Implementación de CSC en macOS con JAMF con Umbrella Module

Contenido

Introducción

Este documento describe cómo implementar Cisco Secure Client con el módulo Umbrella en dispositivos macOS administrados mediante JAMF.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

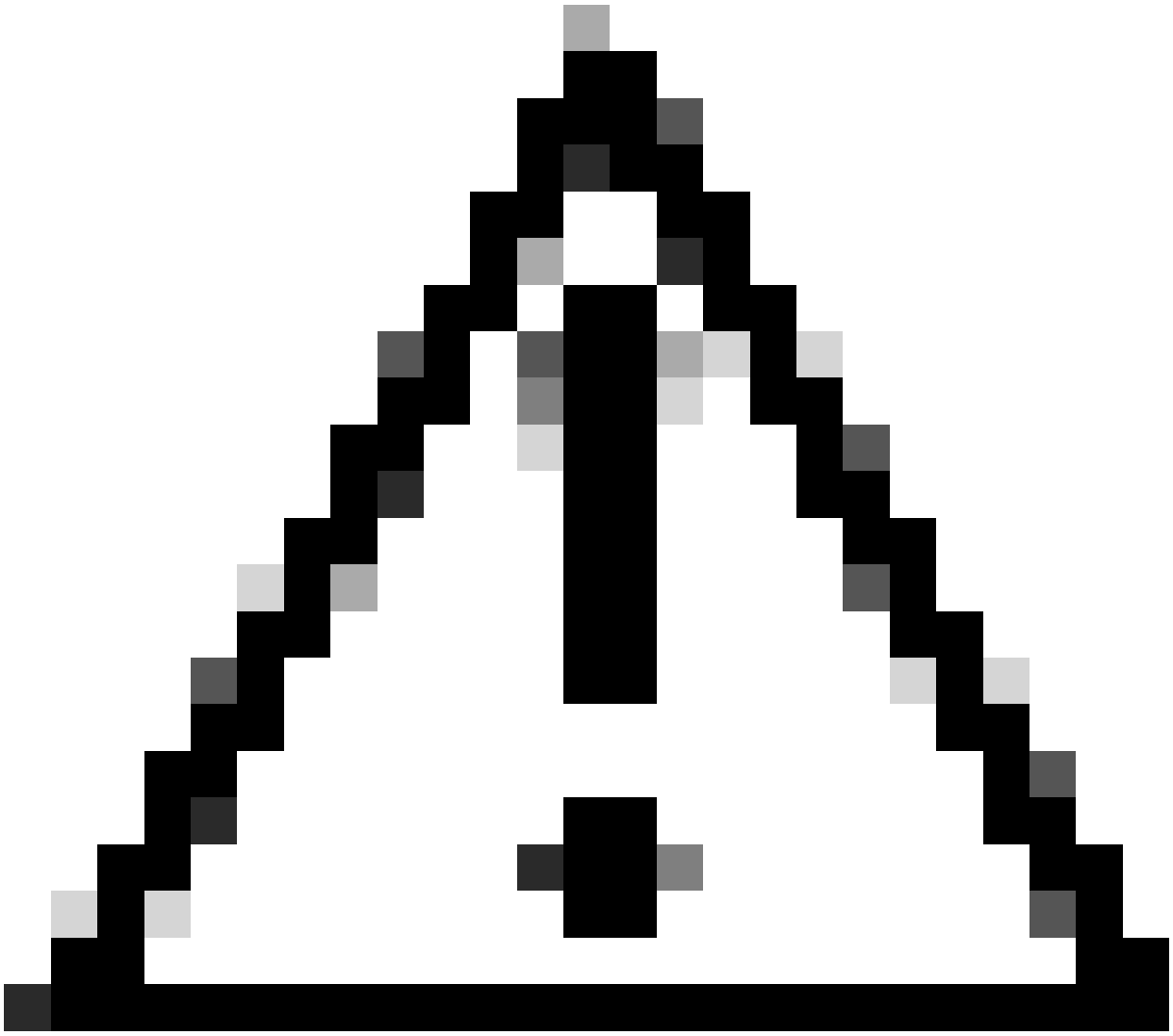
- Los dispositivos macOS deben ser administrados por JAMF.
- Para obtener instrucciones sobre la inscripción de MDM para macOS, consulte la documentación de JAMF.

Componentes Utilizados

La información de este documento se basa en Cisco Secure Client.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente

de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.



Precaución: Este artículo se proporciona tal cual desde el 1 de febrero de 2025. Cisco Umbrella Support no garantiza que estas instrucciones sean válidas después de esta fecha y estén sujetas a cambios en función de las actualizaciones de JAMF y Apple.

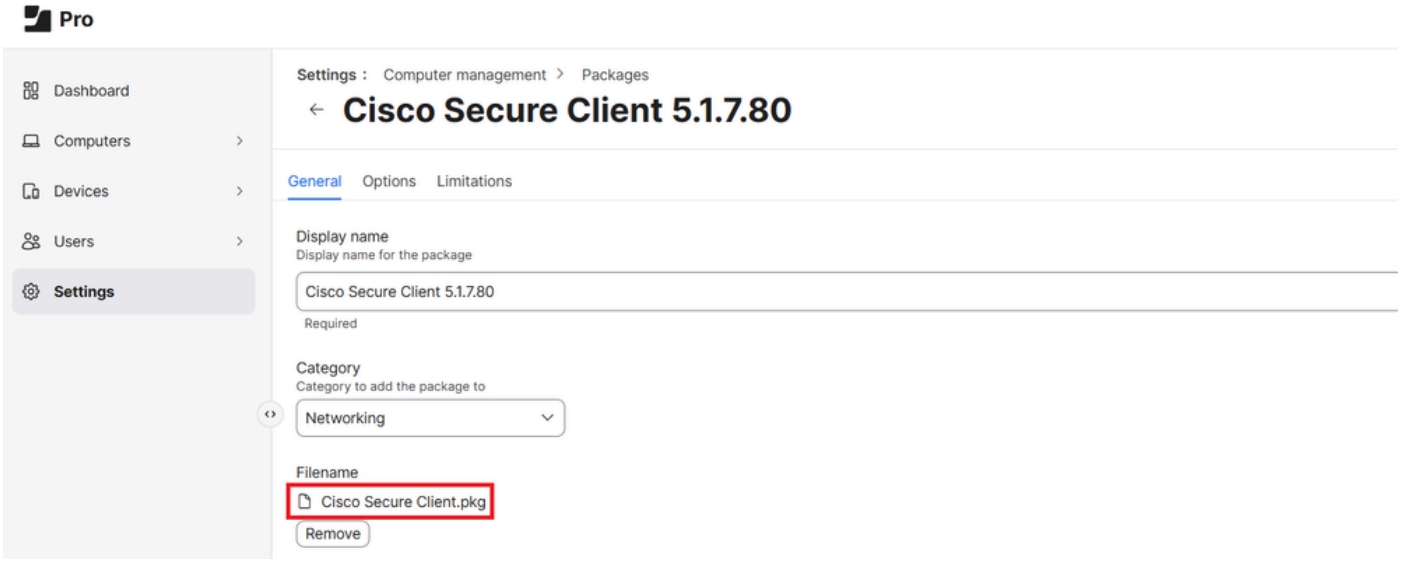
Cargar el paquete de instalación (PKG)

1. Descargue Cisco Secure Client DMG desde el panel de Umbrella enImplementaciones > Equipos en roaming > Cliente en roaming > Paquete de preimplementación > macOS.

