Umbrella 모듈과 함께 JAMF를 사용하여 macOS에 CSC 구축

목차

소개

이 문서에서는 Umbrella 모듈과 함께 Cisco Secure Client를 JAMF를 사용하여 관리되는 macOS 디바이스에 구축하는 방법에 대해 설명합니다.

사전 요구 사항

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

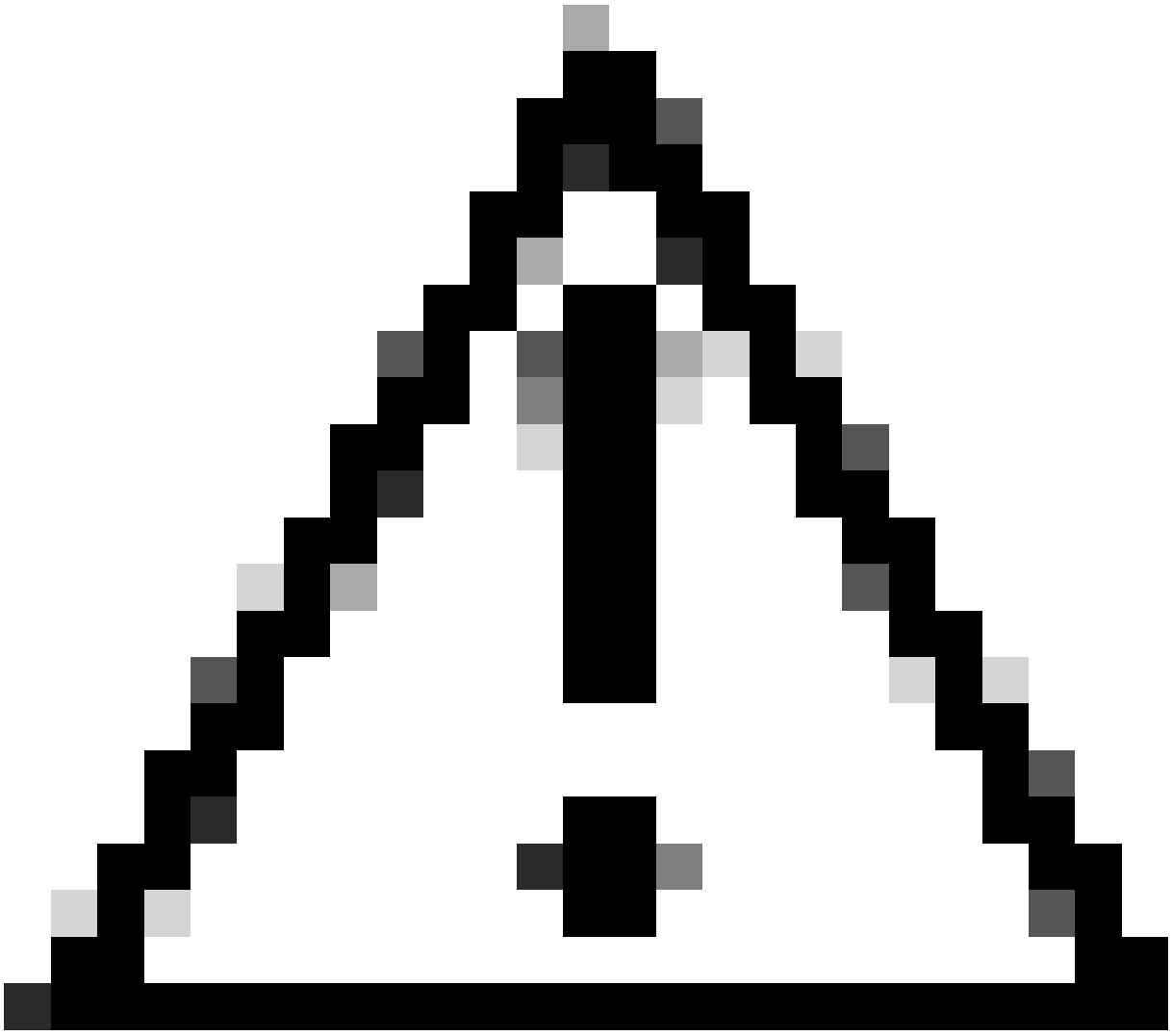
- macOS 디바이스는 JAMF에서 관리해야 합니다.
- macOS에 대한 MDM 등록 지침은 JAMF 설명서를 참조하십시오.

사용되는 구성 요소

이 문서의 정보는 Cisco Secure Client를 기반으로 합니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든

명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.



주의: 이 문서는 2025년 2월 1일자로 제공됩니다. Cisco Umbrella Support는 이러한 지침이 이 날짜 이후에 유효하다고 보장하지 않으며 JAMF 및 Apple의 업데이트에 따라 변경될 수 있습니다.

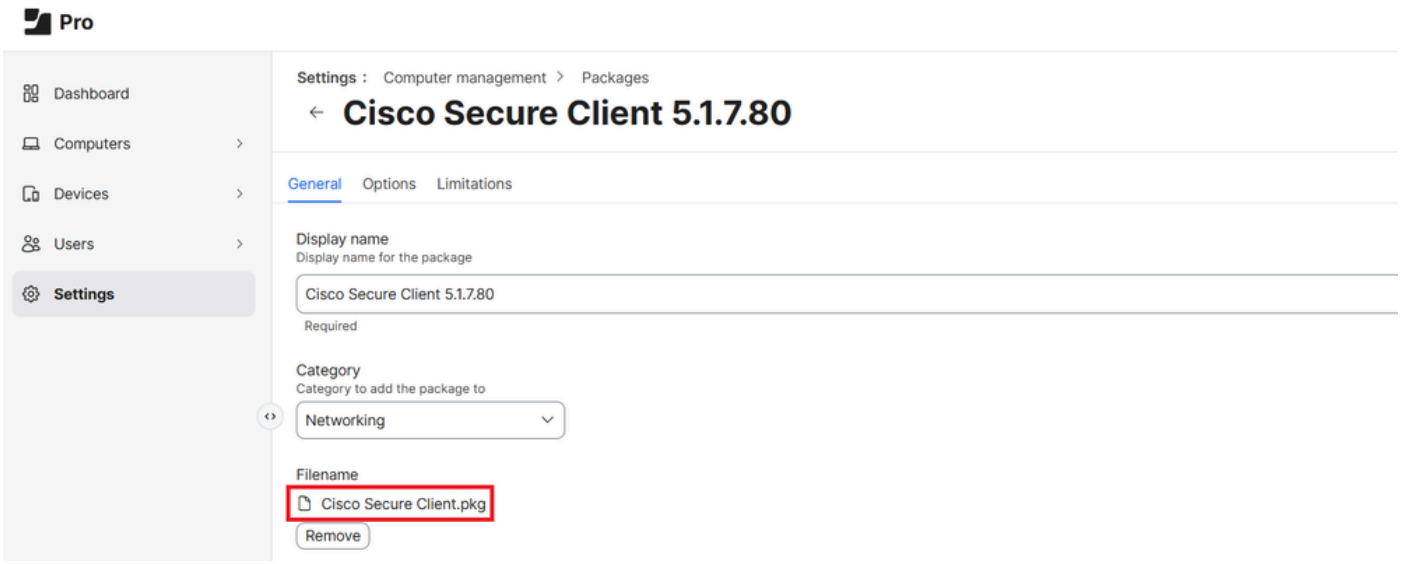
설치 패키지(PKG) 업로드

1. Umbrella 대시보드에서 Deployments(구축) > Roaming Computers(로밍 컴퓨터) > Roaming Client(로밍 클라이언트) > Pre-Deployment Package(사전 구축 패키지) > macOS 아래의 Cisco Secure Client DMG를 다운로드합니다.

2. JAMF Pro 클라우드 인스턴스에 로그인합니다.

3. 설정 > 컴퓨터 관리 > 패키지 > 새로 만들기로 이동합니다.

