使用帶有Umbrella模組的JAMF將CSC部署到macOS

目錄

簡介

本文檔介紹如何使用JAMF將帶Umbrella模組的Cisco安全客戶端部署到受管macOS裝置。

必要條件

需求

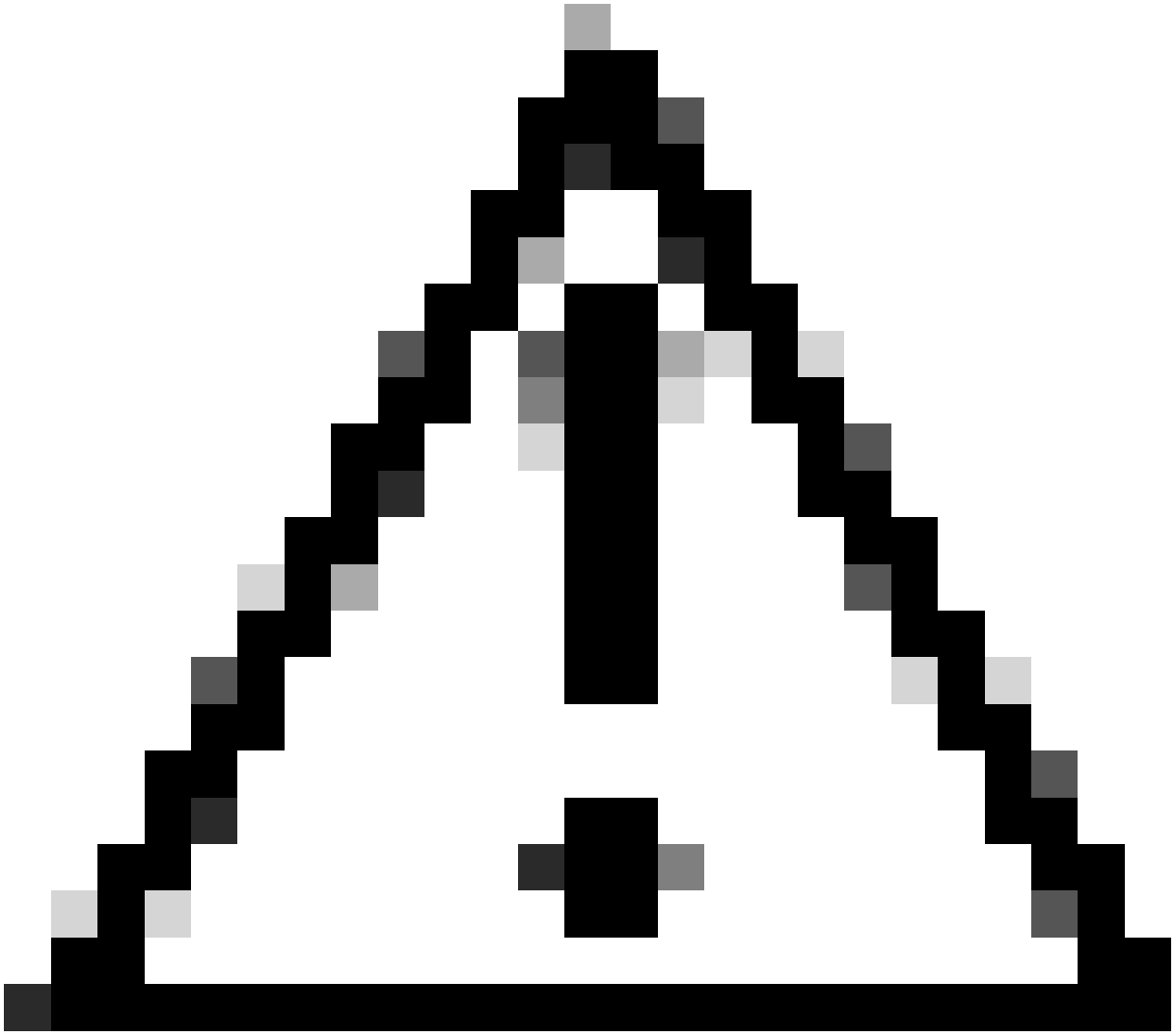
思科建議您瞭解以下主題：

- macOS裝置必須由JAMF管理。
- 有關MacOS的MDM註冊說明，請參閱JAMF文檔。

採用元件

本檔案中的資訊是根據思科安全使用者端。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。



注意：本文自2025年2月1日起提供。Cisco Umbrella支援不保證這些說明在此日期之後有效，並且可能會根據JAMF和Apple的更新進行更改。

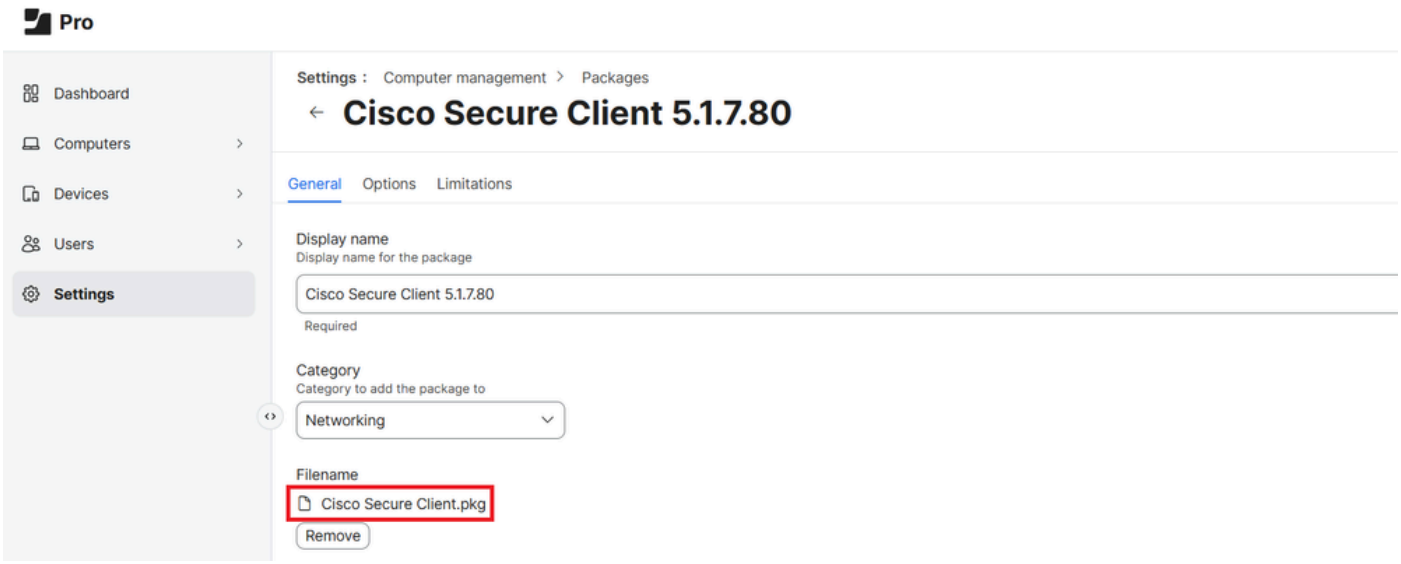
上傳安裝包(PKG)