2. Inicie sesión en la instancia de nube de JAMF Pro.

3. Vaya a Configuración > Administración de equipos > Paquetes > Nuevo.

4. Cargue el PKG extraído del paquete DMG que ha descargado del panel de Umbrella.

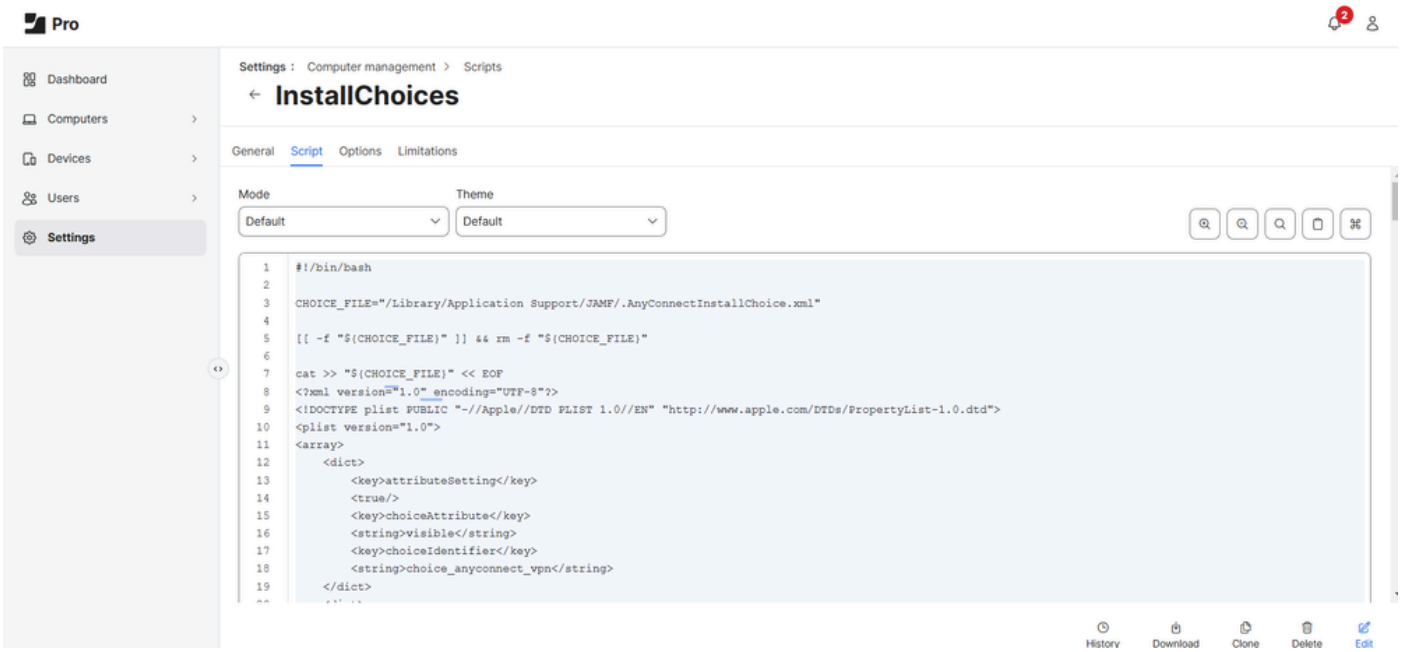


Agregar scripts de selección de módulo y configuración

1. Vaya a Configuración > Administración de equipos > Secuencias de comandos y agregue esta secuencia de comandos para controlar qué módulos se instalan durante la implementación.

2. Puede controlar la instalación de los módulos Secure Client estableciendo un módulo en 0 para omitirlo o en 1 para instalarlo ya que PKG está configurado para instalar todos los módulos de forma predeterminada.

- Puede obtener el archivo XML de ejemplo en la documentación de Umbrella: Personalizar la instalación de macOS de Cisco Secure Client
- Umbrella también añadió el script "installoptions" a este enlace github. En este ejemplo, los módulos Core VPN, Umbrella y DART se establecen en 1 y se pueden incluir en la instalación de Secure Client.



3. Navegue hasta Settings > Computer management> Scripts y agregue este script de modo que cree un archivo de configuración `Orginfo.json` requerido por Cisco Secure Client.

- Descargue el perfil del módulo directamente desde el panel de Umbrella y, a continuación, agregue el Organization ID, Fingerprint y User ID al script:

