispositivi per i quali non è stato precedentemente distribuito il certificato radice Cisco Umbrella. Se si sta eseguendo la migrazione dal client Umbrella Roaming o dal client Cisco AnyConnect 4.10 e/o il certificato radice Cisco Umbrella è già stato distribuito in passato, è possibile ignorare questa sezione.

Scaricare il certificato radice Cisco Umbrella da Criteri > Certificato radice nel dashboard Umbrella.

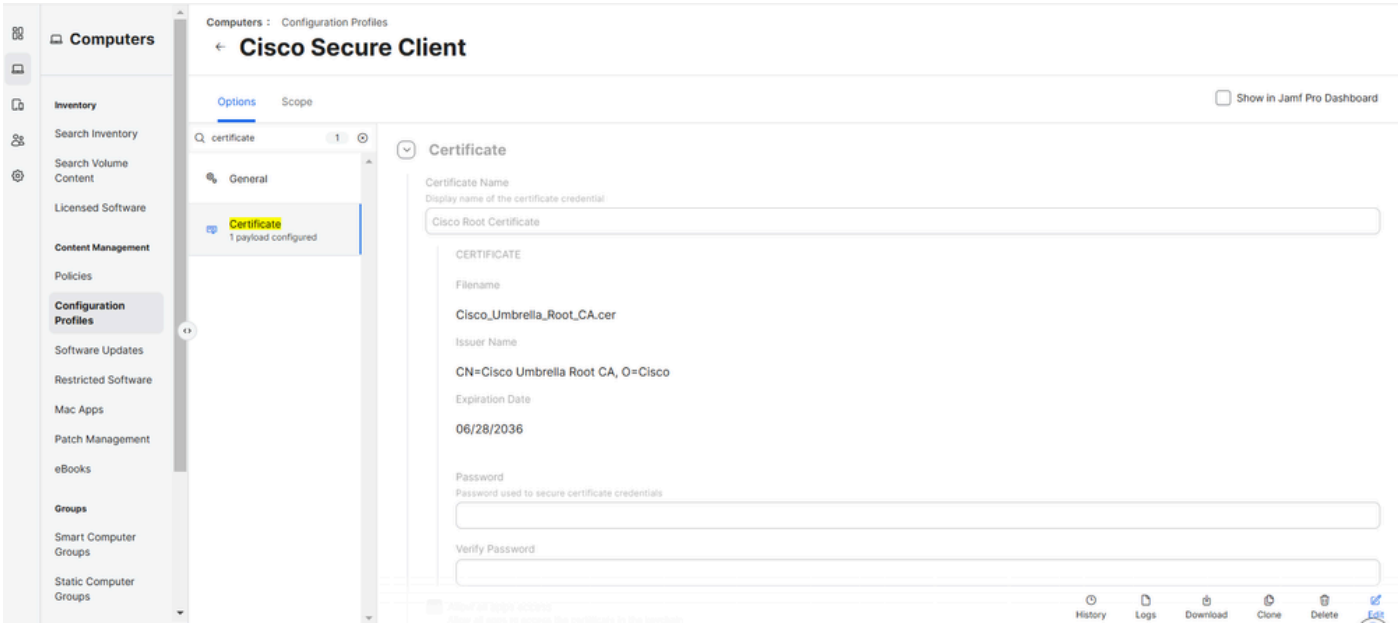
1. Nel dashboard Umbrella in Criteri > Certificato radice, scaricare il certificato radice Cisco Umbrella.

2. In JAMF, selezionare Computer > Profili di configurazione > Cisco Secure Client > Modifica.

3. Cercare Certificato > Configura. Assegnare un nome univoco.

4. In Seleziona opzione certificato, selezionare Upload e caricare il certificato radice Cisco Umbrella scaricato in precedenza nel passaggio 1.

5. Accertarsi di non configurare una password e selezionare Salva.



6. Se viene visualizzato il messaggio Redistribution Options (Opzioni di ridistribuzione), selezionare Distribute to All (Distribuisci su tutti) per annullare immediatamente le modifiche apportate ai dispositivi macOS desiderati.

Verifica

Per verificare se Cisco Secure Client con il modulo Umbrella funziona, selezionare https://policy-debug.checkumbrella.com o eseguire questo comando:

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

Ciascun output deve contenere informazioni univoche e rilevanti per l'organizzazione Umbrella, ad esempio il proprio OrgID.

Soluzione per macOS 14.3

Per macOS versione 14.3 (o successive) con Cisco Secure Client 5.1.x, se si verifica un errore in cui "l'agente client VPN non è in grado di creare il punto di comunicazione tra processi":

1. In JAMF, passare a Impostazioni > Gestione computer > Script > Nuovo.

2. Assegnare un nome univoco e definire la categoria.

3. Passare alla scheda Script e aggiungere quanto segue:

```
#!/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. In Opzioni, verificare che la priorità sia impostata su Dopo. Questo script bash verifica se Cisco Secure Client - AnyConnect VPN service.app è in esecuzione tramite la restituzione di un output previsto con l'ID processo `pgrep -fl`.

- Se restituisce un output vuoto, è possibile verificare che `Cisco Secure Client - AnyConnect VPN service.app` non sia in esecuzione e che lo script venga eseguito per avviare i servizi di base Cisco Secure Client necessari per la corretta esecuzione del modulo Umbrella.

Aggiornamenti automatici

Cisco ha deciso di estendere il supporto per l'aggiornamento automatico dal dashboard Umbrella per includere Secure Client a partire da Secure Client 5.1.6.103 (MR6). In futuro, i clienti che hanno eseguito l'aggiornamento almeno a Cisco Secure Client 5.1.6 MR6 potranno eseguire l'aggiornamento automatico alle versioni più recenti se l'aggiornamento automatico è stato configurato nel dashboard Umbrella.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).