1.從部署>漫遊電腦>漫遊客戶端>預部署包> macOS下的Umbrella控制面板下載Cisco Secure Client DMG。

2.登入您的JAMF Pro雲例項。

3.導覽至「設定」>「電腦管理」>「包」>「新建」。

4.上傳從您從Umbrella控制面板下載的DMG包提取的PKG。

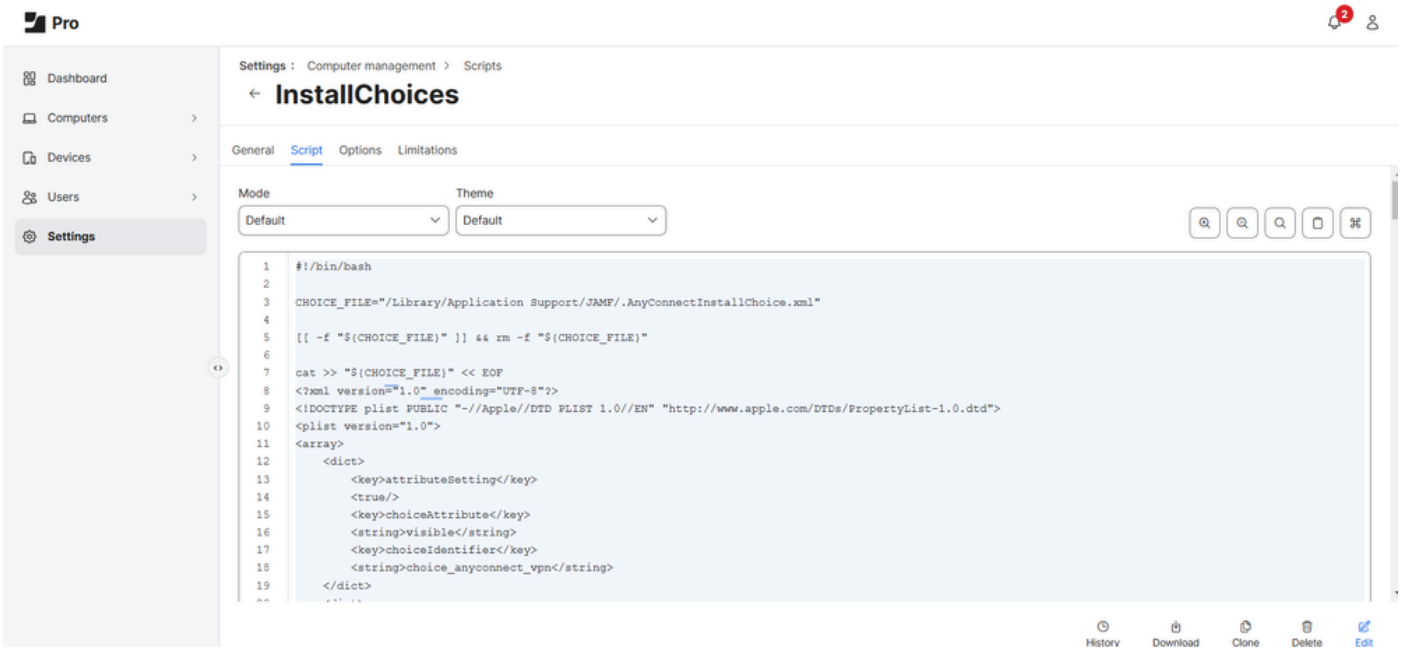


新增配置和模組選擇指令碼

1.轉到設定>電腦管理>指令碼，然後新增此指令碼以控制部署過程中安裝哪些模組。

2.您可以控制安全客戶端模組的安裝，方法是將模組設定為0以跳過安全客戶端模組，或設定為1以安裝安全客戶端模組，因為PKG配置為預設安裝所有模組。

- 您可以從Umbrella文檔獲取示例XML檔案：自定義Cisco Secure Client的macOS安裝
- Umbrella還將「installchoices」指令碼新增到此github連結中。在本示例中，核心VPN、Umbrella和DART模組設定為1，可以包括在安全客戶端安裝中。