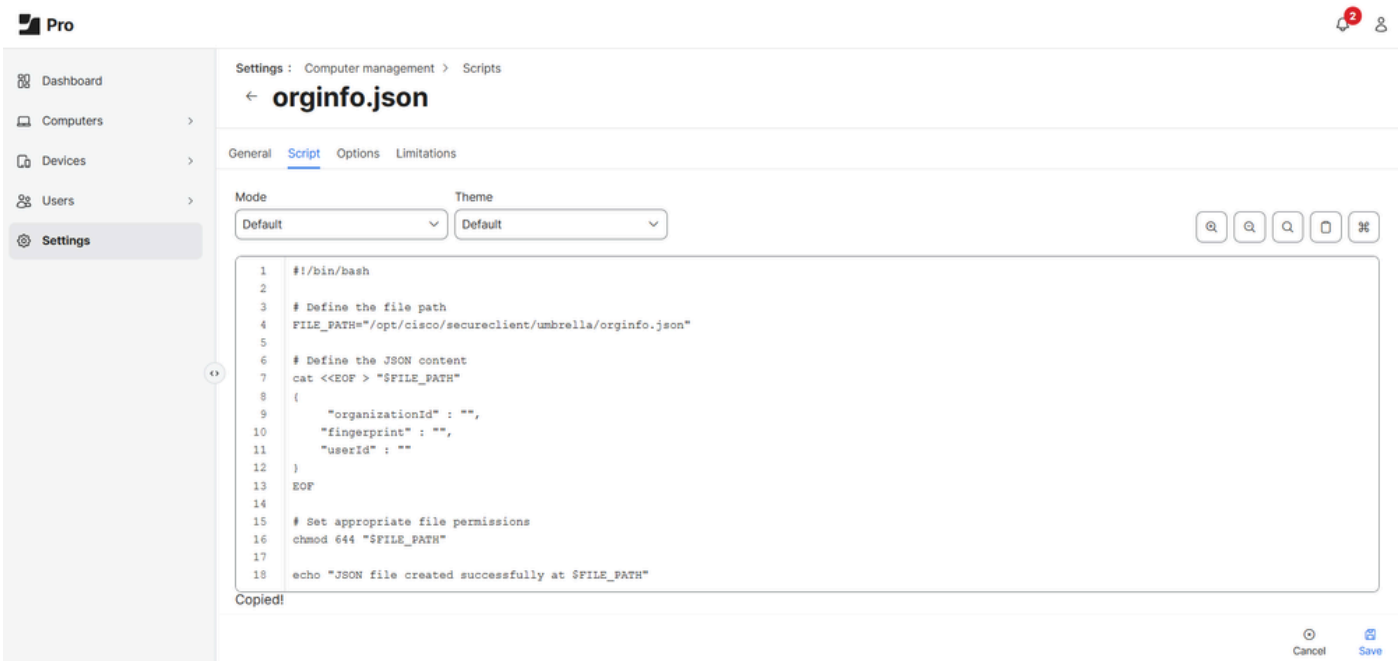
```
#!/bin/bash

# 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

Creación de la política JAMF

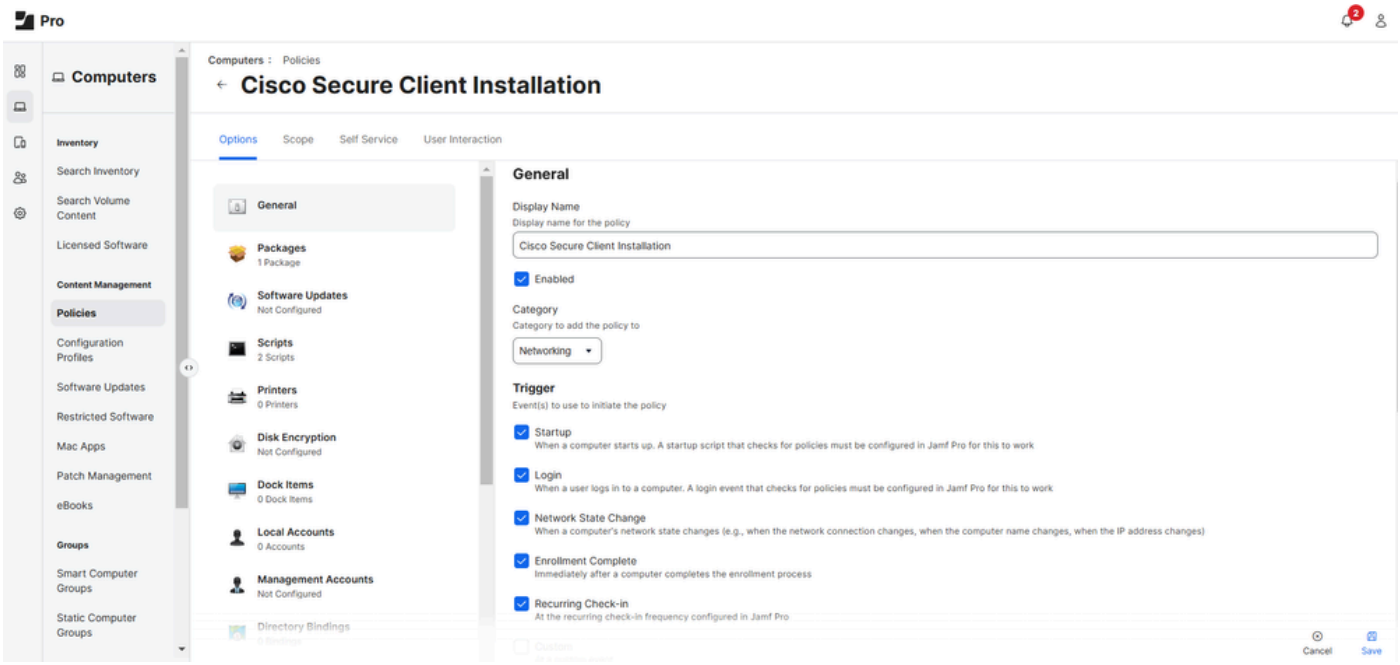
La política JAMF se utiliza para determinar cómo y cuándo se extrae el módulo Cisco Secure Client con Umbrella.

1. Vaya a Equipos > Administración de contenido > Políticas > Nuevo.

2. Asigne un nombre único a la política y seleccione los eventos de categoría y disparador que desee (por ejemplo, cuando se ejecuta esta política).

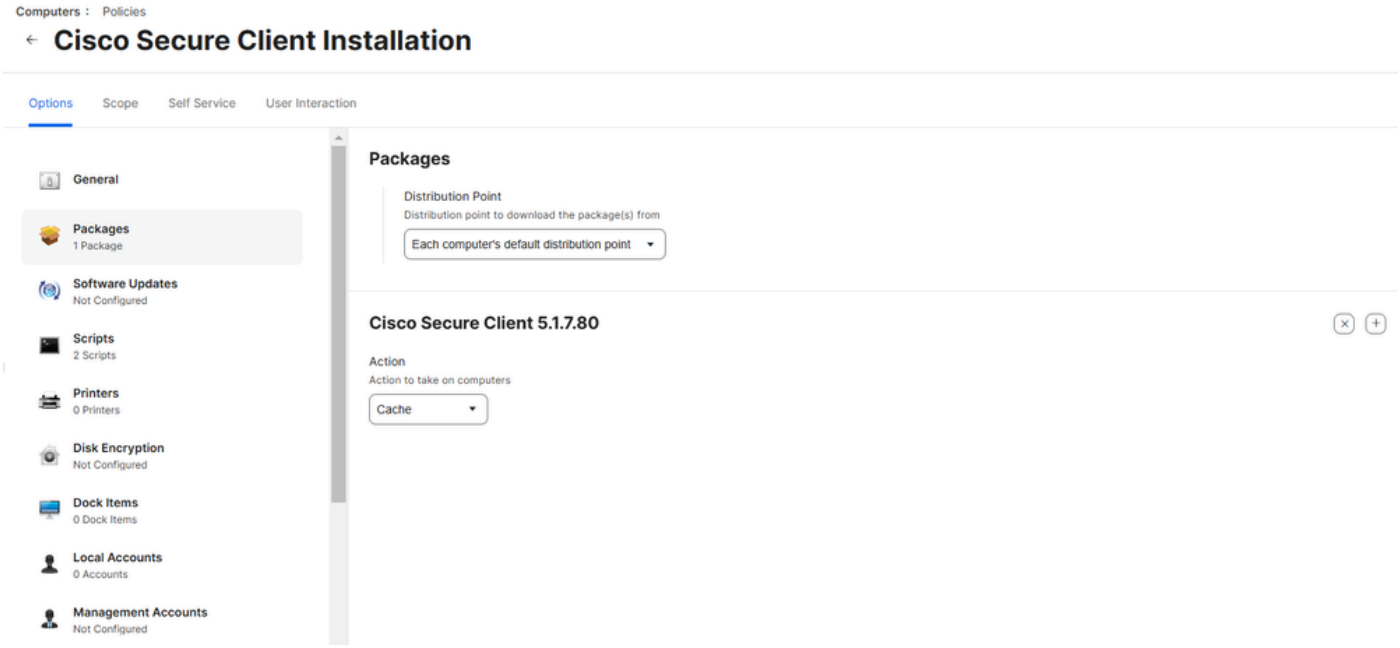
3. Opcionalmente, también puede configurar un comando personalizado que se puede ejecutar en Personalizado. El comando para ejecutar y ejecutar esta política tendría el siguiente aspecto:

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

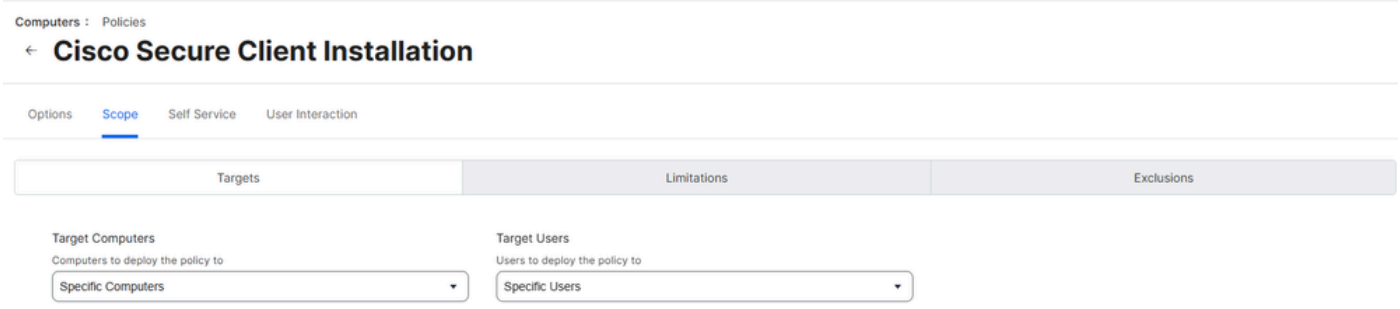


4. Seleccione Paquetes > Configurar y seleccione Agregar junto al paquete de Cisco Secure Client.

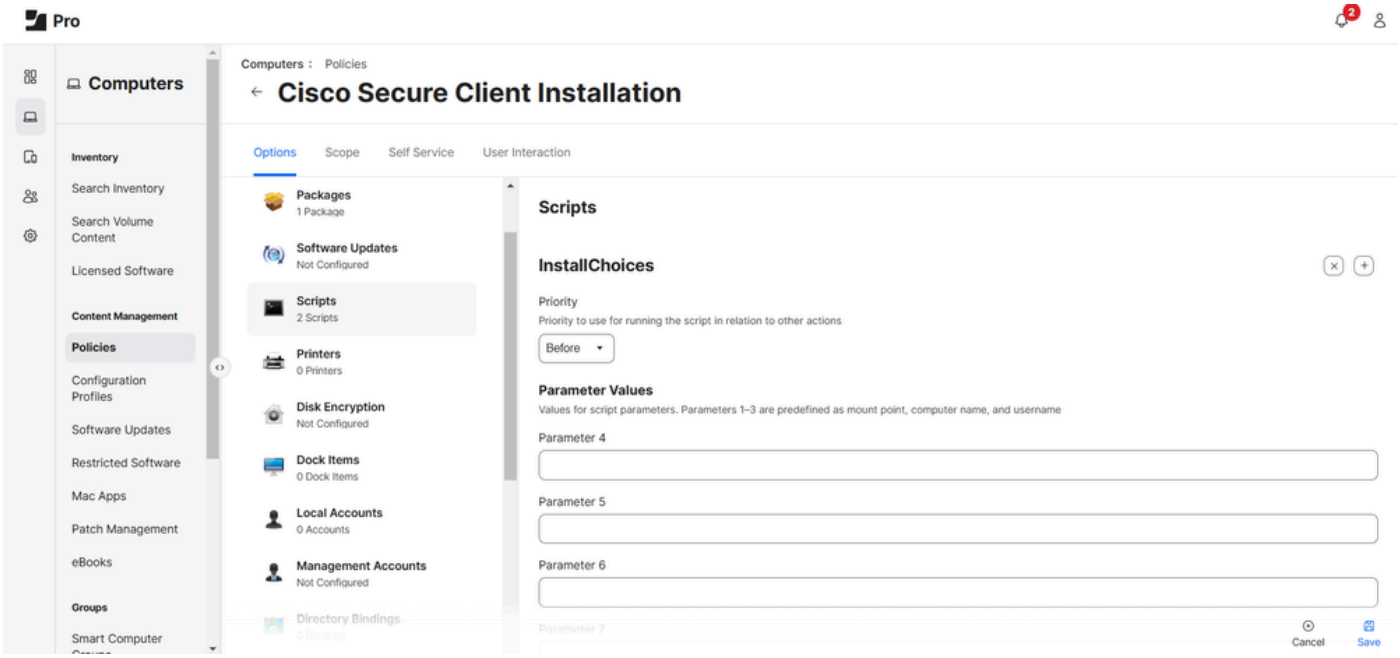
- En Punto de distribución, seleccione Punto de distribución predeterminado de cada equipo.
- En Acción, seleccione Caché.

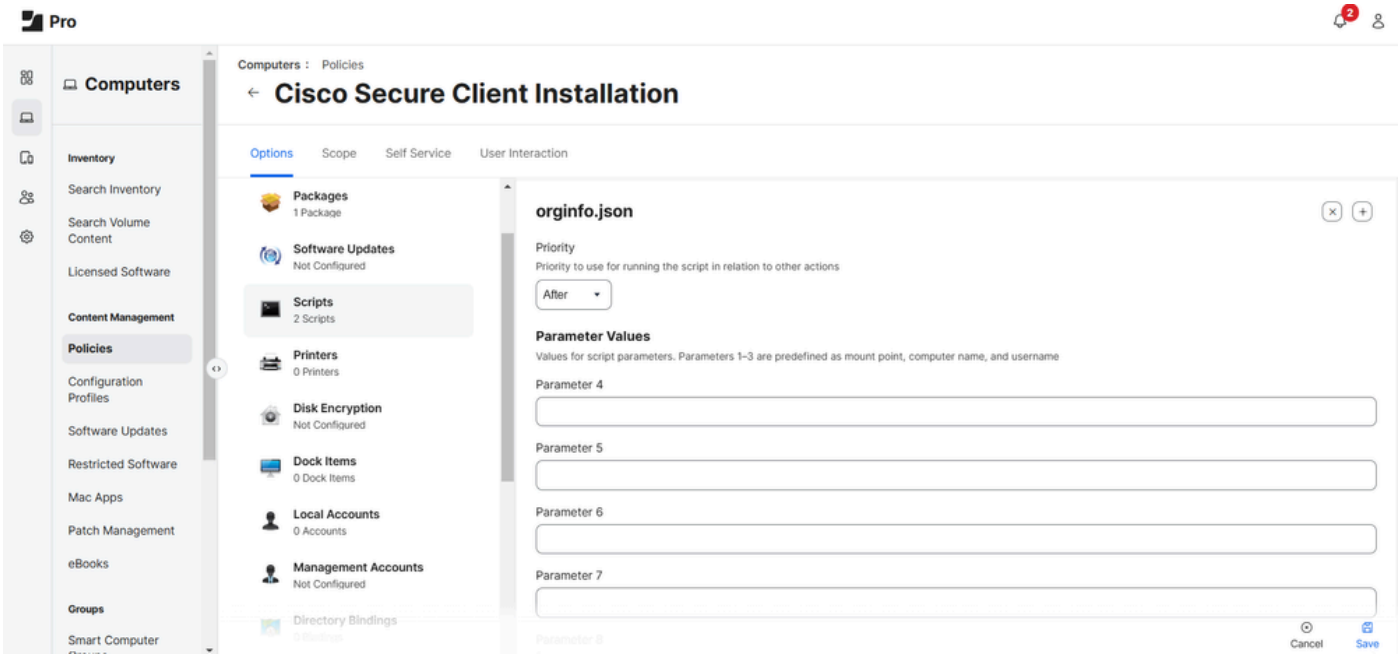


5. Defina el alcance de los dispositivos o usuarios para la implementación y seleccione Guardar.



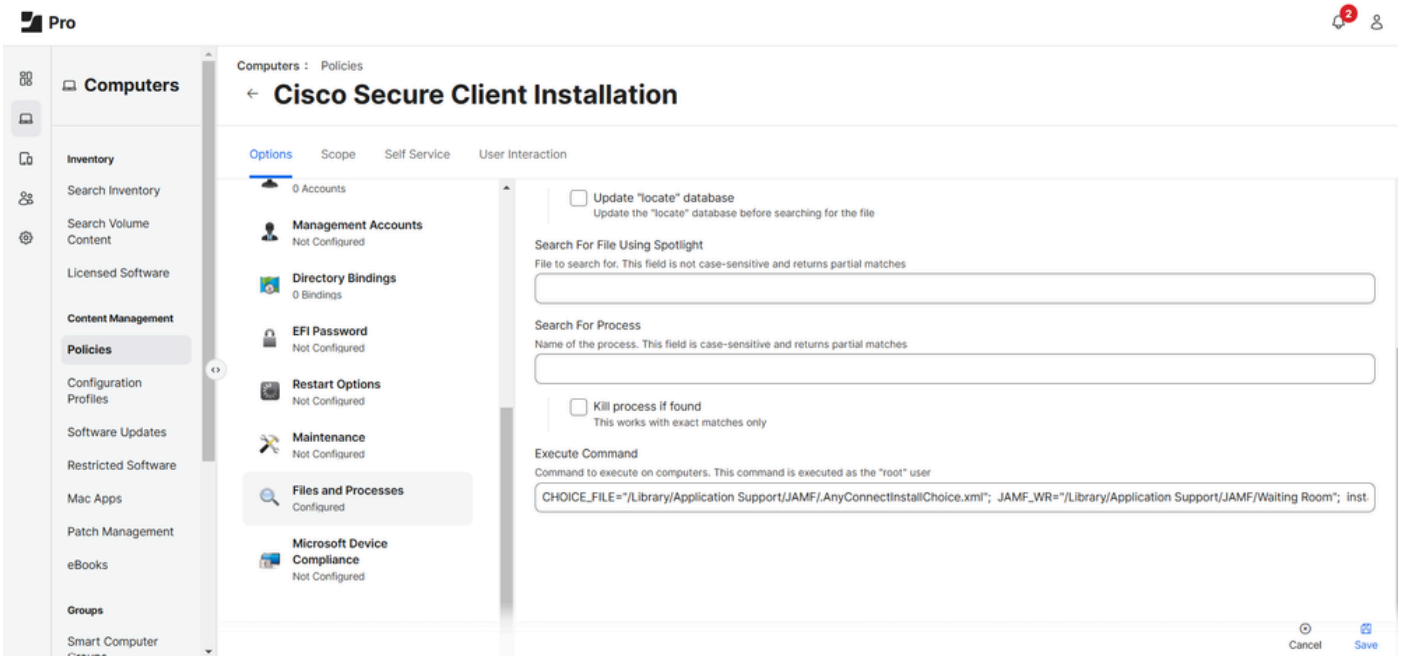
6. Añada losInstallChoicesy los **orginfo.json** scripts y asígneles una prioridad para ejecutarlos en relación con otras acciones.





7. Ejecute este comando para instalar el paquete Cisco Secure Client con los módulos seleccionados en los dispositivos:

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