4. Umbrella 대시보드에서 다운로드한 DMG 패키지에서 추출된 PKG를 업로드합니다.

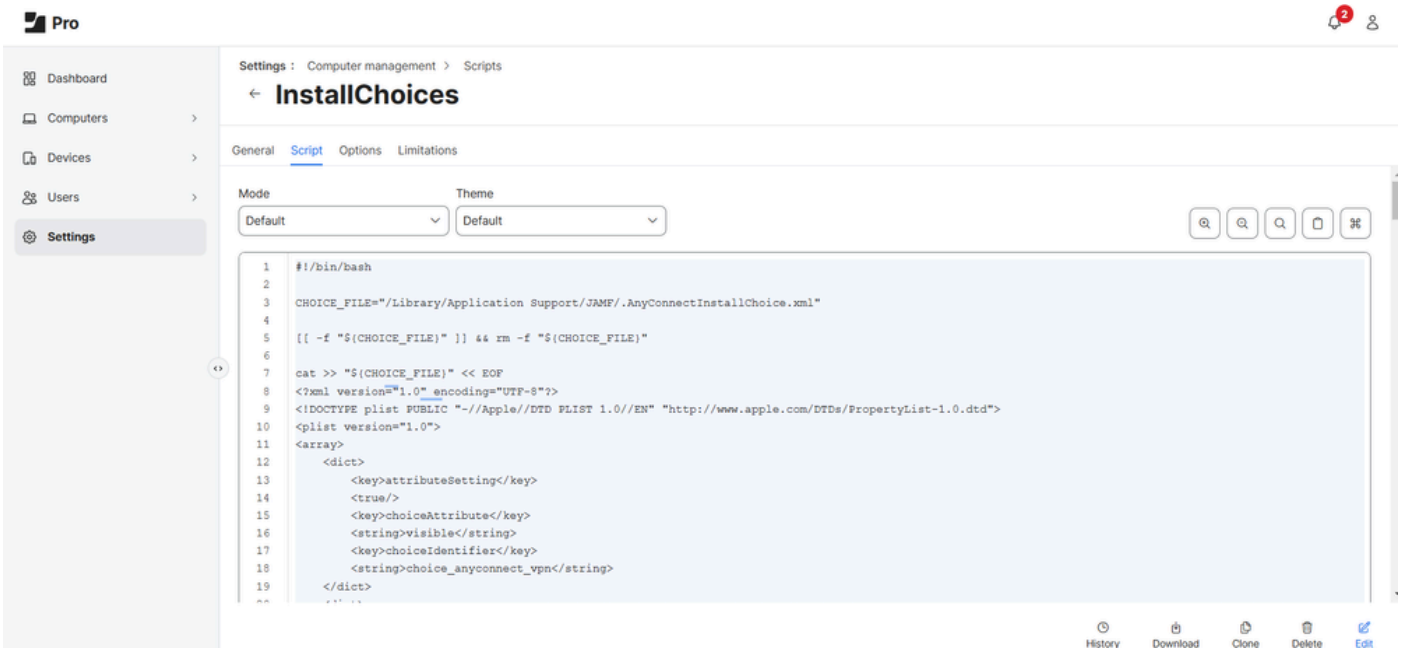


구성 및 모듈 선택 스크립트 추가

1. 설정 > 컴퓨터 관리 > 스크립트로 이동하여 배포 중에 설치되는 모듈을 제어하기 위해 이 스크립트를 추가합니다.

2. 모듈을 0으로 설정하여 모듈을 건너뛰거나 1로 설정하여 Secure Client 모듈의 설치를 제어할 수 있습니다. PKG가 기본적으로 모든 모듈을 설치하도록 구성되어 있기 때문입니다.

- Umbrella 설명서: Cisco Secure Client의 macOS 설치 사용자 정의에서 샘플 XML 파일을 가져올 수 있습니다
- 또한 Umbrella는 이 github 링크에 "installchoices" 스크립트를 추가했습니다. 이 예에서 Core VPN, Umbrella 및 DART 모듈은 1로 설정되며 Secure Client 설치에 포함될 수 있습니다.



3. Settings(설정) > Computer management(컴퓨터 관리) > Scripts(스크립트)로 이동하여 Cisco Secure Client에 필요한 구성 파일 `Orginfo.json`을 생성하도록 이 스크립트를 추가합니다.

- Umbrella 대시보드에서 모듈 프로파일을 직접 다운로드한 다음 스크립트에 Organization ID, Fingerprint 및 User ID를 추가합니다.