3.導航到設定>電腦管理>指令碼，然後新增此指令碼，以便它建立Cisco Secure Client所需的配置檔案Orginfo.json。

- 直接從Umbrella控制面板下載模組配置檔案，然後將Organization ID、Fingerprint和User

ID新增到指令碼：

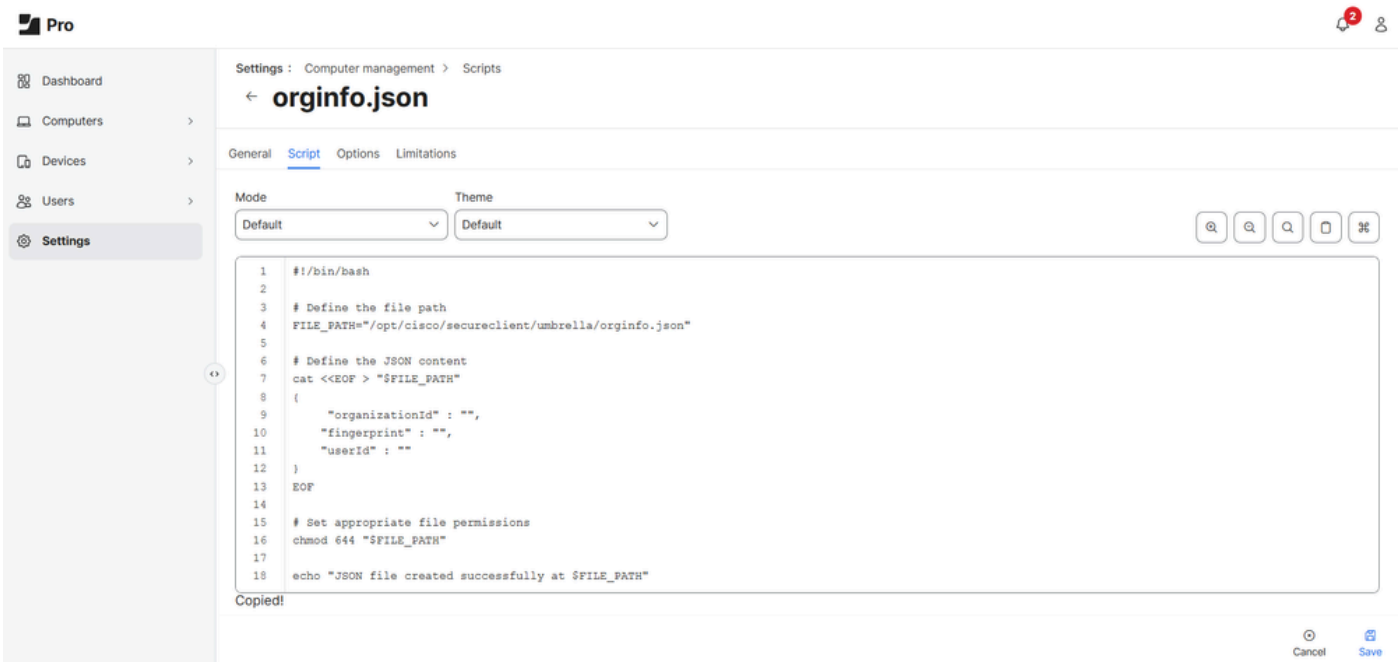
```
#!/bin/bash

# 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

建立JAMF策略

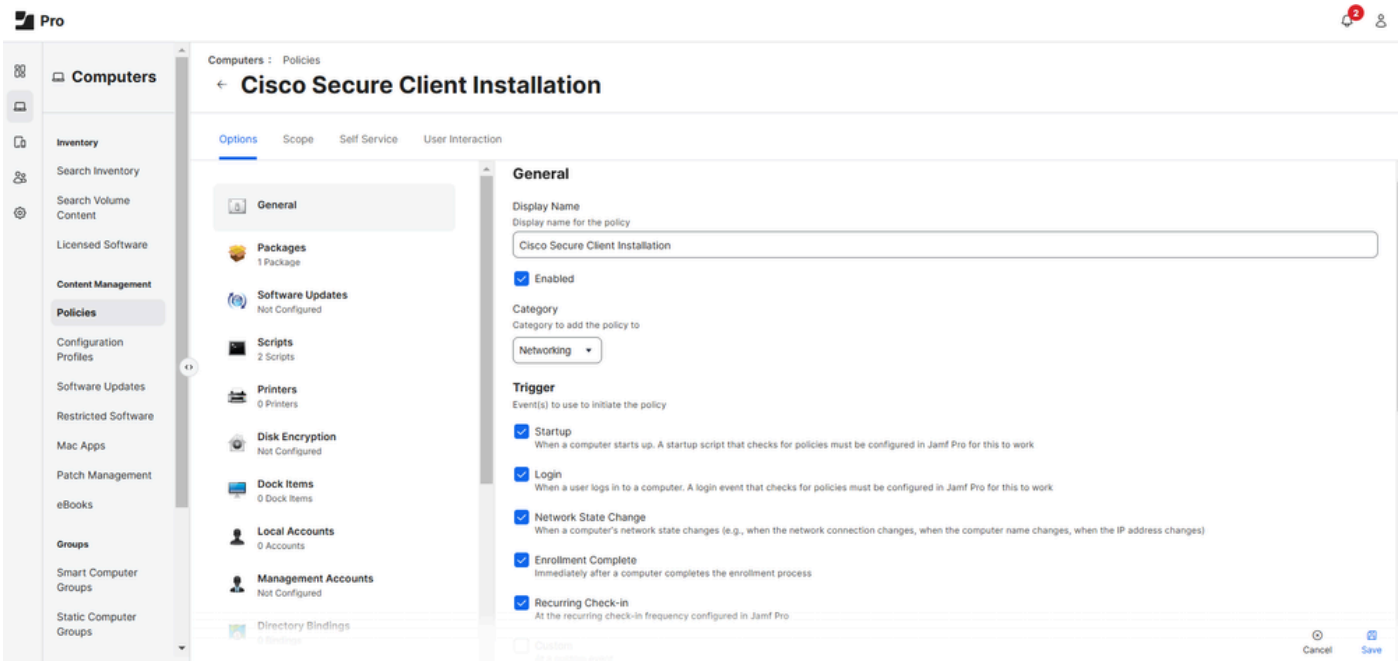
JAMF策略用於確定如何以及何時推出帶有Umbrella模組的思科安全客戶端。

1.導覽至電腦>內容管理>策略>新建。

2.為策略分配唯一的名稱，並選擇所需的Category和Trigger事件（例如，執行此策略時）。

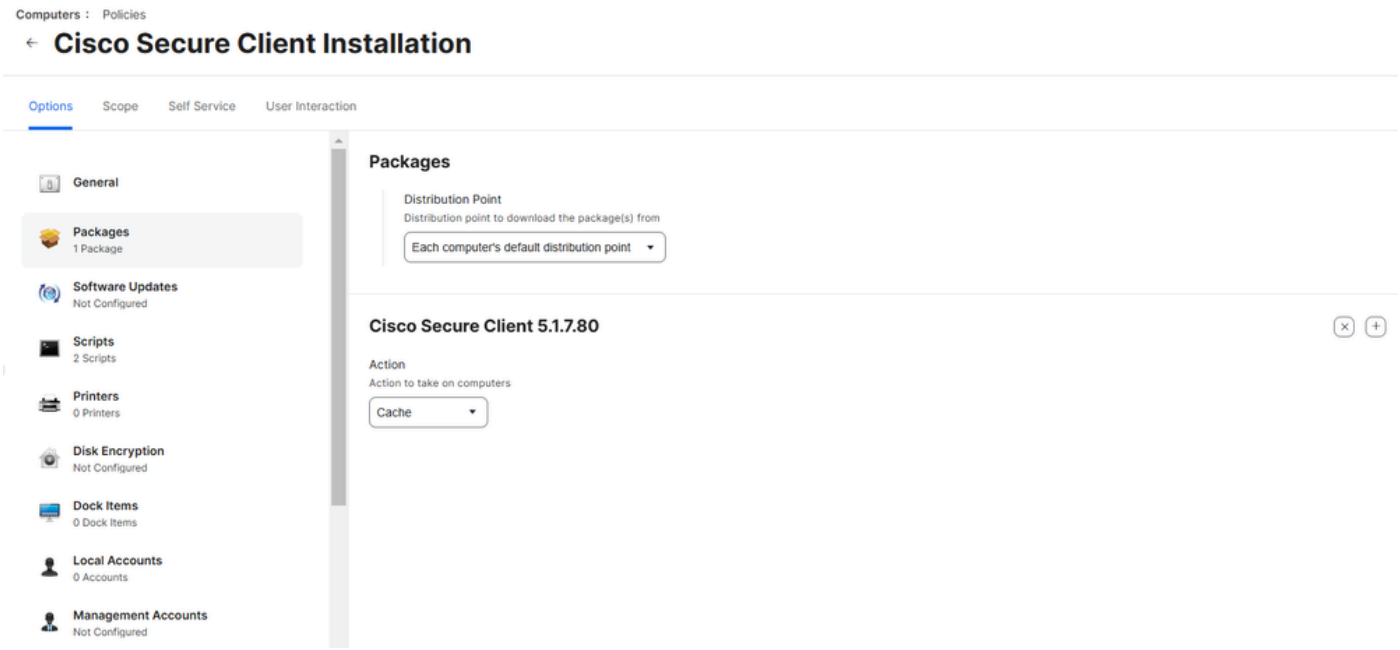
3.（可選）您也可以配置可在「自定義」下執行的自定義命令。用於執行和運行此策略的命令如下所示：

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

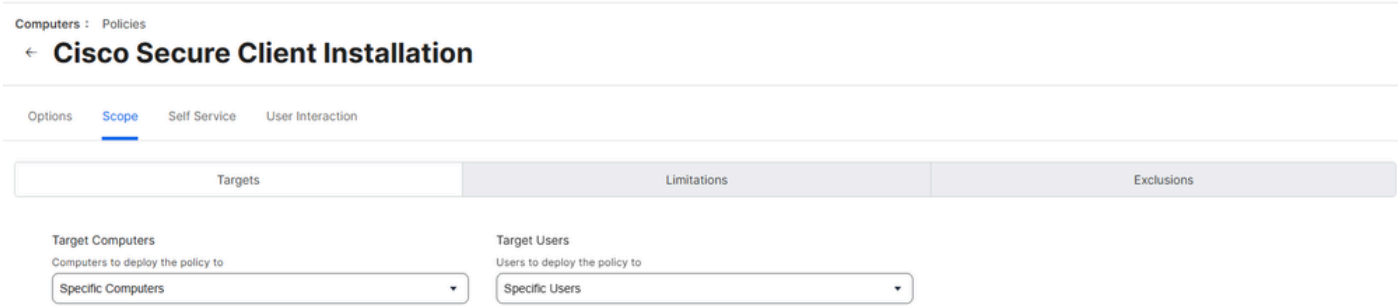


4.選擇Packages > Configure，然後選擇Cisco Secure Client軟體包旁邊的Add。

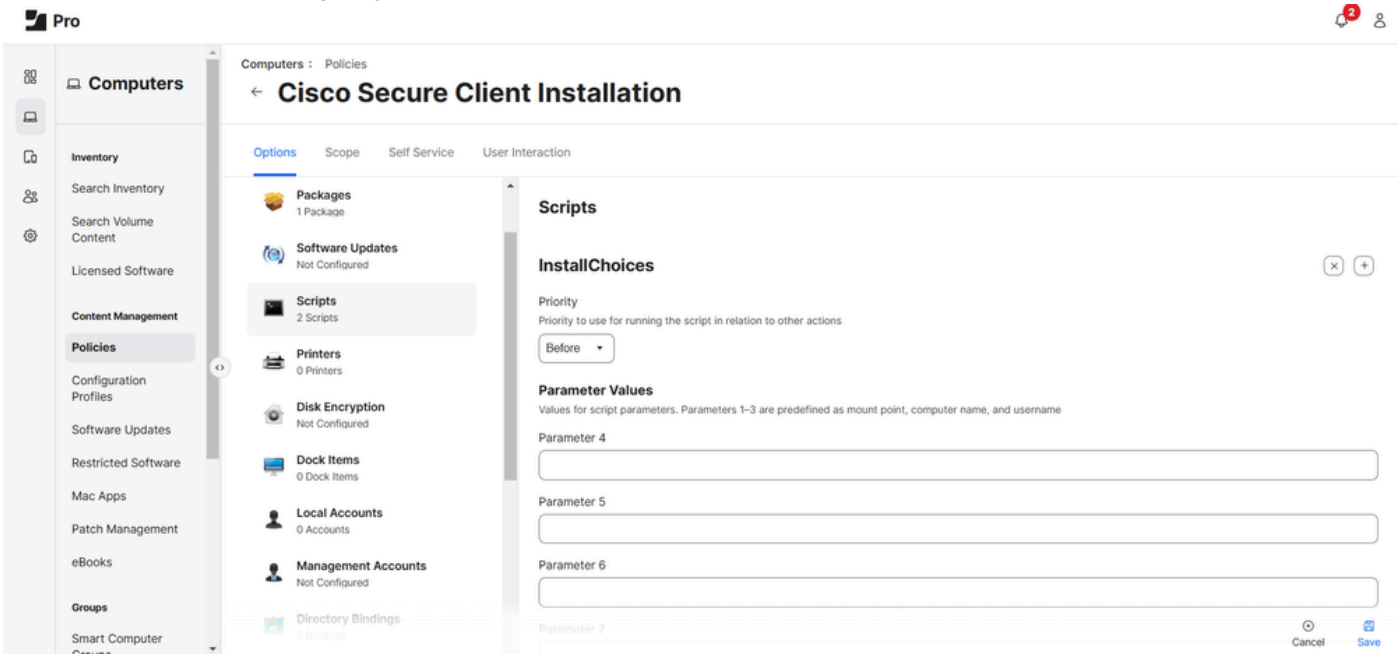
- 在分發點下，選擇每台電腦的預設分發點。
- 在Action下，選擇Cache。

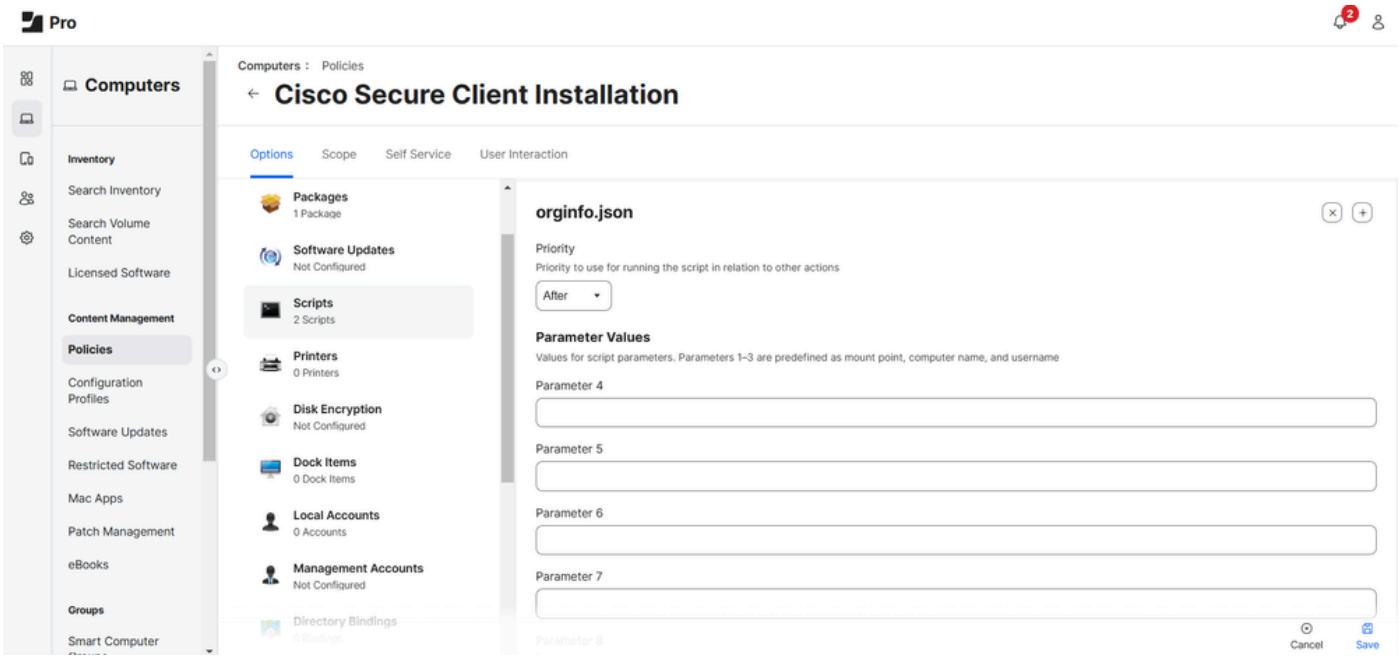


5.定義要部署的裝置或使用者的範圍，然後選擇Save。