Configuración de una instalación silenciosa de la extensión del sistema

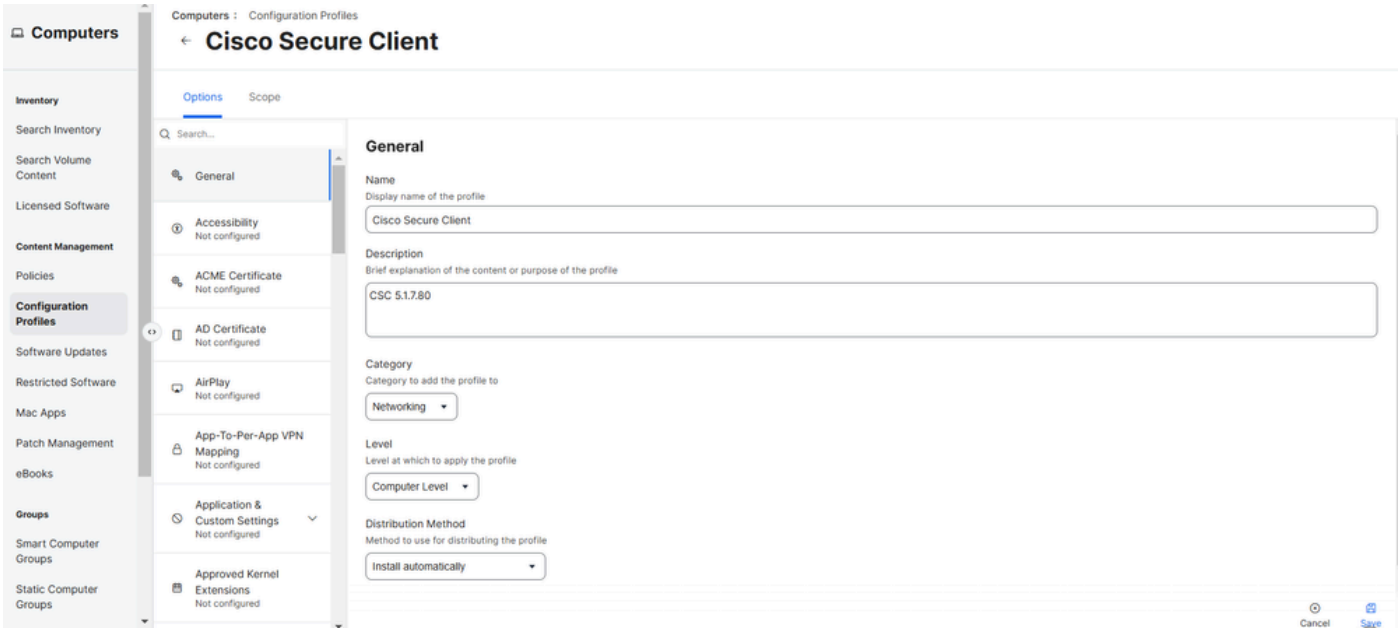
A continuación, utilice JAMF para configurar y permitir las extensiones del sistema necesarias de

Cisco Secure Client para que el módulo Cisco Secure Client con Umbrella se ejecute correctamente sin interacciones del usuario.

1. Vaya a Equipos > Administración de contenido > Perfiles de configuración > Nuevo.

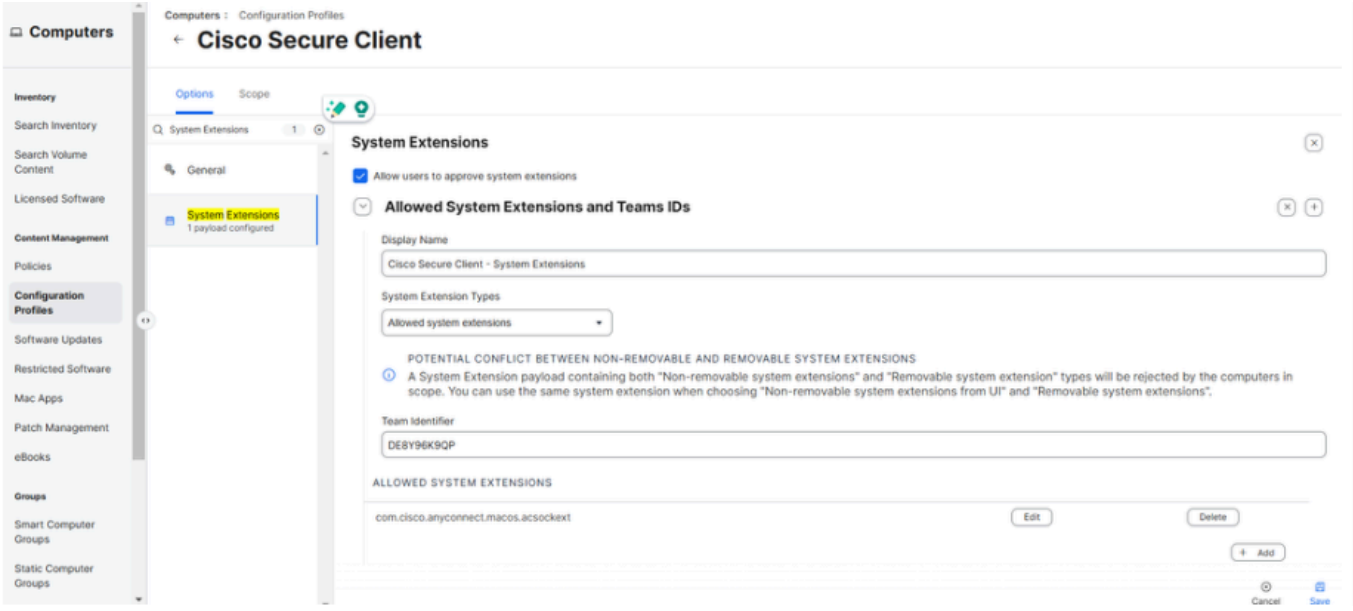
2. Asigne un nombre único al perfil y seleccione la categoría y el método de distribución.

3. Asegúrese de que el nivel está establecido en el nivel de equipo.



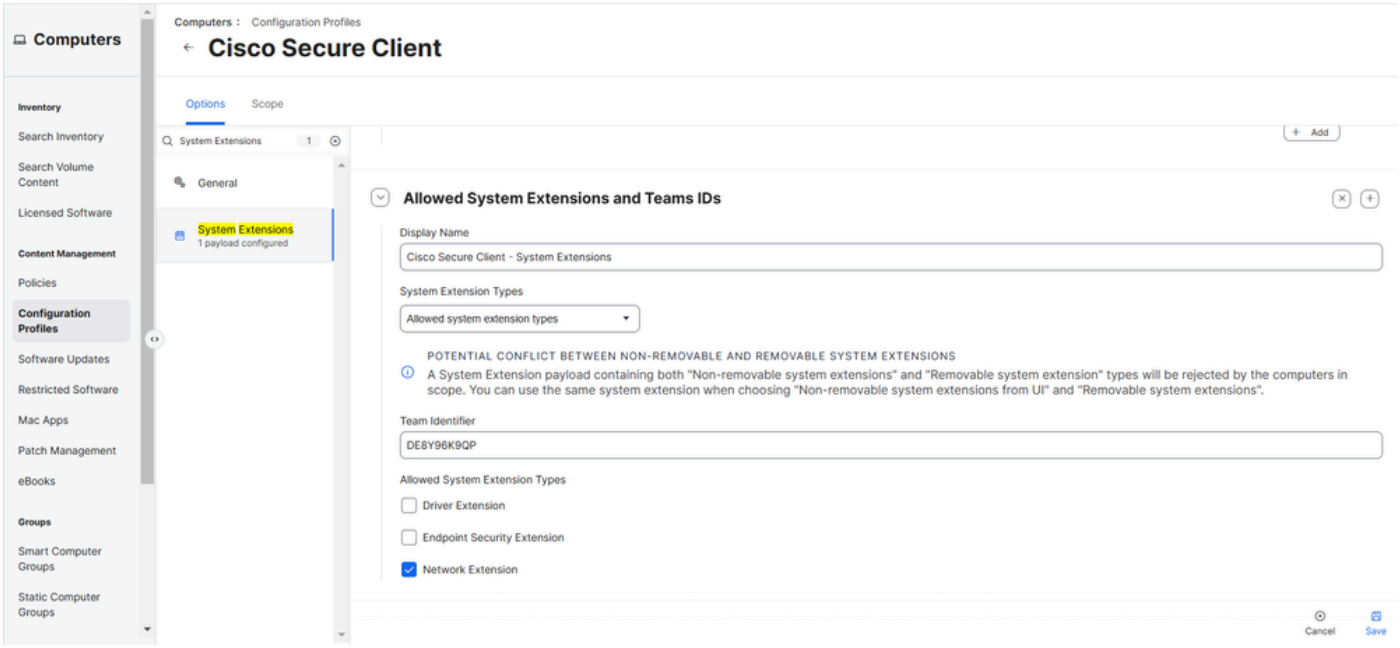
4. Busque Extensiones del sistema > Configurar. Introduzca estos valores:

- Nombre para mostrar: Cisco Secure Client - Extensiones del sistema
- Tipos de extensiones del sistema: Extensiones de sistema permitidas
- Identificador de equipo: DE8Y96K9QP
- Extensiones de sistema permitidas: com.cisco.anyconnect.macos.acsockext y, a continuación, seleccione Guardar.



5. Seleccione el icono + situado junto a ID de equipo y extensiones del sistema permitidos para añadir otra extensión del sistema. A continuación, introduzca estos valores:

- Nombre para mostrar: Cisco Secure Client - Extensiones del sistema
- Tipos de extensiones del sistema: Permitir tipos de extensión del sistema
- Identificador de equipo: DE8Y96K9QP
- Permitir tipos de extensión del sistema: Extensión de red

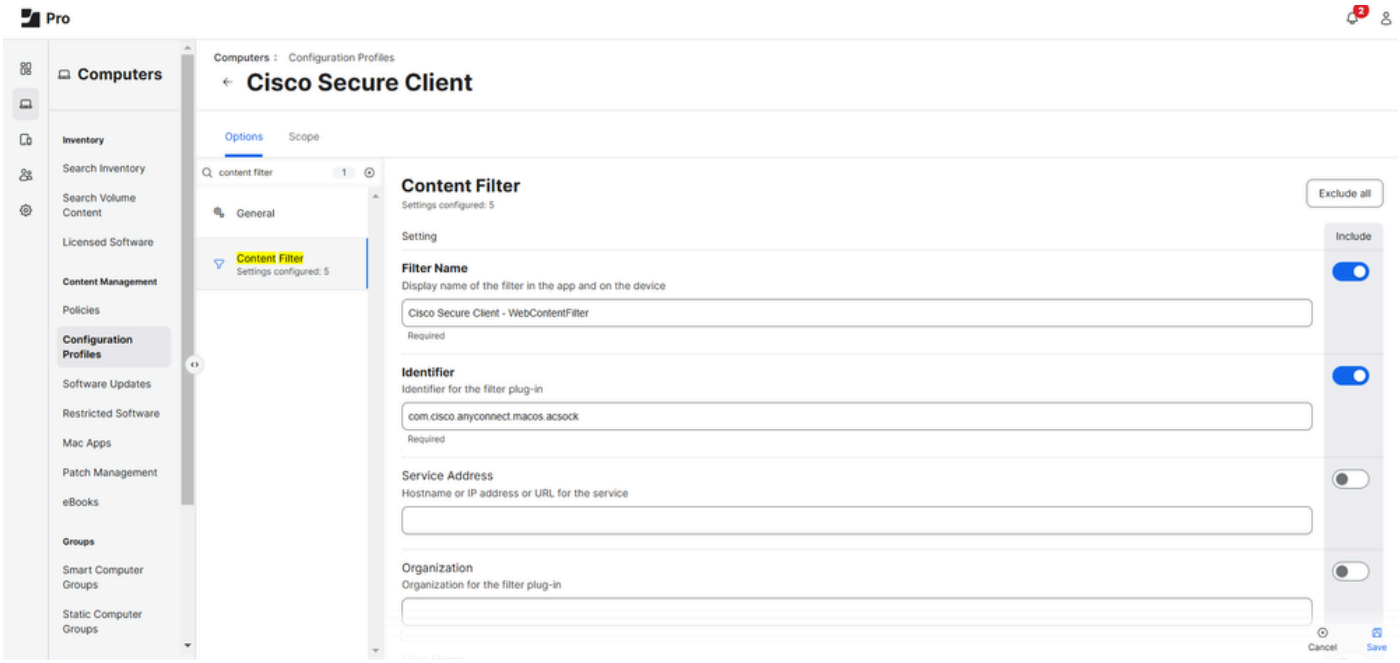


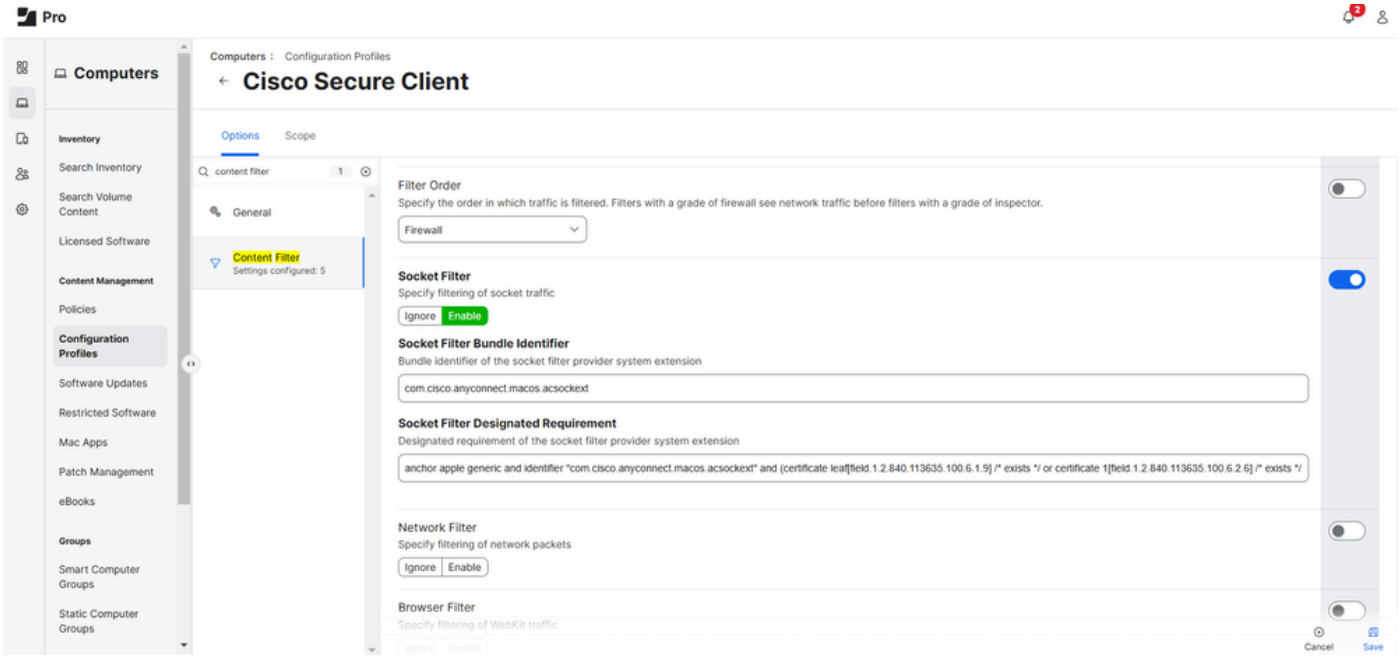
Configuración de la instalación silenciosa para el filtro de contenido