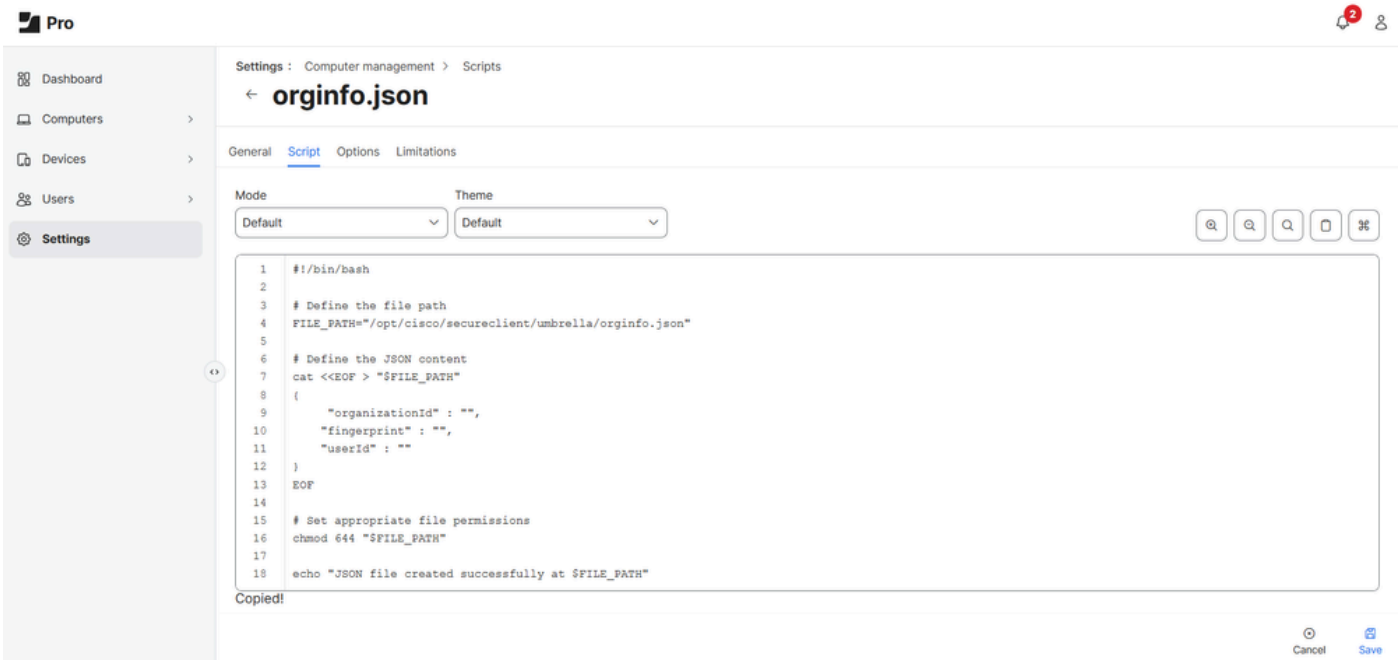
```
#!/bin/bash

# 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

JAMF 정책 생성

JAMF 정책은 Cisco Secure Client with Umbrella 모듈이 푸시되는 방법과 시기를 결정하는 데 사용됩니다.

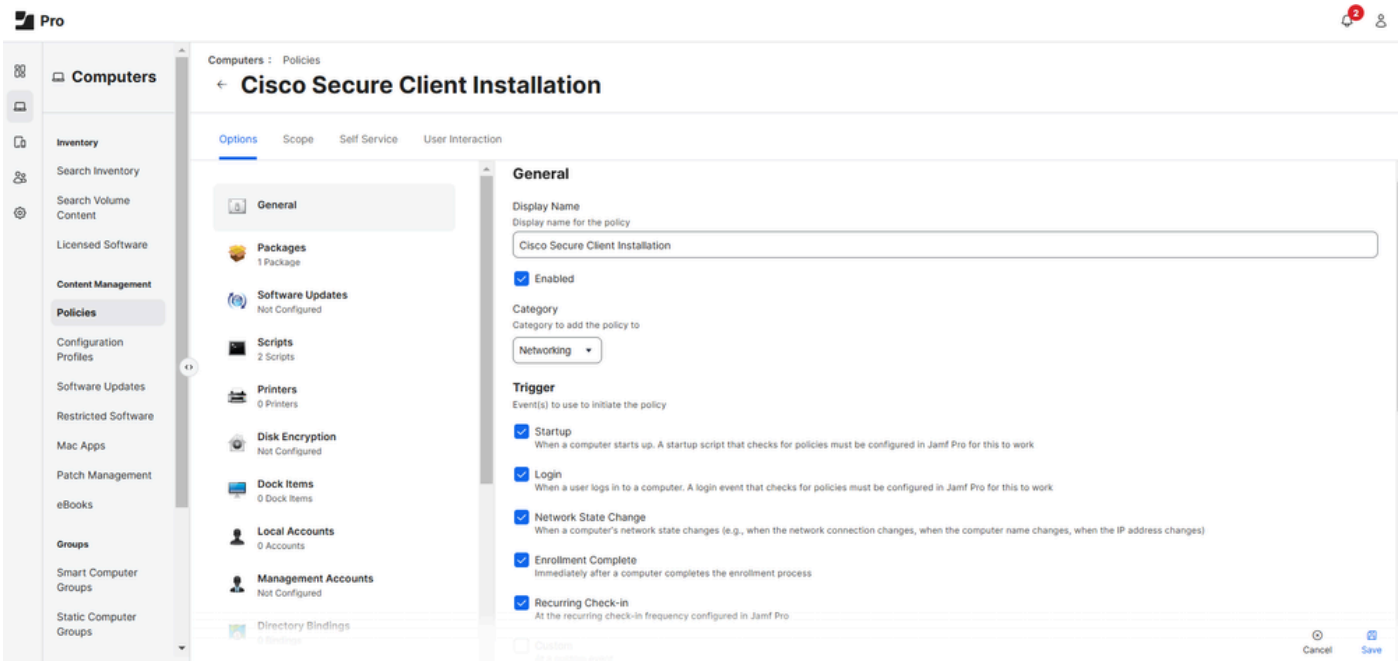
1. 컴퓨터 > 콘텐츠 관리 > 정책 > 새로 만들기로 이동합니다.

2. 정책에 고유한 이름을 지정하고 원하는 범주 및 트리거 이벤트를 선택합니다(예: 이 정책이 실행

되는 경우).

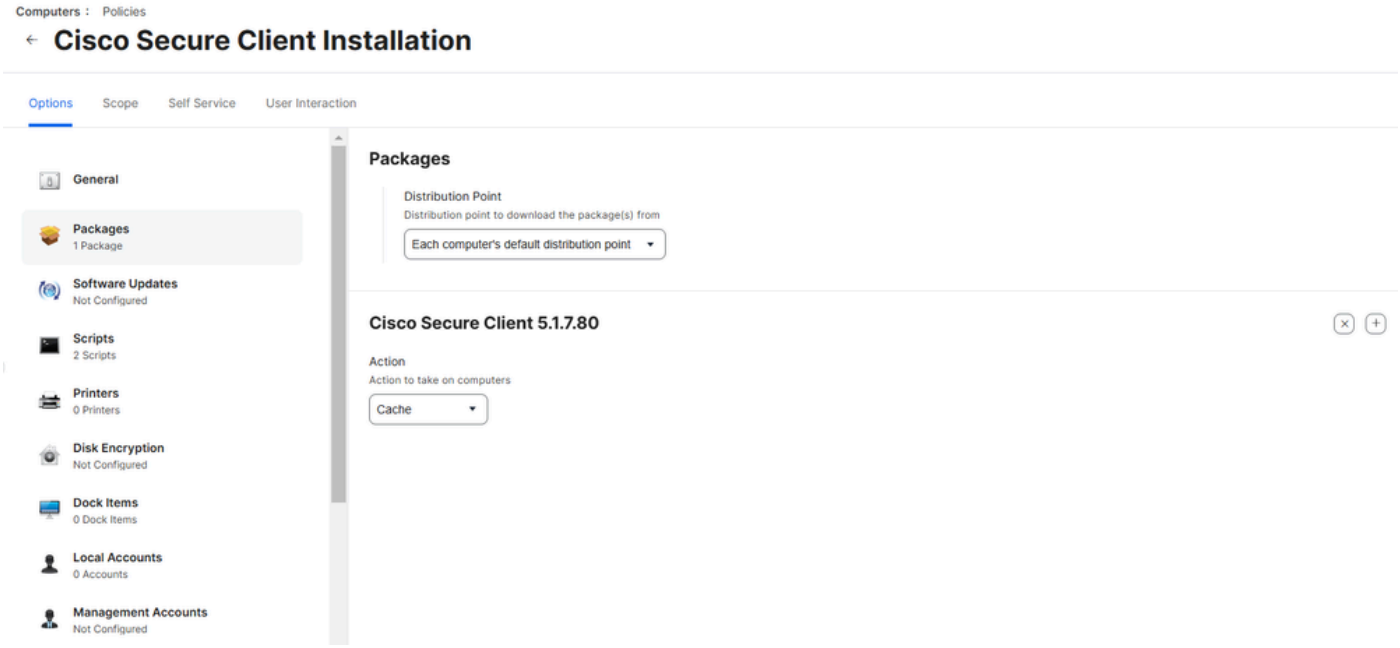
3. 선택적으로, Custom(사용자 지정)에서 실행할 수 있는 사용자 지정 명령을 구성할 수도 있습니다. 이 정책을 실행 및 실행하는 명령은 다음과 같습니다.

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

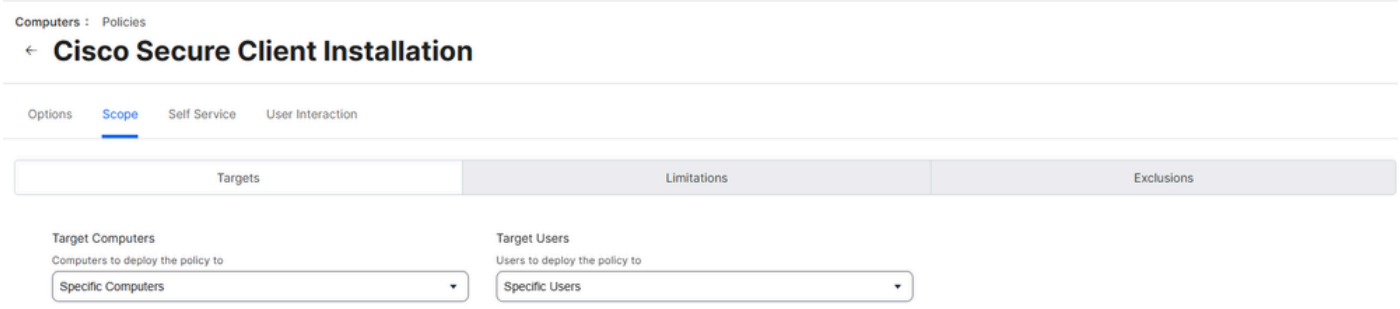


4. Packages(패키지) > Configure(구성)를 선택하고 Cisco Secure Client 패키지 옆에 있는 Add(추가)를 선택합니다.

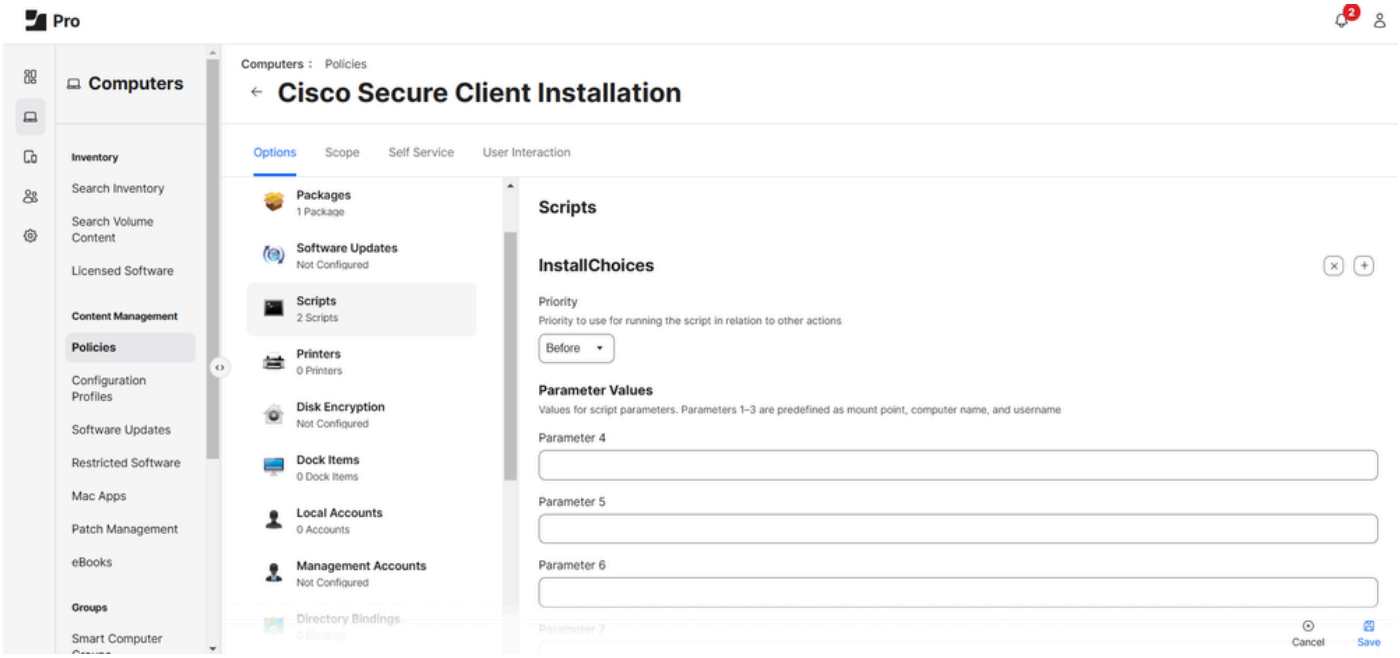
- 배포 지점 아래에서 각 컴퓨터의 기본 배포 지점을 선택합니다.