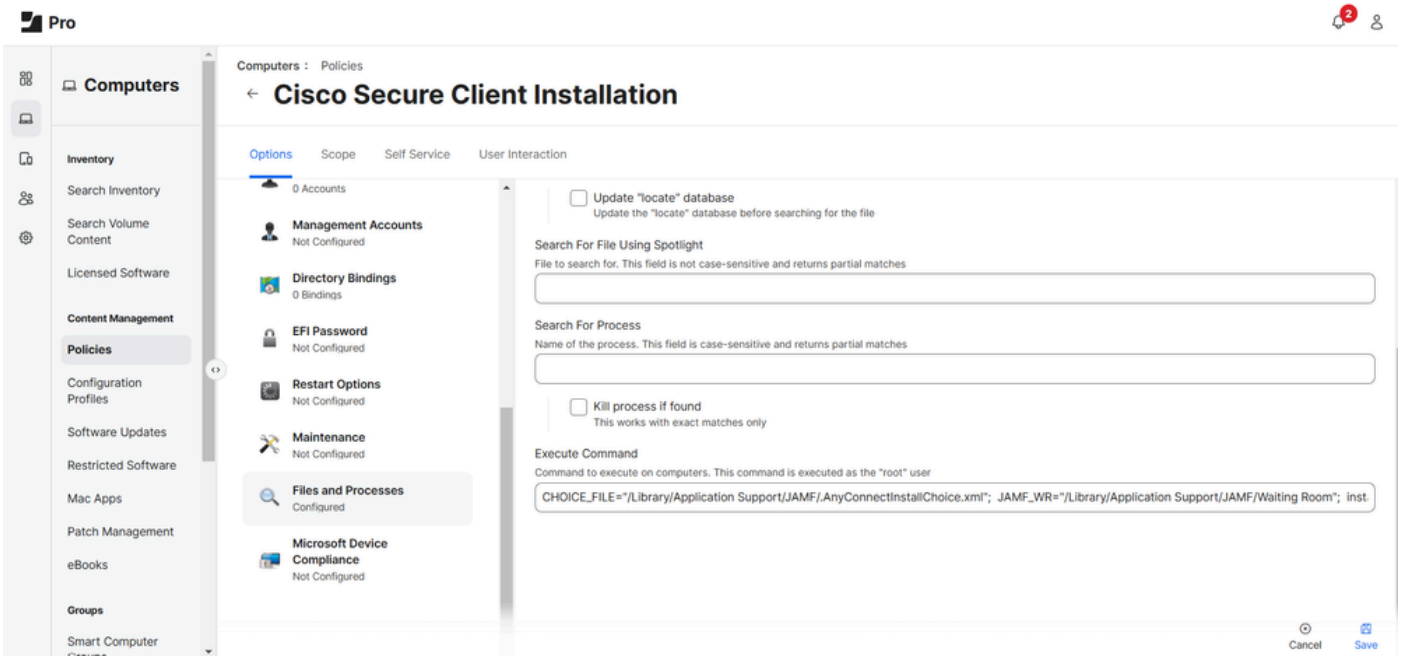
6.新增和InstallChoices腳**orginfo.json** 本，並賦予它們相對於其他操作運行指令碼的優先順序。





7.執行以下命令在裝置上安裝帶有選定模組的Cisco Secure Client軟體包：

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



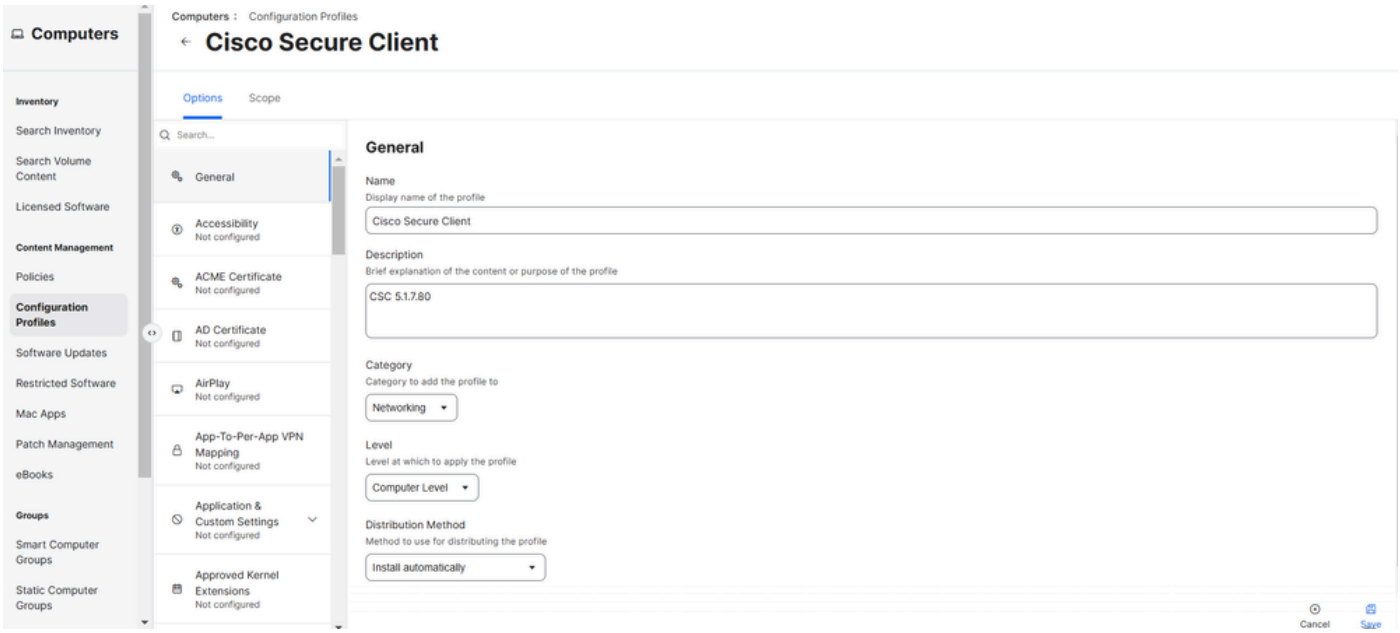
配置無提示安裝系統擴展

接下來，使用JAMF配置並允許Cisco Secure Client所需的系統擴展，以便帶Umbrella模組的Cisco Secure Client能夠正常運行而無需使用者互動。

1.轉至電腦>內容管理>配置檔案>新建。

2.為配置檔案提供一個唯一的名稱，然後選擇Category和Distribution Method。

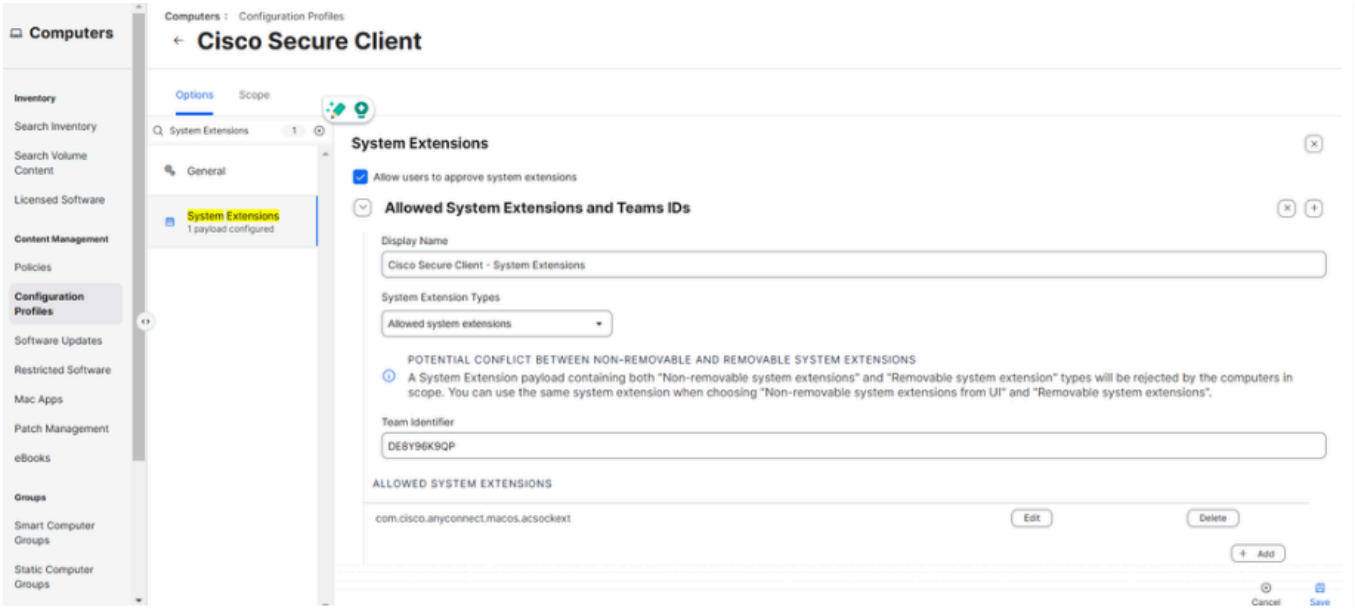
3. EnsureLevel設定為Computer Level。



4.搜尋System Extensions > Configure。輸入以下值：

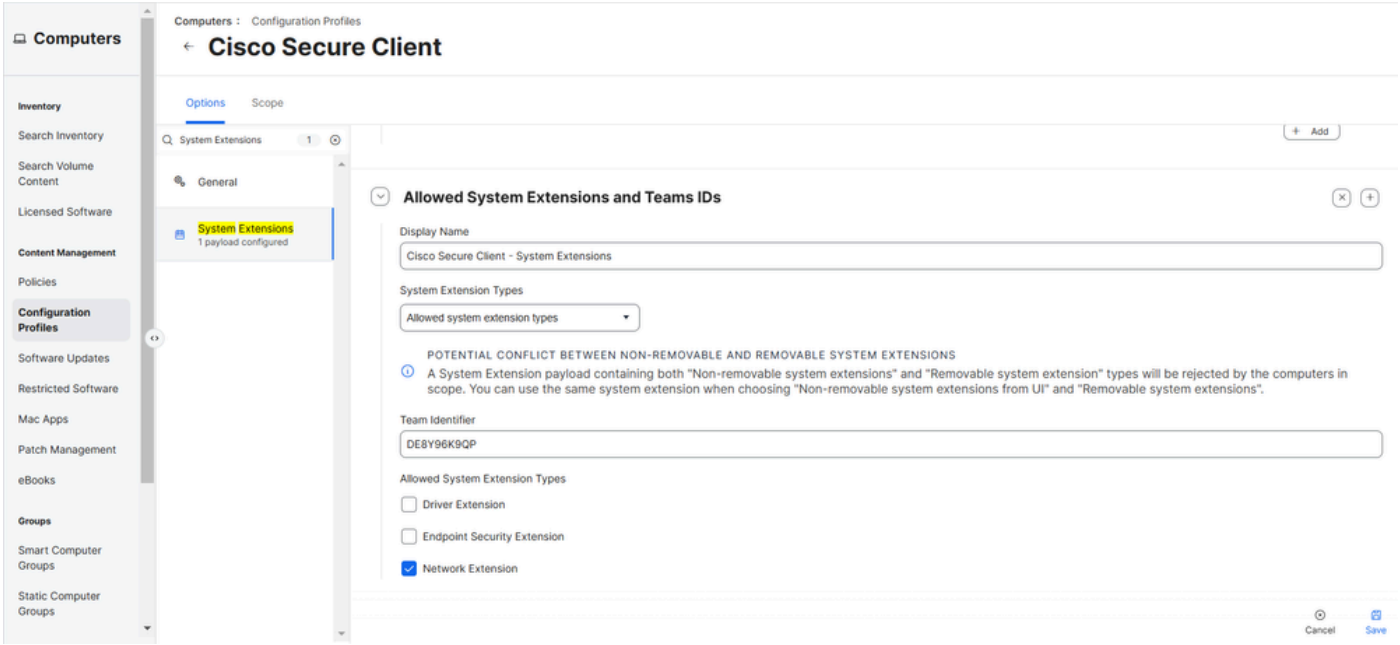
- 顯示名稱：思科安全使用者端 — 系統擴充模組

- 系統擴展型別：允許的系統擴展
- 團隊識別符號：DE8Y96K9QP
- 允許的系統擴展：com.cisco.anyconnect.macos.acsockext，然後選擇Save。



5.選擇Allowed Team IDs and System Extensions旁邊的+圖示以新增另一個System Extension。然後，輸入以下值：

- 顯示名稱：思科安全使用者端 — 系統擴充模組