A continuación, configure una instalación silenciosa para el filtro de contenido, que se correlaciona con el filtro de socket del módulo Cisco Secure Client with Umbrella:

1. Busque Filtro de contenido. Habilite y complete estos campos con sus valores respectivos:

- Nombre del filtro: Cisco Secure Client: WebContentFilter
- Identifier: com.cisco.anyconnect.macos.acsock
- Filtro de socket: Habilitado
- Identificador de conjunto de filtro de socket: com.cisco.anyconnect.macos.acsockext
- Requisito designado de filtro de socket:
  `delimitador de manzana genérico e identificador "com.cisco.anyconnect.macos.acsockext" y (hoja de certificado [campo.1.2.840.113635.100.6.1.9] /* existe */ o certificado 1[campo.1.2.840.113635.100.6.2.6] /* existe */ y hoja de certificado [campo.1.2.840.113635.100.6.1.13] /* existe */ y certificado leaf[subject.OU] = DE8Y96K9QP)`





2. En Datos personalizados, seleccione Agregar cinco veces e introduzca estos valores:

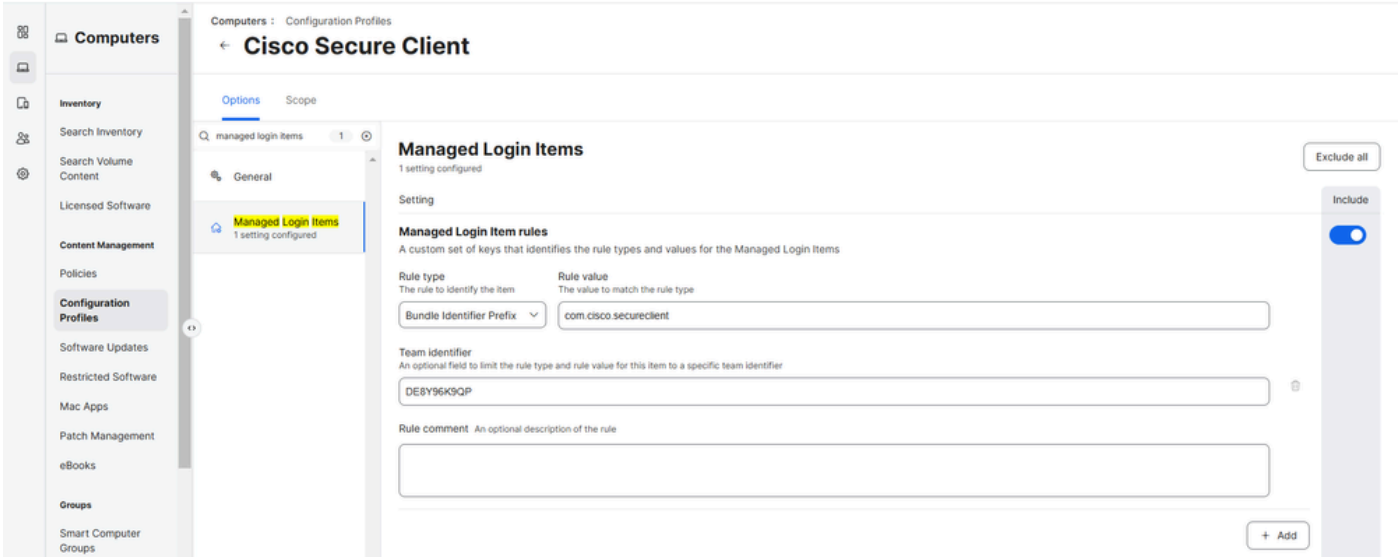
Clave	Valor
AutofiltroActivado	falso
FilterBrowsers	falso
FilterSockets	verdadero
FilterPackets	falso
GradoFiltro	firewall

Configurar elementos de inicio de sesión administrados

La configuración de los elementos de inicio de sesión gestionados para el módulo Cisco Secure Client con Umbrella garantiza que Cisco Secure Client se inicie al iniciar el dispositivo.

Para realizar la configuración, busque Managed Login Items y configure los campos con estos valores:

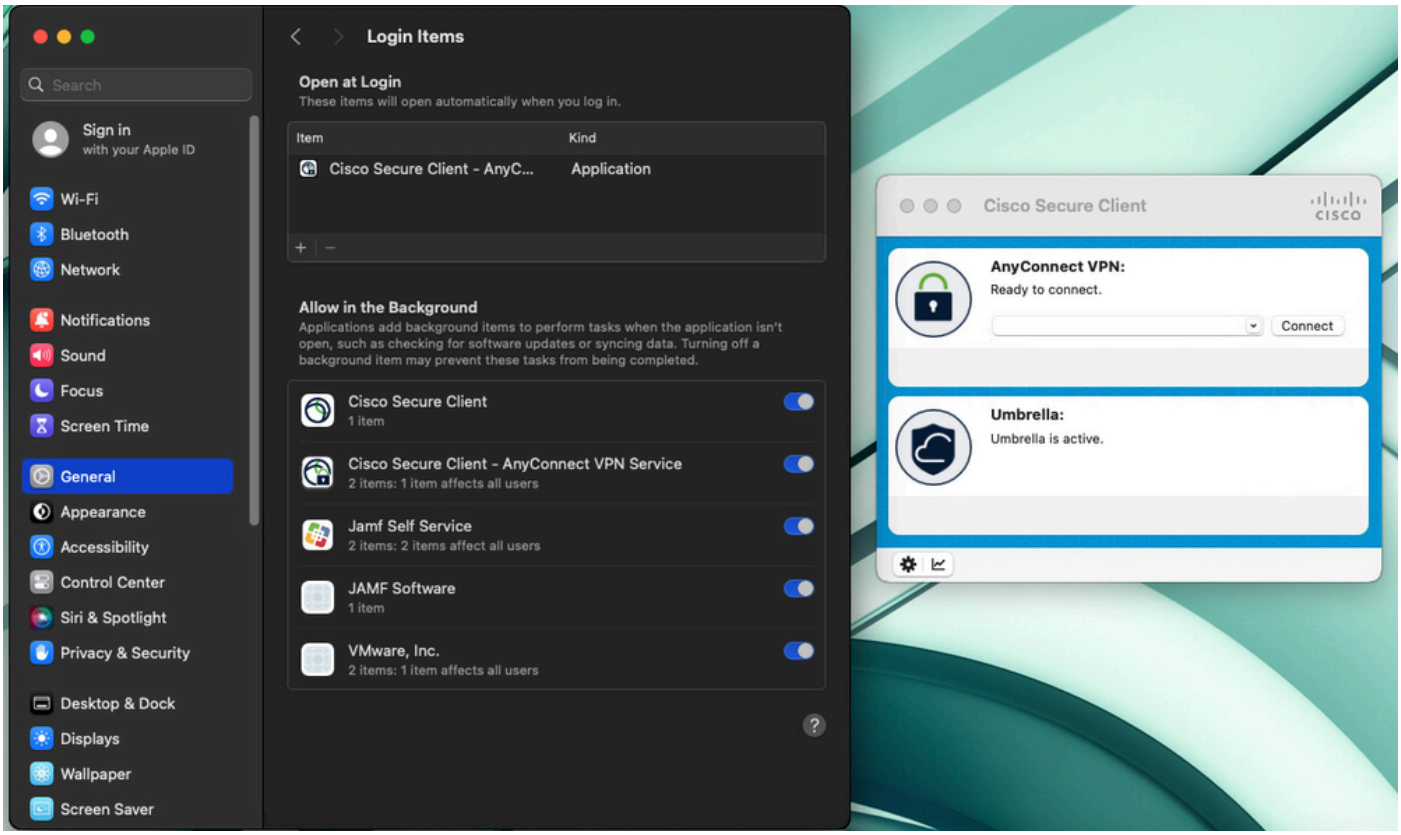
- Tipo de regla: Prefijo de identificador de paquete
- Valor de regla: com.cisco.secureclient
- Identificador de equipo: DE8Y96K9QP