- Action(작업) 아래에서 Cache(캐시)를 선택합니다.

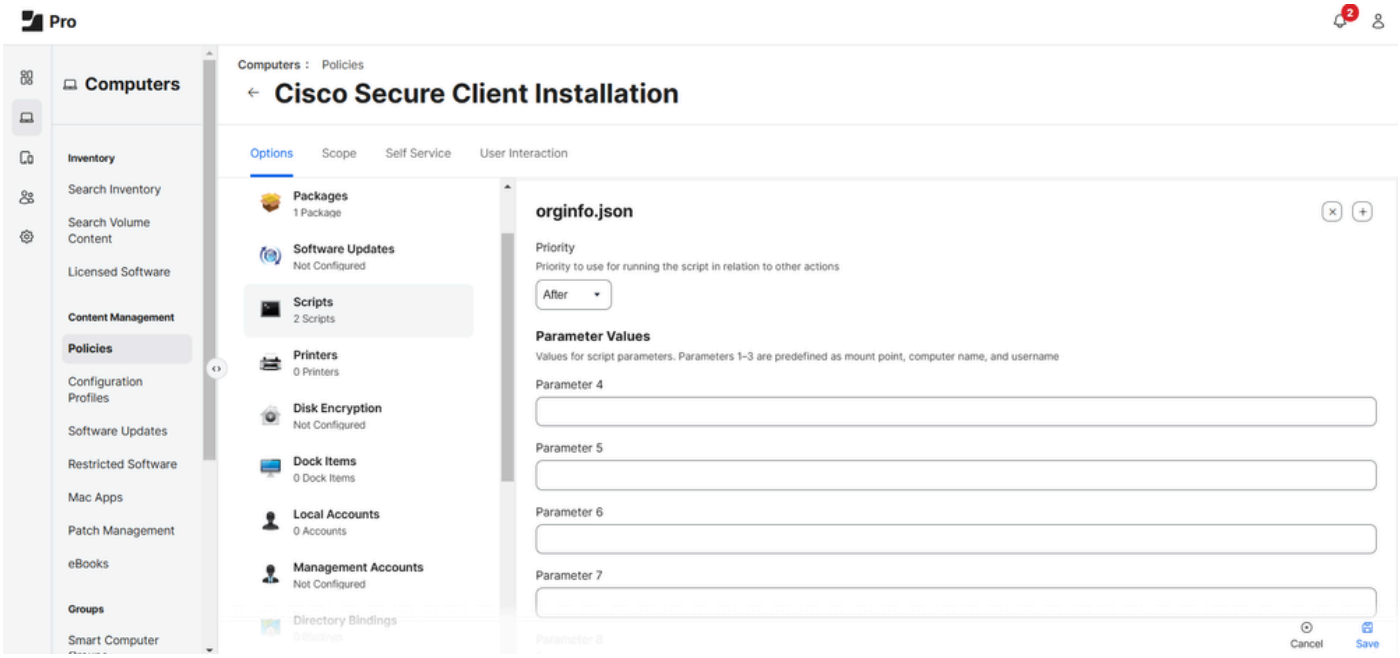


5. 배포할 장치 또는 사용자의 범위를 정의하고 저장을 선택합니다.



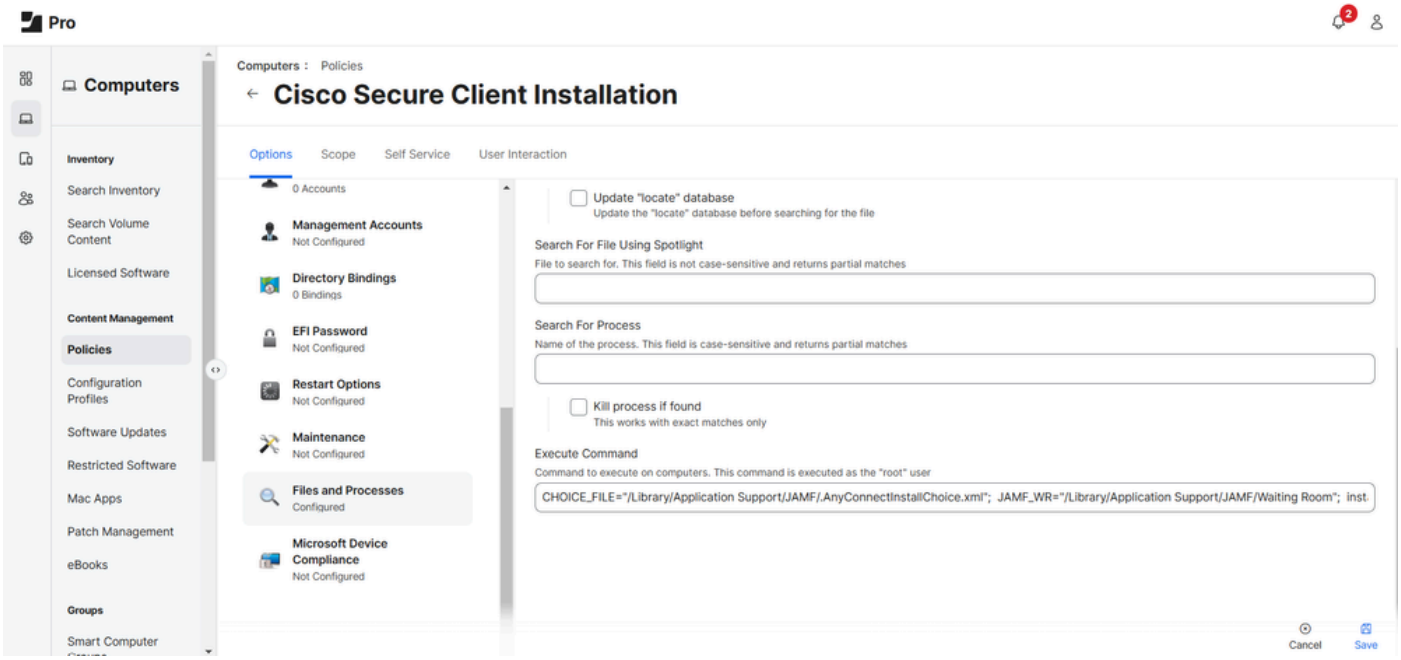
6.InstallChoices 및 **orginfo.json** 스크립트를 모두 추가하고 다른 작업과 관련하여 스크립트를 실행하는 데 사용할 수 있는 우선 순위를 지정합니다.





7. 이 명령을 실행하여 선택한 모듈이 있는 Cisco Secure Client 패키지를 장치에 설치합니다.

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



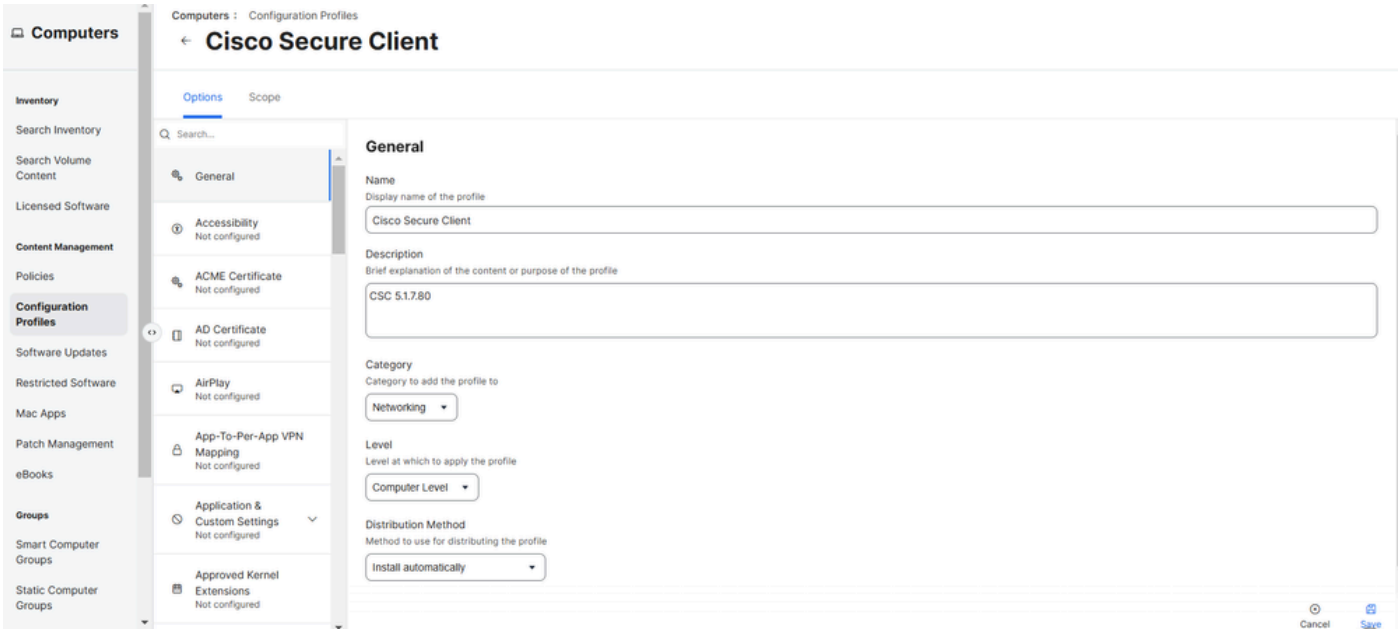
시스템 확장의 자동 설치 구성

그런 다음 JAMF를 사용하여 Umbrella 모듈이 포함된 Cisco Secure Client가 사용자 상호 작용 없이 올바르게 실행되도록 Cisco Secure Client의 필수 시스템 확장을 구성하고 허용합니다.

1. 컴퓨터 > 콘텐츠 관리 > 구성 프로필 > 새로 만들기로 이동합니다.

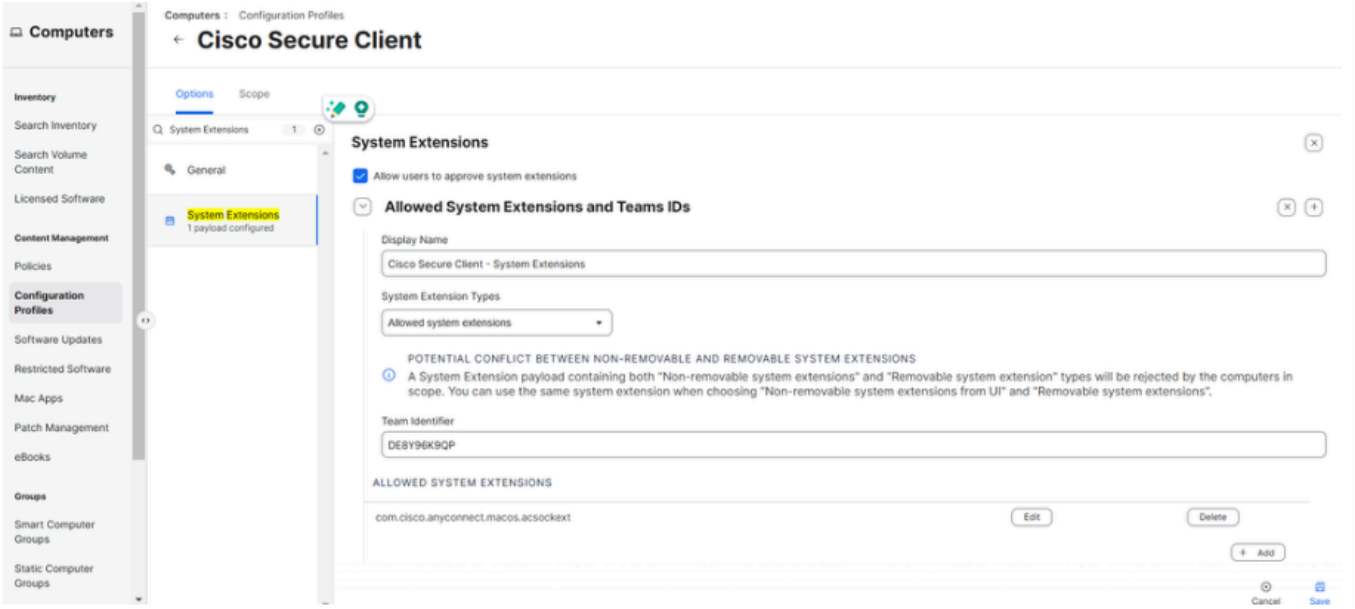
2. 프로파일에 고유한 이름을 지정하고 범주 및 분배 방법을 선택합니다.

3. Level이 컴퓨터 수준으로 설정되었는지 확인합니다.



4. 시스템 확장 > 구성을 검색합니다. 다음 값을 입력합니다.