- 系統擴展型別：允許系統擴展型別
- 團隊識別符號：DE8Y96K9QP
- 允許系統擴展型別：網路延伸



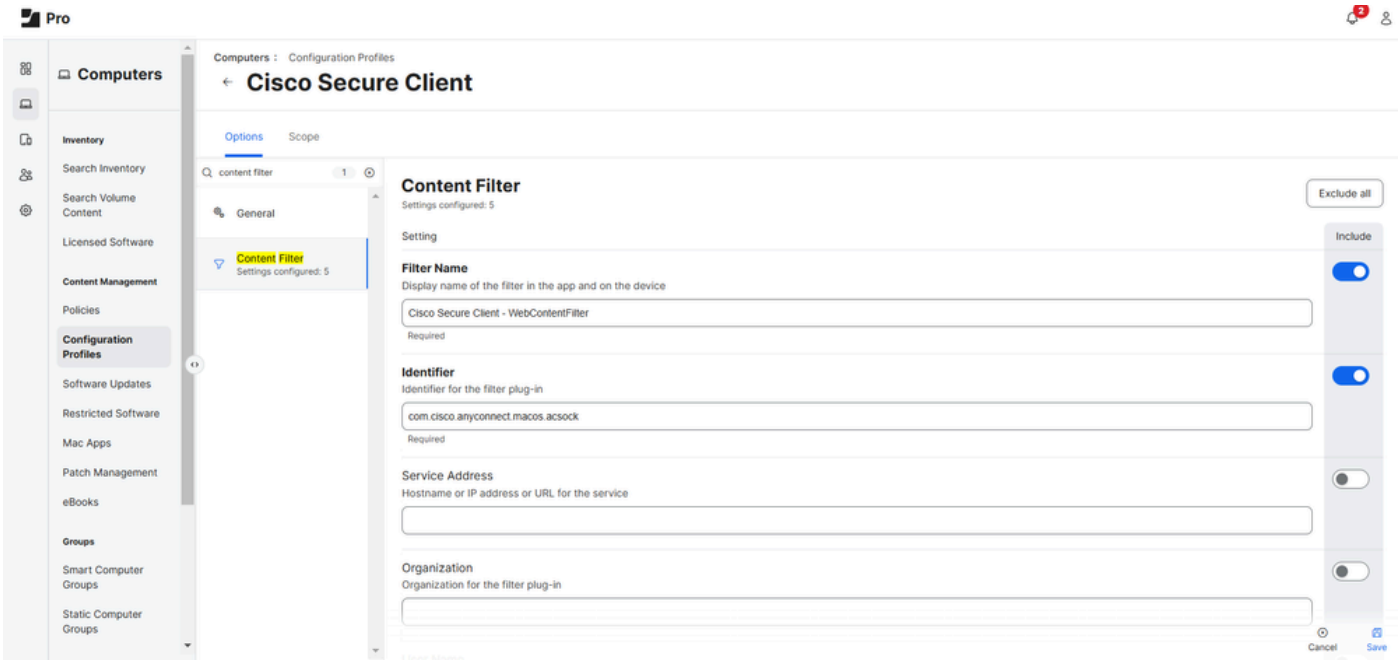
為內容過濾器配置靜默安裝

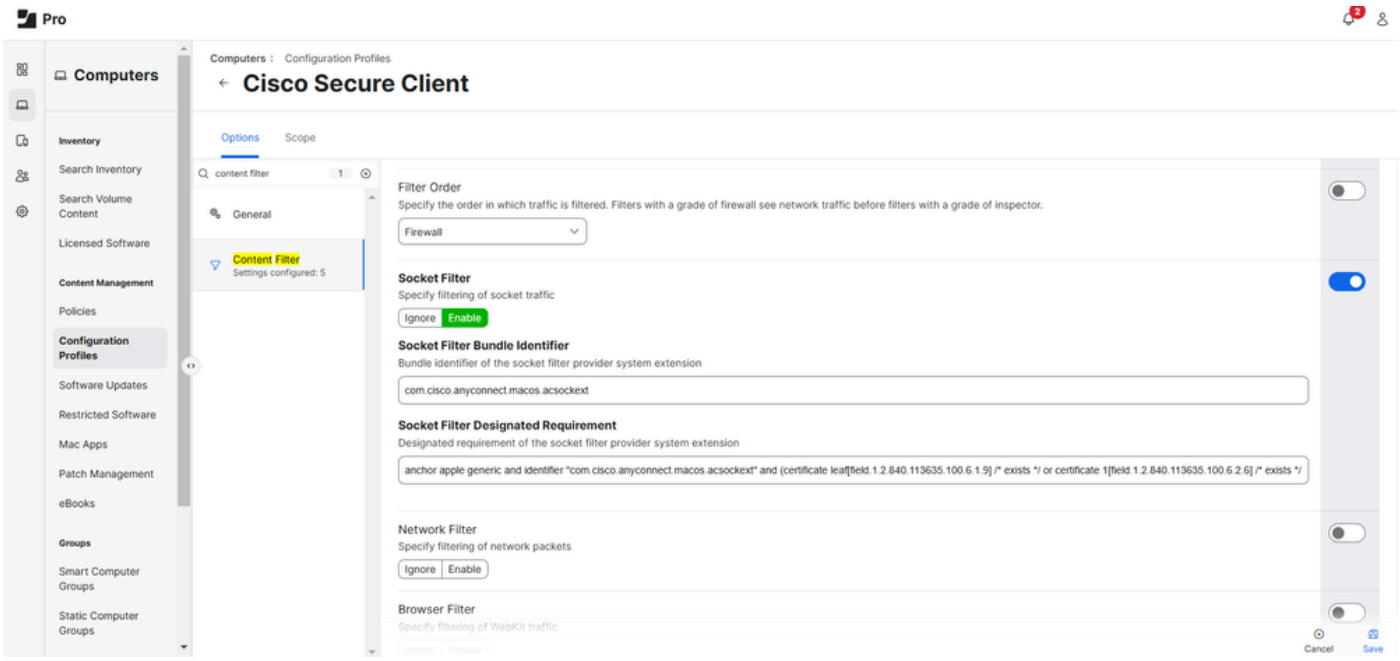
接下來，為內容過濾器配置靜默安裝，它將思科安全客戶端與Umbrella模組的Socket Filter相關聯：

1.搜尋內容篩選器。啟用這些欄位並填寫其各自的值：

- 篩選器名稱：思科安全使用者端 — WebContentFilter
- 識別碼:com.cisco.anyconnect.macos.acsock
- 套接字篩選器：已啟用
- 套接字篩選器捆綁包識別符號：com.cisco.anyconnect.macos.acsockext
- 套接字篩選器指定要求：

  anchor apple generic and identifier "com.cisco.anyconnect.macos.acsockext"和(certificate leaf[field.1.2.840.113635.100.6.1.9] /*存在*/或certificate 1[field.1.2.840.113635.100.6.2.6] /*存在*/和certificate leaf[field.1.2.840.113635.100.6.13] /*存在*/和certificate leaf[subject.OU] = DE8Y96K9QP)





2.在自定義資料下，選擇Add五次，然後輸入以下值：

主要	價值

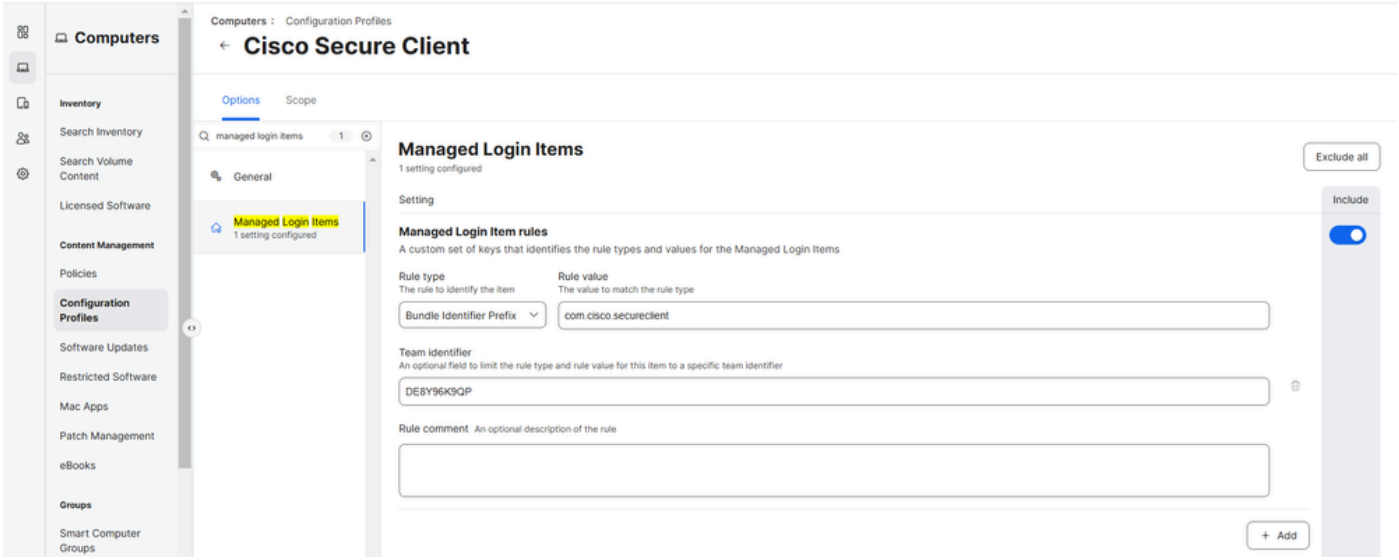
AutoFilterEnabled	假
過濾器瀏覽器	假
FilterSockets	true
過濾資料包	假