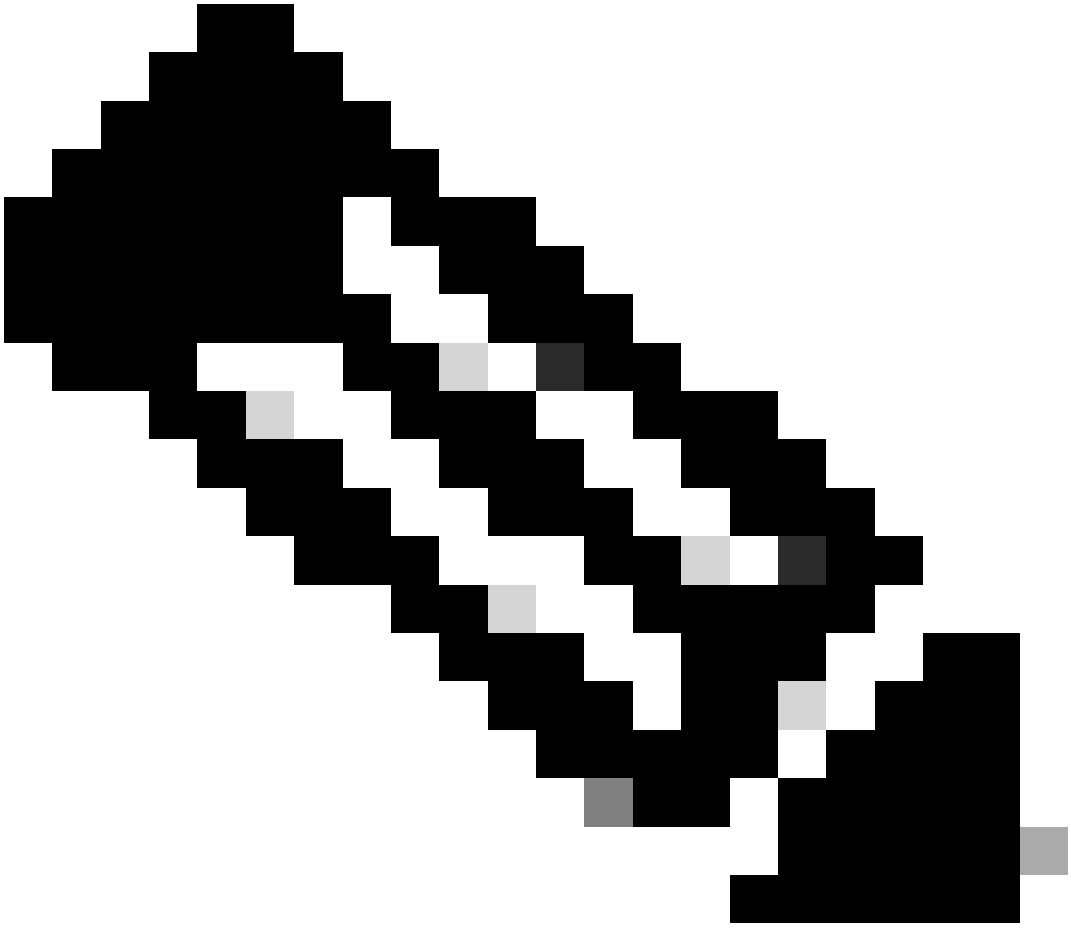


Asignar ámbito e implementación de inserción

1. Navegue hasta Alcance y defina el alcance para dispositivos o usuarios.

2. El módulo Cisco Secure Client con Umbrella se puede enviar a los dispositivos macOS deseados cuando uno de los desencadenadores que configuró en el paso 2 de Create a JAMF Policy está activado. Como alternativa, puede publicar esto a través del portal de autoservicio de 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: Incluso si un usuario intenta desactivar el proxy DNS o el proxy transparente en Configuración del sistema (Red > Filtro), se volverá a activar automáticamente de forma predeterminada, ya que el filtro de contenido se activará mediante JAMF como se describe en este artículo y no se podrá desactivar.

Configurar excepción de firewall macOS

Si el firewall macOS está configurado para Bloquear todas las conexiones entrantes, también debe agregar Cisco Secure Client y sus componentes a su lista de excepciones:

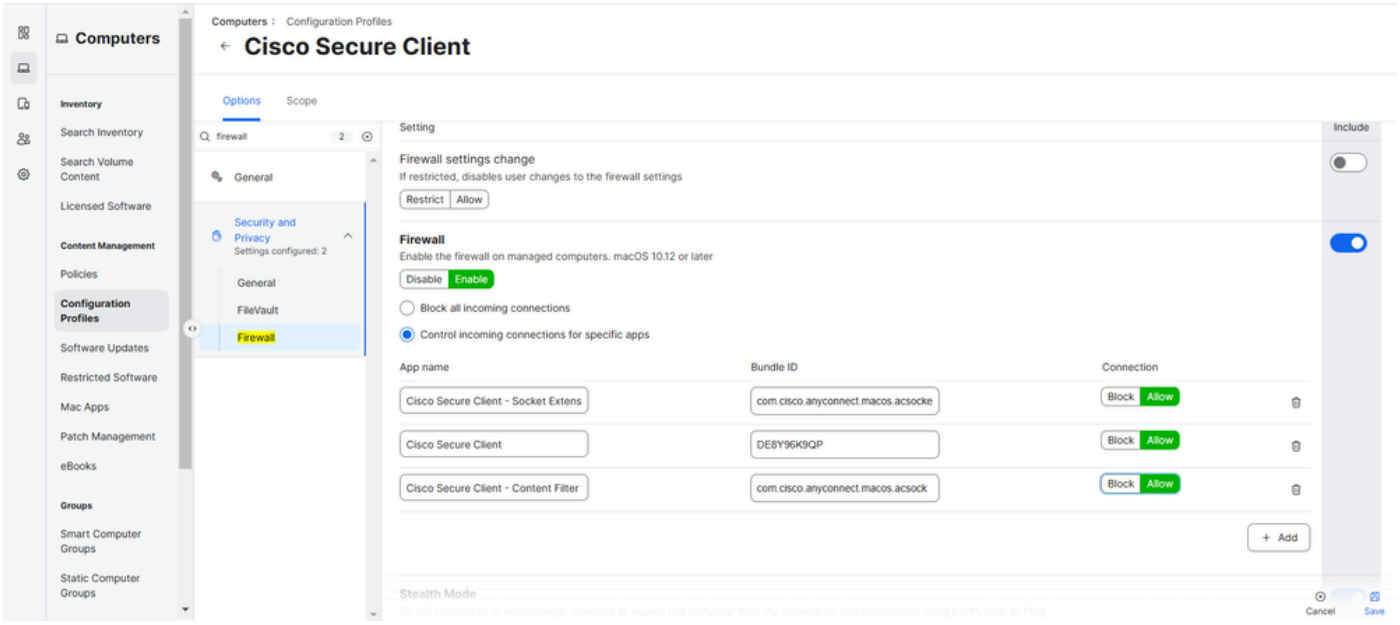
1. Vaya a Equipos > Administración de contenido > Perfiles de configuración.

2. Seleccione el perfil de configuración de Cisco Secure Client y busque Seguridad y privacidad.

3. Configúrelo con estos parámetros:

- Firewall: Habilitar: controla las conexiones entrantes para aplicaciones específicas

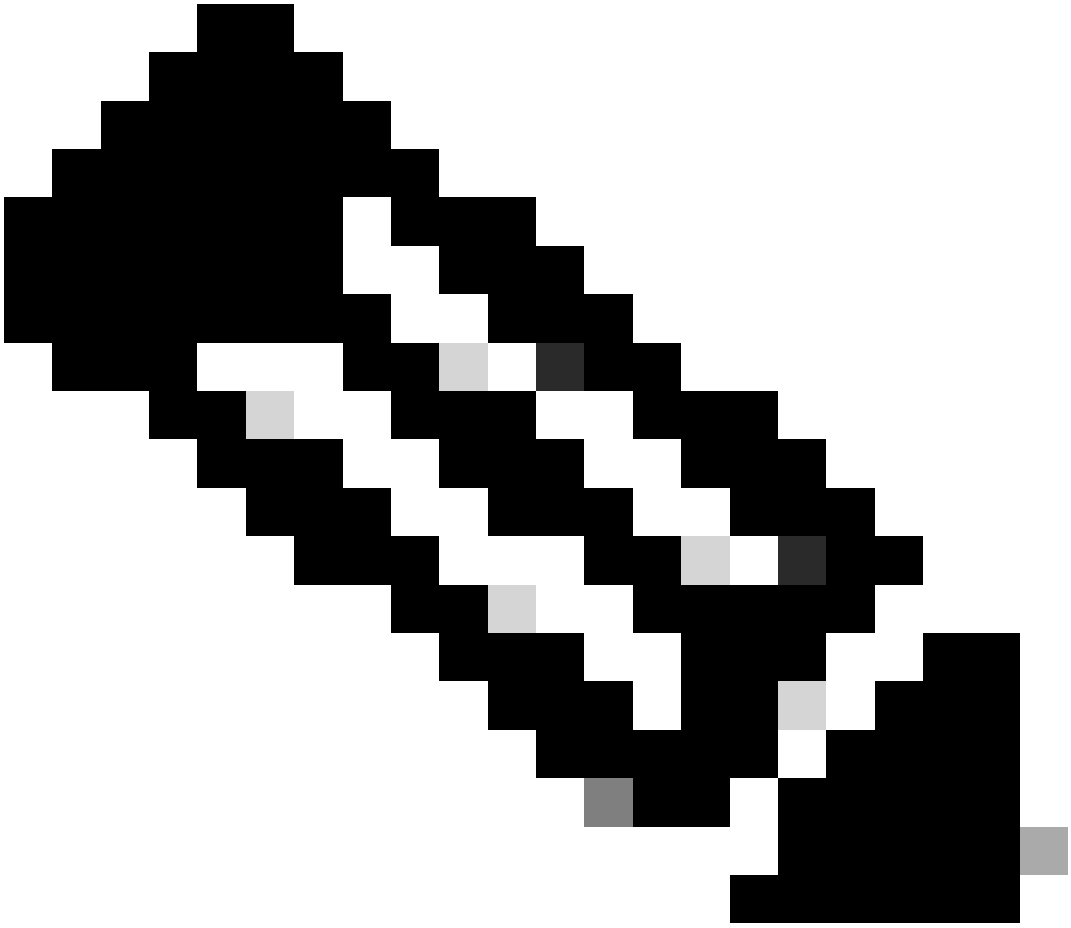
Nombre de aplicación	ID del paquete
Cisco Secure Client - Extensiones de socket	com.cisco.anyconnect.macos.acsockext
Cliente seguro de Cisco	DE8Y96K9QP
Cisco Secure Client - Filtro de contenido	com.cisco.anyconnect.macos.acsock