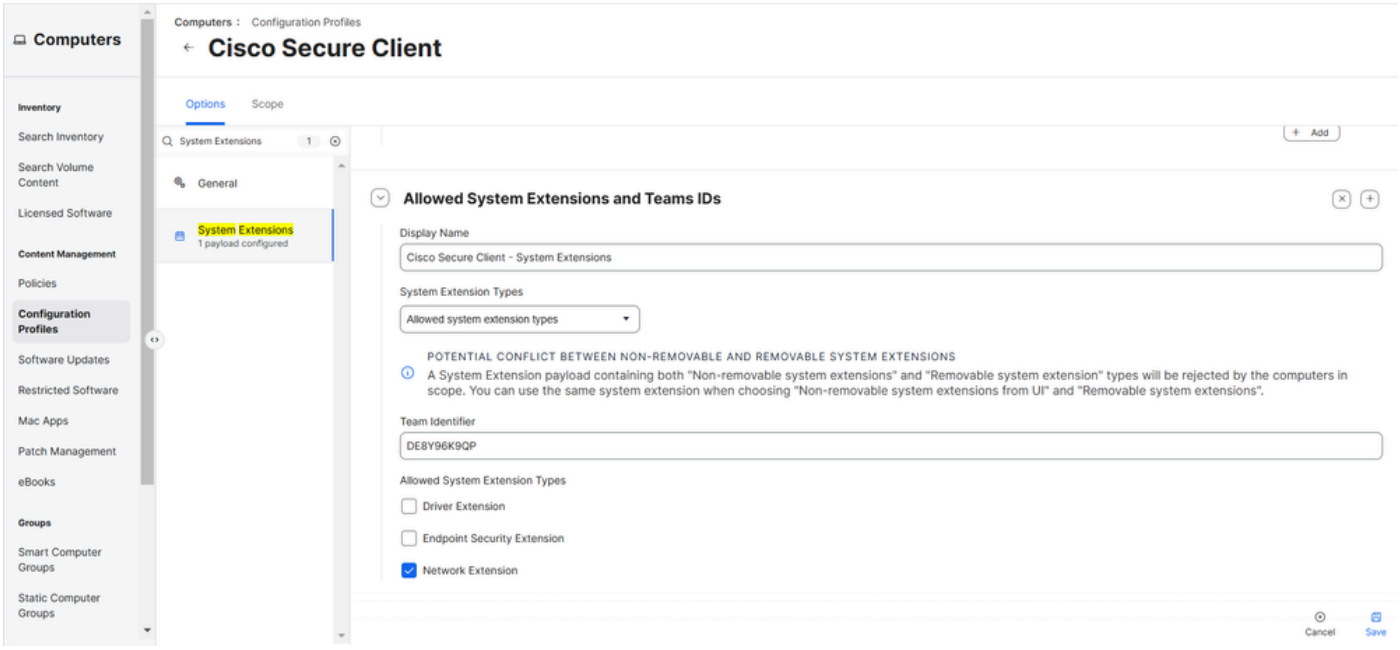
- 표시 이름: Cisco Secure Client - 시스템 확장
- 시스템 확장 유형: 허용된 시스템 확장
- 팀 식별자: DE8Y96K9QP
- 허용된 시스템 확장: com.cisco.anyconnect.macos.acsockext를 선택한 다음 Save를 선택합니다.



5. 다른 시스템 확장을 추가하려면 허용된 팀 ID 및 시스템 확장 옆에 있는 + 아이콘을 선택합니다. 그런 다음 다음 다음 값을 입력합니다.

- 표시 이름: Cisco Secure Client - 시스템 확장
- 시스템 확장 유형: 시스템 확장 유형 허용

- 팀 식별자: DE8Y96K9QP
- 시스템 확장 유형 허용: 네트워크 확장



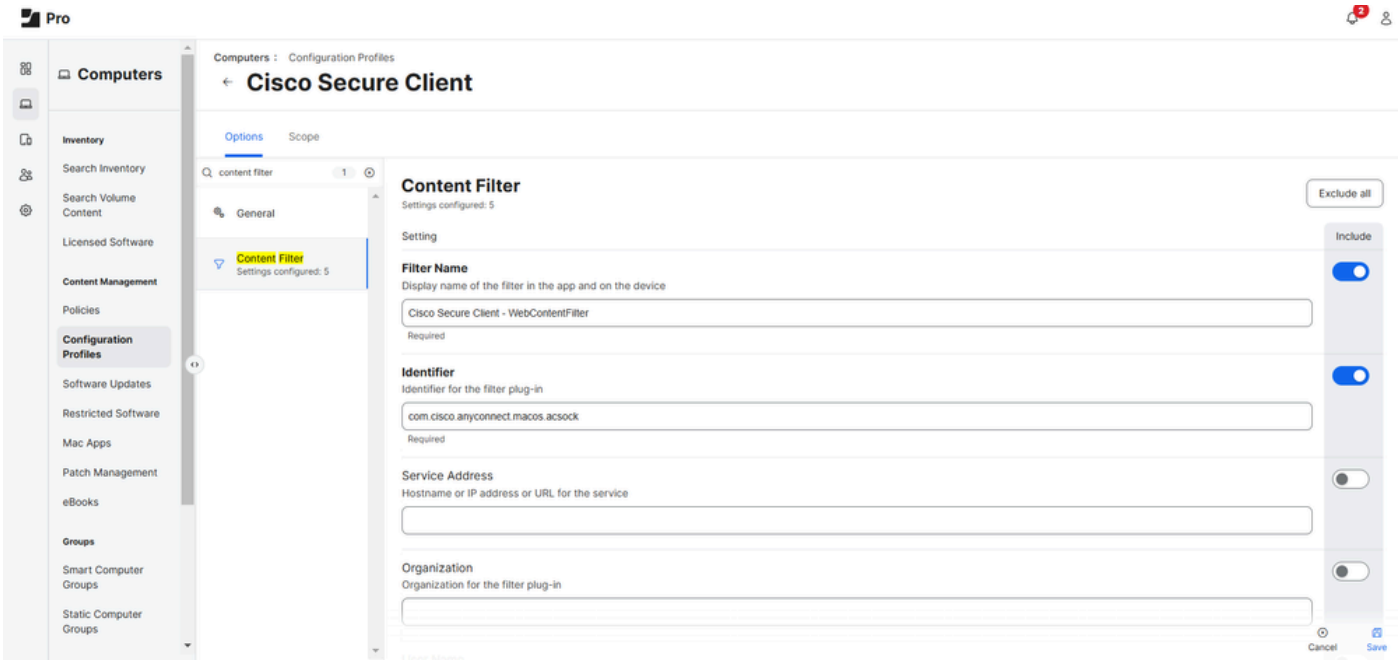
콘텐츠 필터에 대한 자동 설치 구성

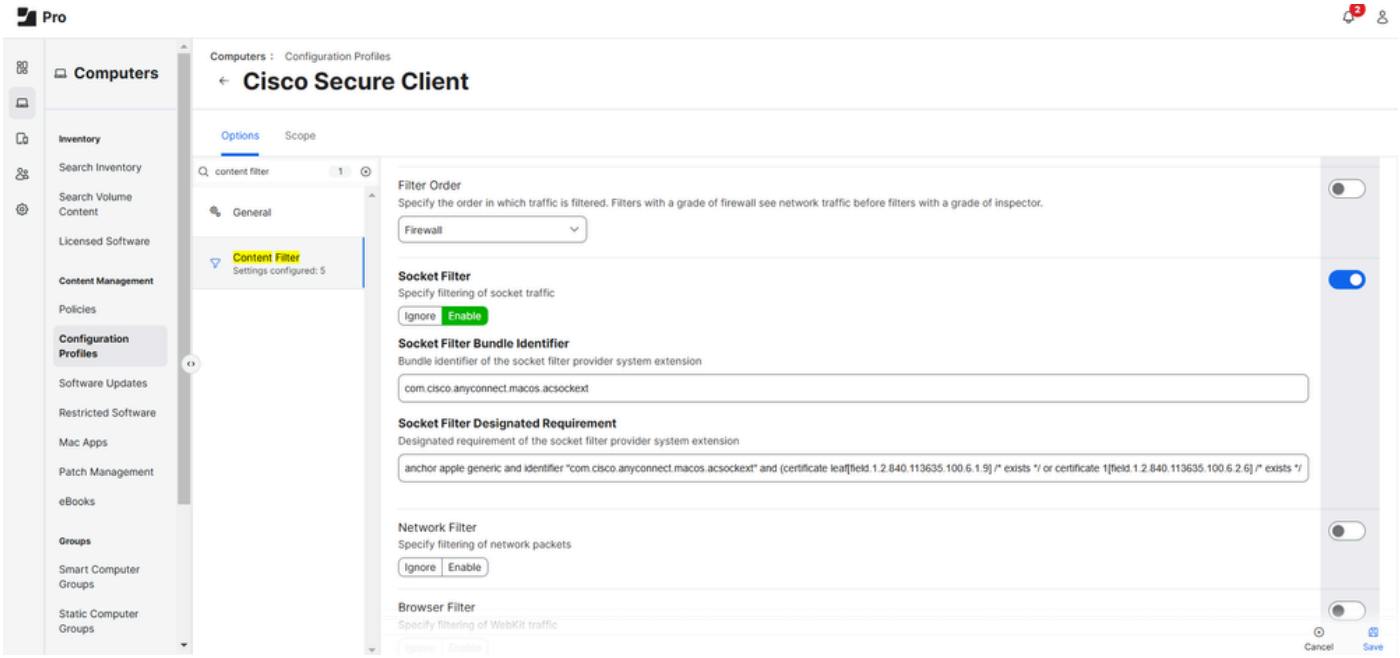
다음으로, Umbrella 모듈의 소켓 필터와 Cisco Secure Client의 상관관계가 있는 콘텐츠 필터에 대한 자동 설치를 구성합니다.

1. 콘텐츠 필터를 검색합니다. 다음 필드를 해당 값으로 활성화하고 완성합니다.

- 필터 이름: Cisco Secure Client - WebContentFilter
- 식별자: com.cisco.anyconnect.macos.acsock
- 소켓 필터: 활성화됨
- 소켓 필터 번들 식별자: com.cisco.anyconnect.macos.acsockext