篩選等級	防火牆

配置託管登入專案

為帶有Umbrella模組的思科安全客戶端配置託管登入專案可確保思科安全客戶端在裝置啟動時啟動。

要配置，請搜尋託管登入專案，然後使用以下值配置欄位：

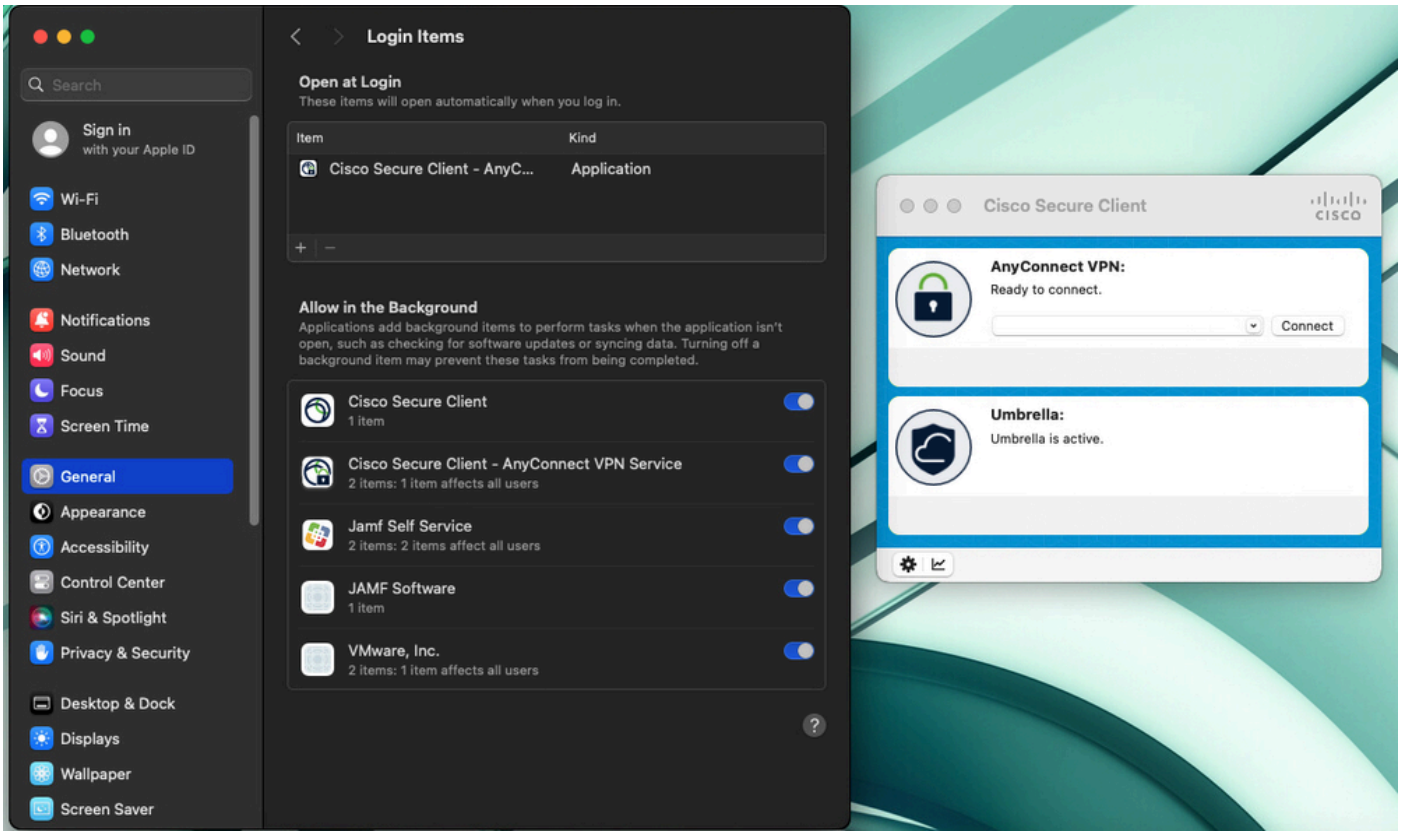
- 規則型別：套件組合識別符首碼
- 規則值：com.cisco.secureclient
- 團隊識別符號：DE8Y96K9QP

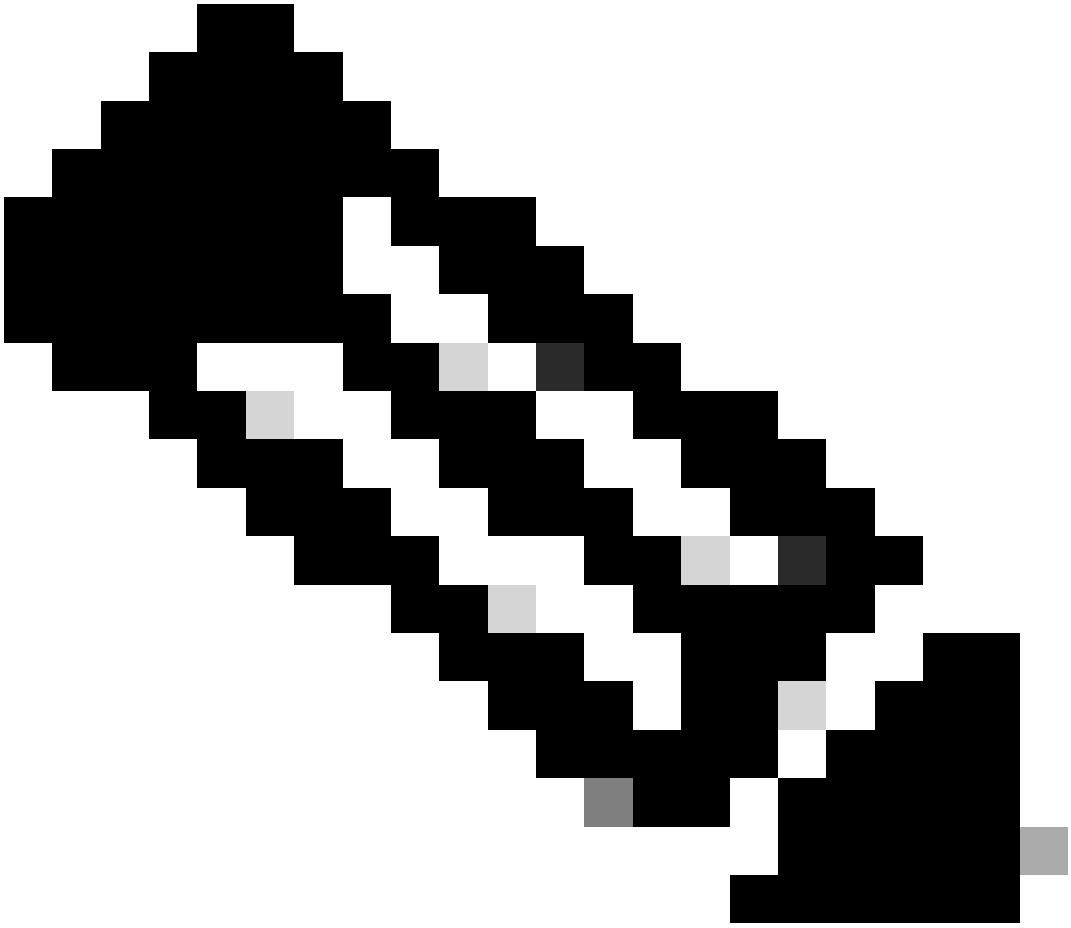


分配範圍和推送部署

1.定位至範圍，然後定義裝置或使用者的範圍。

2.啟用您在建立JAMF策略的步驟2中配置的一個觸發器時，可以將Cisco Secure Client with Umbrella模組推出到所需的macOS裝置。或者，您也可以通過JAMF的自助服務門戶推送此內容。


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.



附註：即使使用者嘗試在「系統設定」(Network > Filter)中停用DNS代理或透明代理，也會因為內容過濾器已透過本文所述的JAMF啟用且無法停用，而預設自動重新啟用該代理。

配置macOS防火牆例外

如果macOS防火牆設定為阻止所有傳入連線，還必須將Cisco安全客戶端及其元件新增到其例外清單中：

1.導覽至電腦>內容管理>配置檔案。

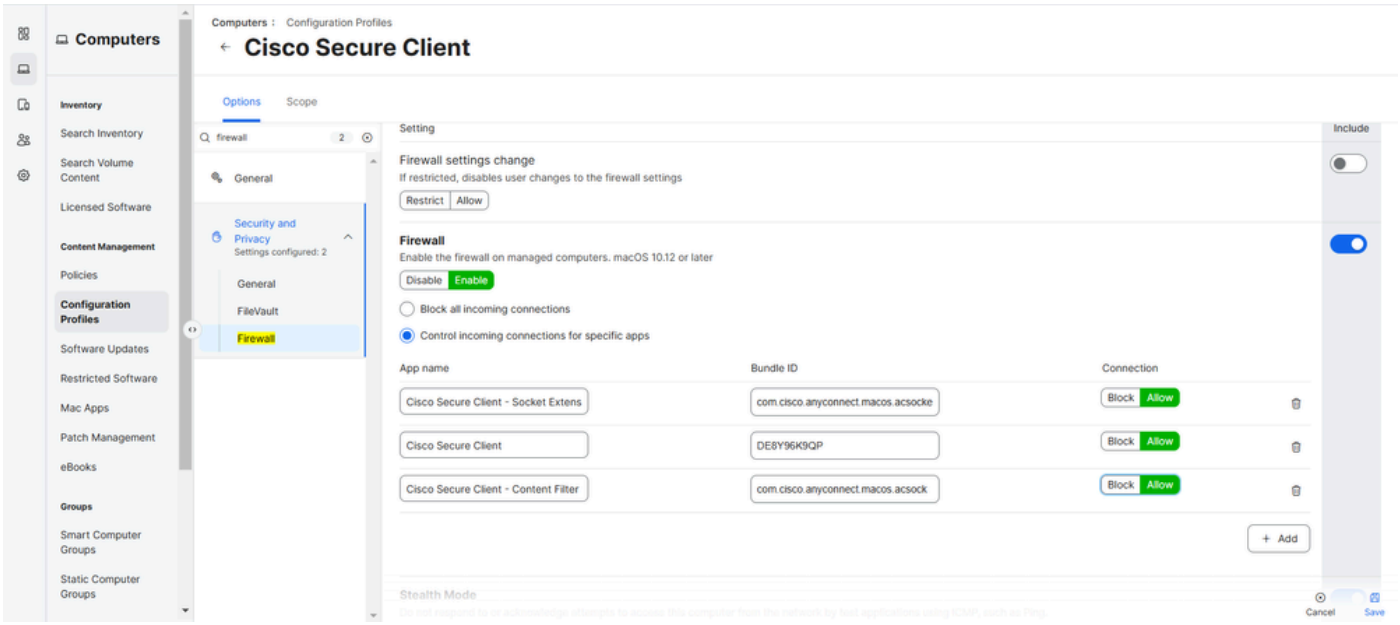
2.選擇您的Cisco Secure Client配置檔案並找到Security and Privacy。

3.使用以下設定進行配置：

- 防火牆：啟用 — 控制特定應用的傳入連線

應用程式名稱	套件組合ID
思科安全使用者端 — 通訊端擴充模組	com.cisco.anyconnect.macos.acsockext