4. Seleccione Guardar.

5. Si se le solicita Opciones de Redistribución, seleccione Distribuir a Todos para aplicar inmediatamente los cambios a los dispositivos macOS que desee.

Implementación del certificado raíz de Cisco Umbrella



> Nota: Este paso sólo se aplica a las nuevas implementaciones de Cisco Secure Client o de dispositivos que no tengan el certificado raíz de Cisco Umbrella implementado anteriormente. Si va a migrar desde el cliente de roaming de Umbrella o desde el cliente Cisco AnyConnect 4.10, y/o ha implementado el certificado raíz de Cisco Umbrella ya en el pasado, puede saltarse esta sección.

Descargue el certificado raíz de Cisco Umbrella desdePolíticas > Certificado raíz en el panel de Umbrella.

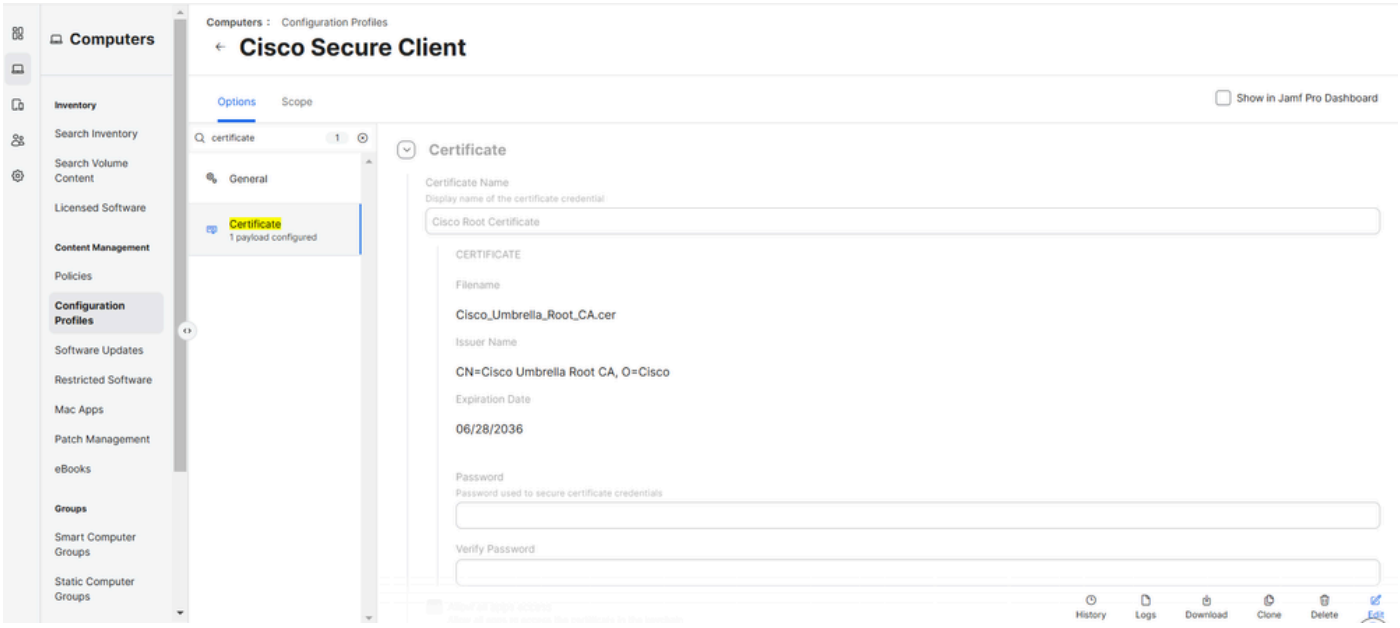
1. En el panel de Umbrella, en Políticas > Certificado raíz, descargue el Certificado raíz de Cisco Umbrella.

2. En JAMF, navegue hasta Computers > Configuration Profiles > Cisco Secure Client > Edit.

3. Busque Certificate > Configure. Denle un nombre único.

4. En Select Certificate Option, seleccione Upload y cargue el certificado raíz de Cisco Umbrella que descargó anteriormente en el paso 1.

5. Asegúrese de que no configura una contraseña aquí y seleccione Guardar.



6. Si se le solicita Opciones de Redistribución, seleccione Distribuir a Todos para aplicar inmediatamente los cambios a los dispositivos macOS que desee.

Verificación

Para verificar si el módulo Cisco Secure Client con Umbrella funciona, navegue hasta https://policy-debug.checkumbrella.com o ejecute este comando:

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