- 소켓 필터 지정 요구 사항:

  anchor apple 일반 및 식별자 "com.cisco.anyconnect.macos.acsockext" 및 (certificate leaf[field.1.2.840.113635.100.6.1.9] /* 있음 */ 또는 certificate 1[field.1.2.840.113635.100.6.2.6] /* 있음 */ 및 certificate leaf[field.1.2.840.113635.100.6.1.13] /* 있음 */ 및 certificate leaf[subject.OU] = DE8Y96K9QP)





2. 사용자 정의 데이터 아래에서 추가를 5회 선택하고 다음 값을 입력합니다.

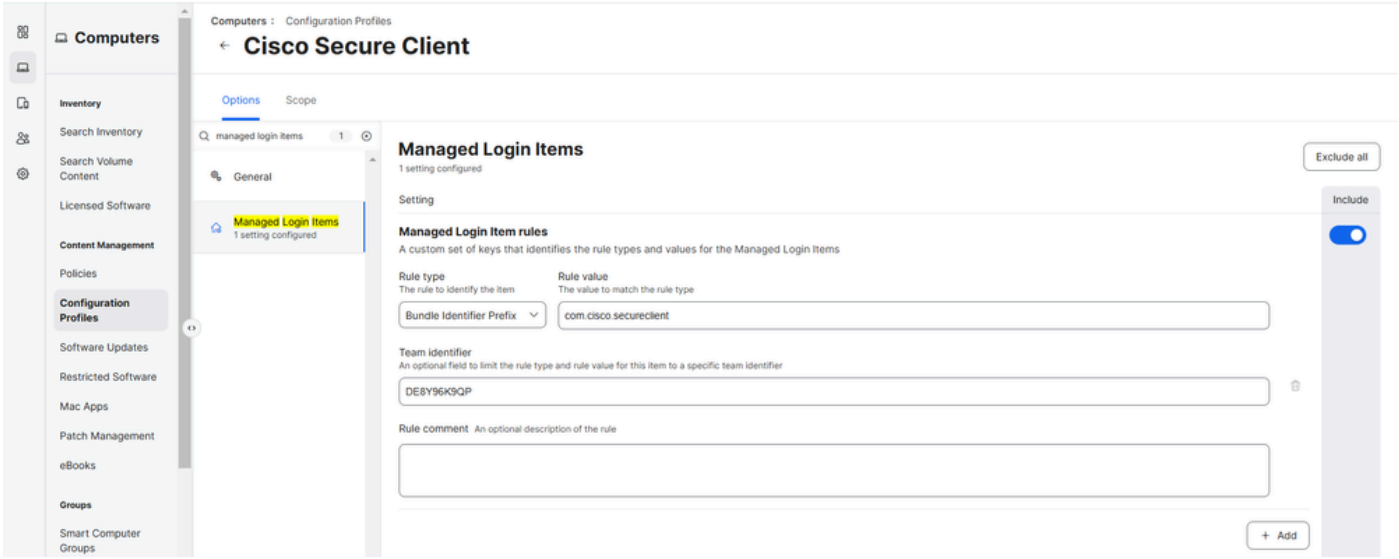
키	가치
자동 필터 사용	틀려
필터브라우저	틀려
필터 소켓	참
필터패킷	틀려
필터 등급	방화벽

관리 로그인 항목 구성

Umbrella 모듈을 사용하여 Cisco Secure Client에 대한 관리 로그인 항목을 구성하면 디바이스 시작 시 Cisco Secure Client가 실행됩니다.

구성하려면 Managed Login Items(관리된 로그인 항목)를 검색하고 다음 값으로 필드를 구성합니다
.

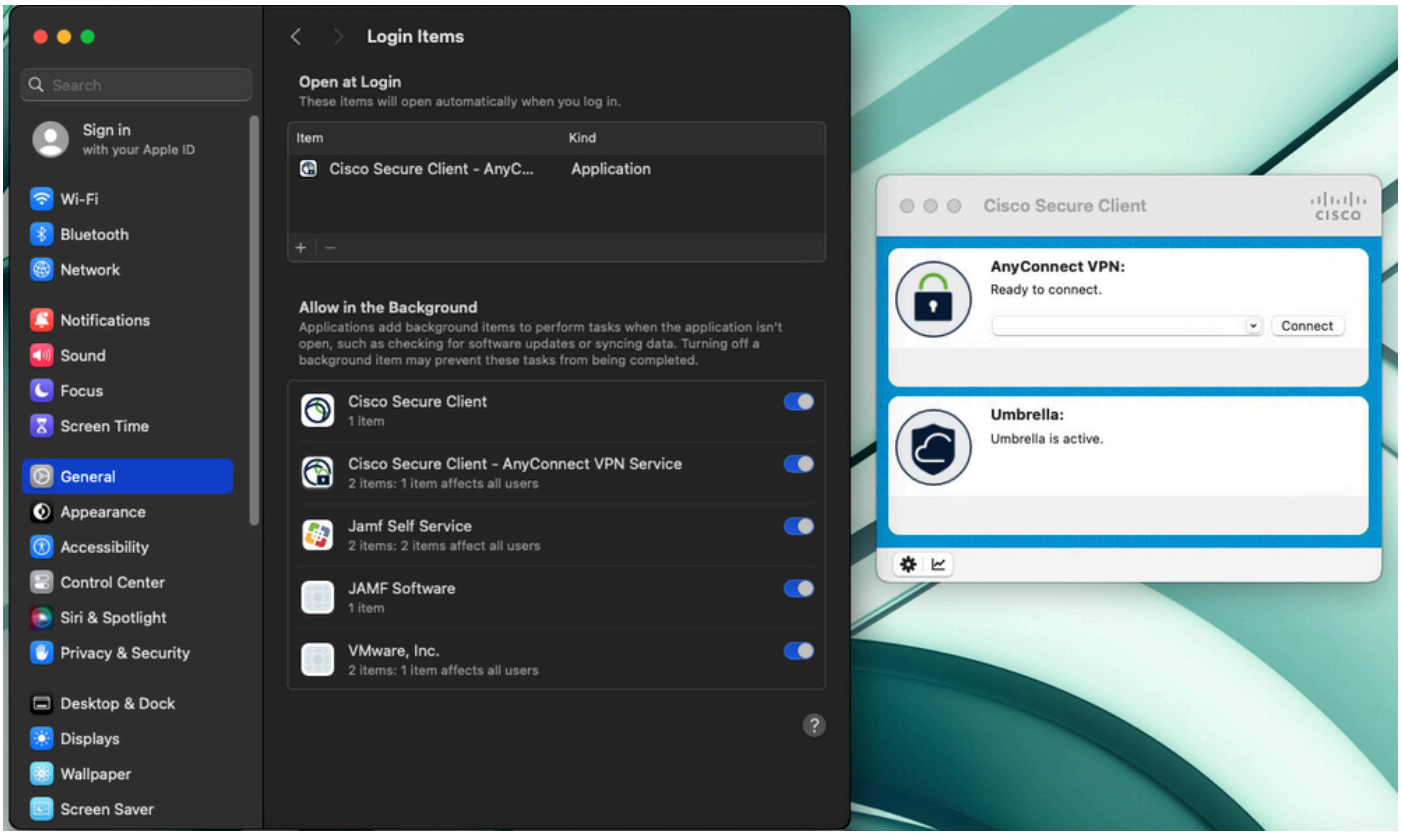
- 규칙 유형: 번들 식별자 접두사
- 규칙 값: com.cisco.secureclient
- 팀 식별자: DE8Y96K9QP