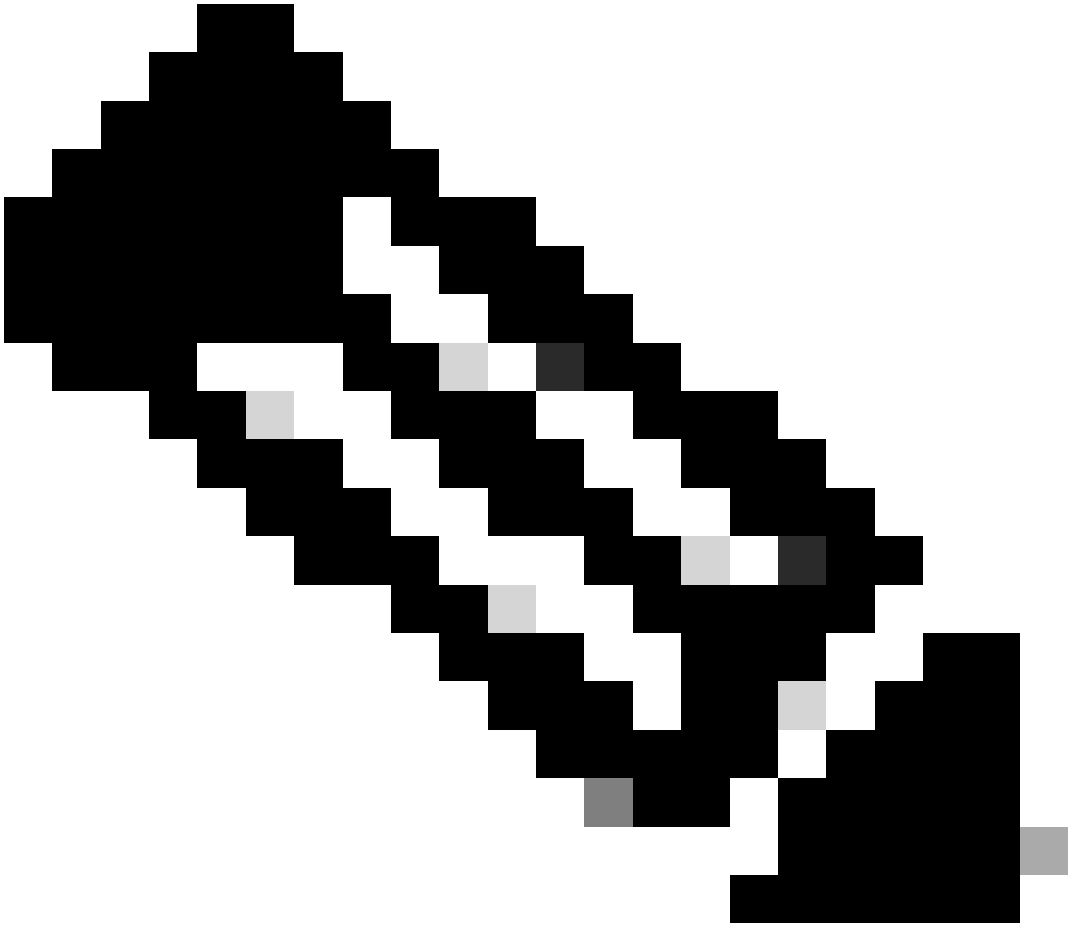
思科安全使用者端	DE8Y96K9QP
思科安全使用者端 — 內容過濾器	com.cisco.anyconnect.macos.acsock



4.選擇儲存。

5.如果系統提示您輸入Redistribution Options，請選擇Distribute to All立即將更改推送到所需的macOS裝置。

部署思科Umbrella根證書



附註：此步驟僅適用於新部署的思科安全客戶端或以前未部署思科Umbrella根證書的裝置。如果您正在從Umbrella漫遊客戶端或Cisco AnyConnect 4.10客戶端進行遷移，並且/或者以前已經部署了思科Umbrella根證書，則可以跳過此部分。

從Umbrella控制面板中的Policies > Root Certificate下載Cisco Umbrella Root Certificate。

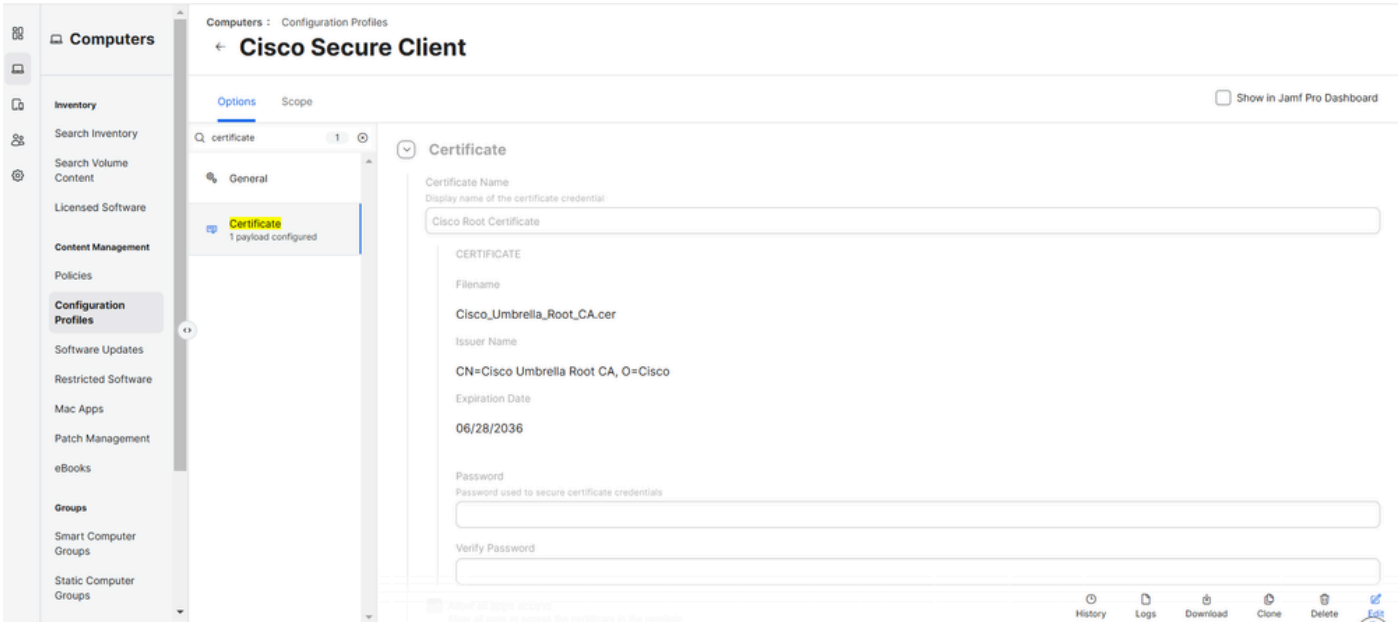
1.在Policies > Root Certificate下的Umbrella控制面板中，下載Cisco Umbrella Root Certificate。

2.在JAMF中，導航到電腦>配置檔案> Cisco安全客戶端>編輯。

3.搜尋Certificate > Configure。為其指定唯一的名稱。

4.在Select Certificate Option下，選擇Upload並上傳先前在第1步中下載的Cisco Umbrella根證書。

5.確保未在此處配置口令，然後選擇Save。



6.如果系統提示您輸入Redistribution Options，請選擇Distribute to All以立即將更改推送到所需的macOS裝置。

驗證