Cualquiera de los resultados debe contener información única y relevante para su organización Umbrella, como su OrgID.

Solución alternativa para macOS 14.3

Para macOS 14.3 (o posterior) con Cisco Secure Client 5.1.x, si encuentra "El agente de cliente VPN no pudo crear el depósito de comunicación entre procesos":

1. En JAMF, vaya aConfiguración > Administración de equipos > Secuencias de comandos > Nuevo.

2. Dé un nombre único y defina su categoría.

3. Acceda a la pestaña Script y añada lo siguiente:

```
#!/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. En Opciones, asegúrese de que la Prioridad está establecida en Después. Esta secuencia de comandos bash comprueba si Cisco Secure Client - AnyConnect VPN service.app se está ejecutando mediante la devolución de una salida esperada con el ID de proceso de `pgrep -fl`.

- Si devuelve un resultado vacío, puede confirmar que `Cisco Secure Client - AnyConnect VPN service.app` no se está ejecutando y que la secuencia de comandos se ejecuta para iniciar los servicios principales de Cisco Secure Client que se requieren para que el módulo Umbrella se ejecute correctamente.

Actualizaciones automáticas

Cisco ha decidido ampliar la compatibilidad con la actualización automática desde el panel Umbrella para incluir Secure Client a partir de Secure Client 5.1.6.103 (MR6). De ahora en adelante, los clientes que hayan actualizado a al menos Cisco Secure Client 5.1.6 MR6 podrán actualizar automáticamente a las versiones más recientes si la actualización automática se ha configurado en el panel de Umbrella.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).