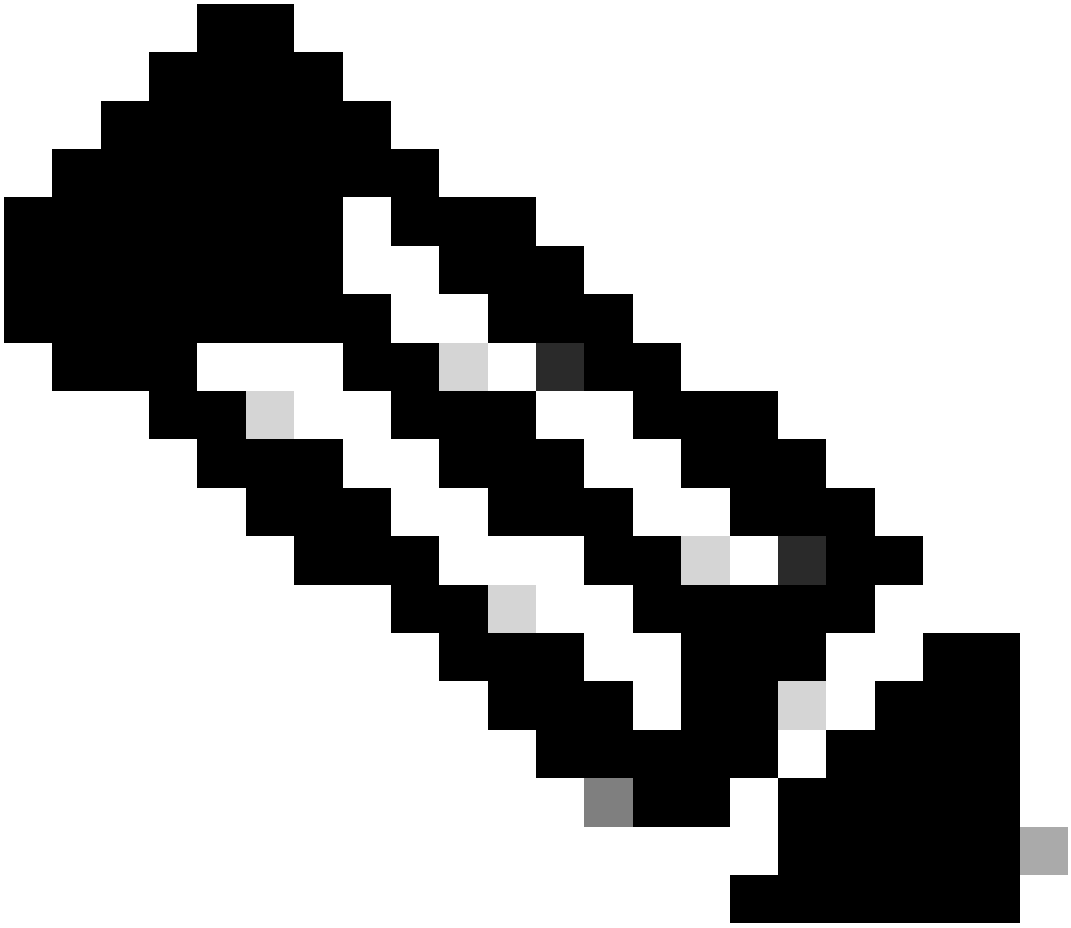


범위 할당 및 푸시 구축

1. Scope(범위)로 이동하여 디바이스 또는 사용자의 범위를 정의합니다.

2. Umbrella 모듈이 있는 Cisco Secure Client는 JAMF 정책 생성의 2단계에서 구성한 트리거 중 하나가 활성화될 때 원하는 macOS 장치로 푸시아웃될 수 있습니다. 또는 JAMF의 셀프 서비스 포털을 통해 이를 푸시할 수 있습니다.


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.



참고: 사용자가 시스템 설정(Network(네트워크) > Filter(필터)에서 DNS 프록시 또는 Transparent Proxy(투명 프록시)를 비활성화하려고 시도하더라도 이 문서에 설명된 대로 JAMF를 통해 콘텐츠 필터가 활성화되므로 기본적으로 다시 활성화됩니다.

macOS 방화벽 예외 구성

macOS 방화벽이 모든 수신 연결을 차단하도록 설정된 경우, Cisco Secure Client 및 해당 구성 요소를 예외 목록에 추가해야 합니다.

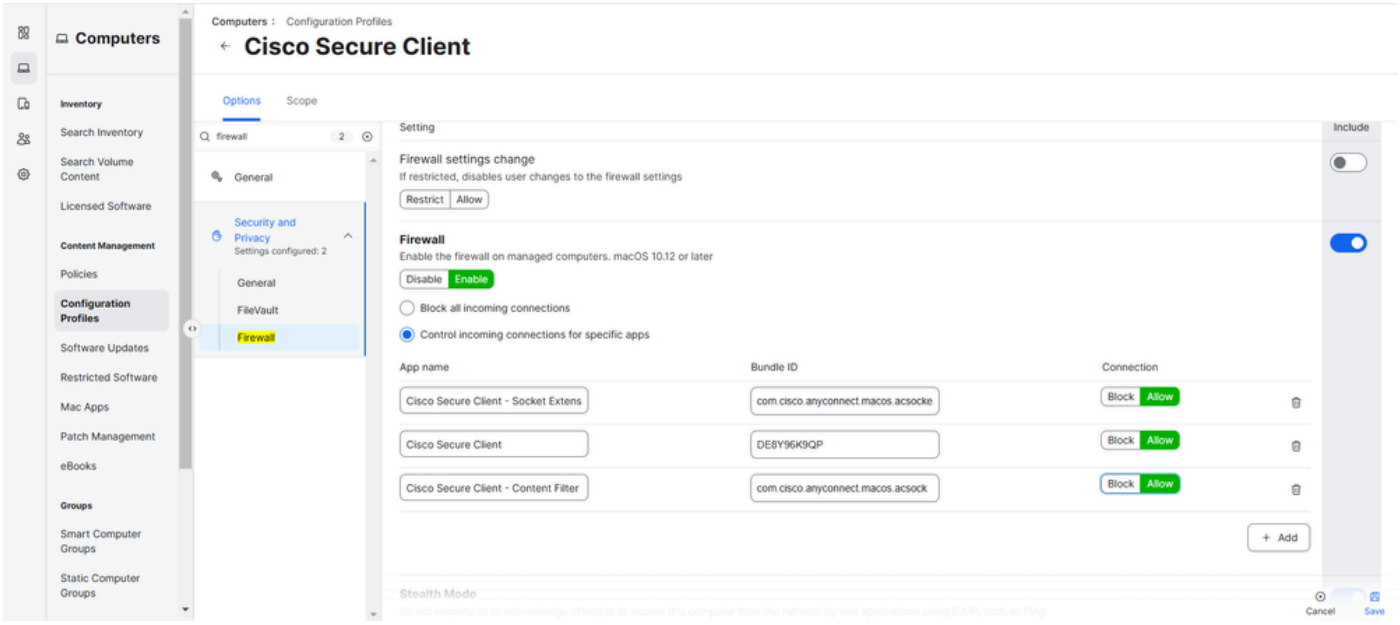
1. Computers(컴퓨터) > Content Management(콘텐츠 관리) > Configuration Profiles(컨피그레이션 프로필)로 이동합니다.

2. Cisco Secure Client 컨피그레이션 프로필을 선택하고 보안 및 개인 정보를 찾습니다.

3. 다음 설정으로 구성합니다.