要驗證帶有Umbrella模組的Cisco Secure Client是否正常工作，請瀏覽到https://policy-debug.checkumbrella.com或運行此命令：

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

任一輸出都必須包含與Umbrella組織相關的獨特資訊，如您的OrgID。

MacOS 14.3的解決方法

對於使用Cisco Secure Client 5.1.x的MacOS 14.3（或更高版本），如果您遇到「VPN客戶端代理無法建立進程間通訊倉庫」：

1.在JAMF中，導航到設定>電腦管理>指令碼>新建。

2.為其指定一個唯一的名稱並定義類別。

3.定位至「指令碼」標籤，然後新增以下內容：

```
#!/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.在選項下，確保優先順序設定為之後。此bash指令碼通過從`pgrep -fl`返回進程ID的預期輸出來檢查Cisco Secure Client - AnyConnect VPN service.app是否正在運行。

- 如果返回空輸出，則可以確認`Cisco Secure Client - AnyConnect VPN service.app`未運行，且指令碼將執行以啟動Umbrella模組正常運行所需的思科安全客戶端核心服務。

自動更新

思科已決定從Umbrella控制面板擴展自動更新支援，以包括從Secure Client 5.1.6.103(MR6)開始的安全客戶端。 今後，如果已在Umbrella控制面板中配置了自動更新，則至少已升級到思科安全客戶端5.1.6 MR6的客戶可以自動更新到較新的版本。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。