- 방화벽: Enable - 특정 앱에 대한 수신 연결 제어

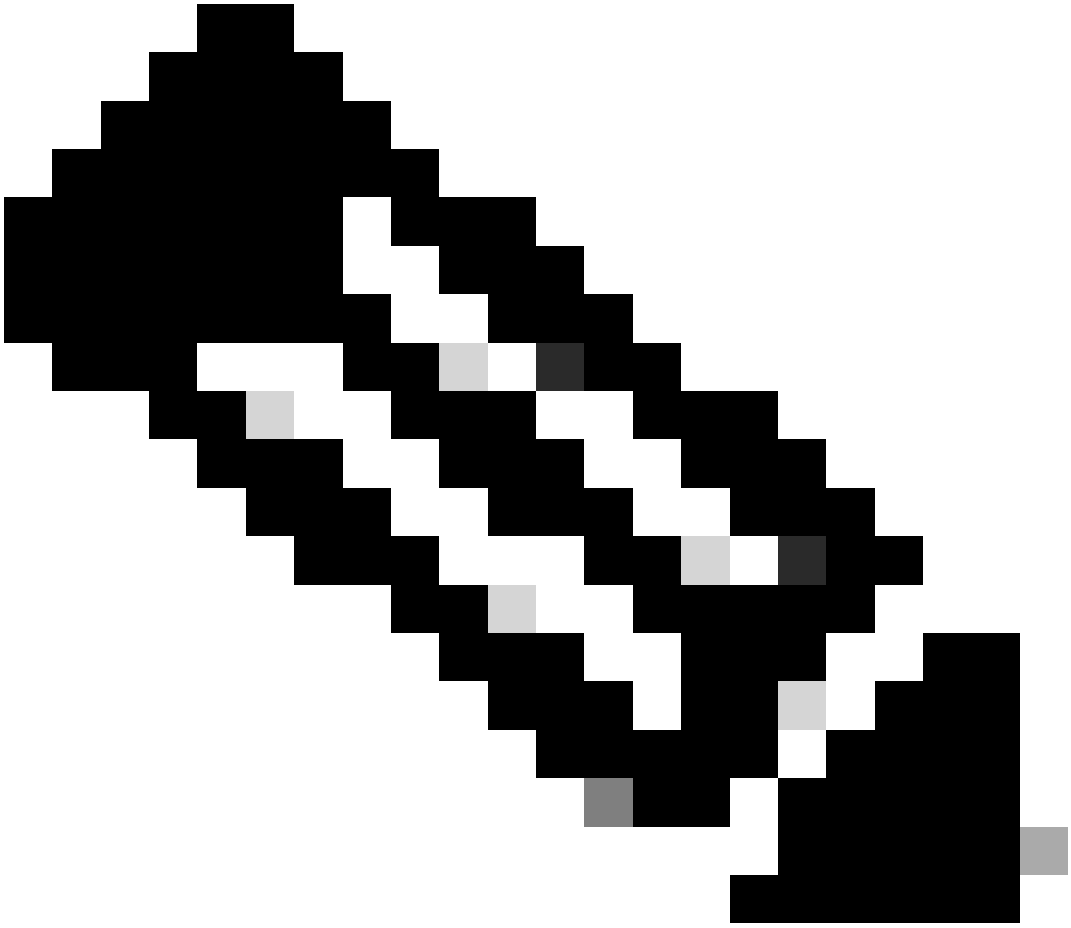
애플리케이션 이름	번들 ID
Cisco Secure Client - 소켓 확장	com.cisco.anyconnect.macos.acsockext
Cisco 보안 클라이언트	DE8Y96K9QP
Cisco Secure Client - 콘텐츠 필터	com.cisco.anyconnect.macos.acsock



4. 저장을 선택합니다.

5. 재배포 옵션을 입력하라는 메시지가 표시되면 전체 배포를 선택하여 변경 사항을 원하는 macOS 장치에 즉시 적용합니다.

Cisco Umbrella 루트 인증서 구축



참고: 이 단계는 이전에 Cisco Umbrella 루트 인증서가 배포되지 않은 장치 또는 Cisco Secure Client의 새 배포에만 적용됩니다. Umbrella Roaming Client 또는 Cisco AnyConnect 4.10 클라이언트에서 마이그레이션하거나 이전에 이미 Cisco Umbrella 루트 인증서를 배포한 경우 이 섹션을 건너뛸 수 있습니다.

Umbrella 대시보드의 Policies(정책) > Root Certificate(루트 인증서)에서 Cisco Umbrella 루트 인증서를 다운로드합니다.

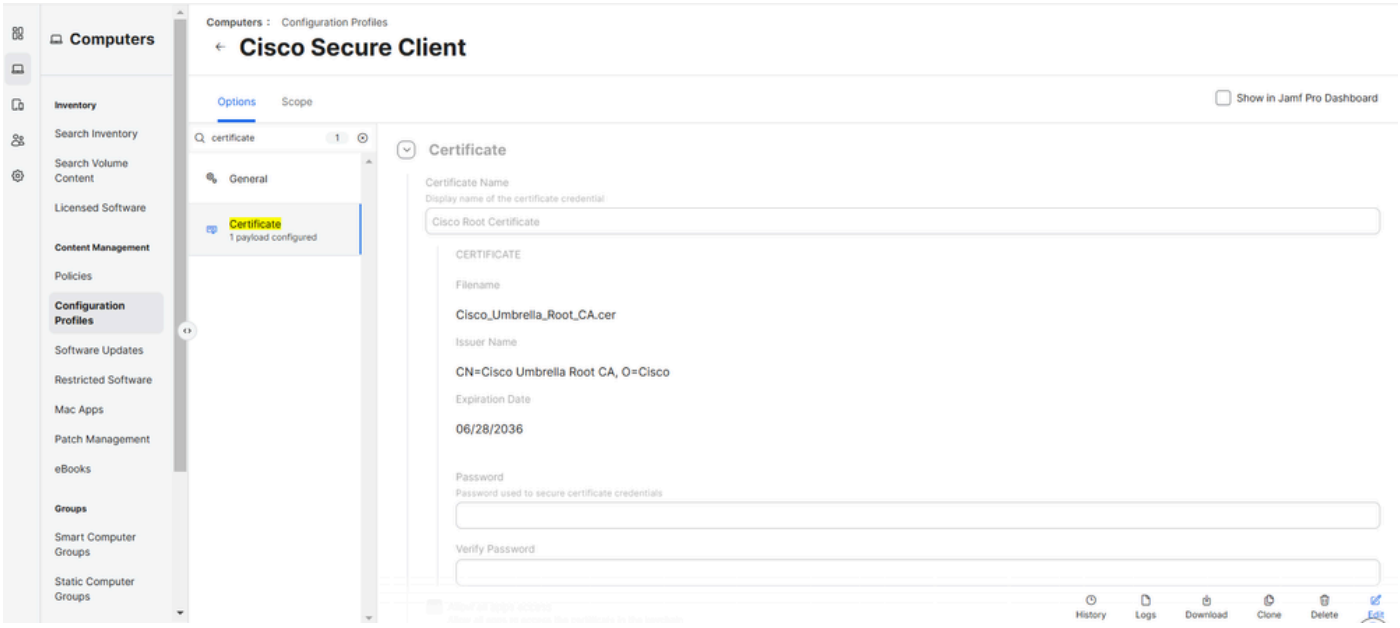
1. Umbrella 대시보드의 Policies(정책) > Root Certificate(루트 인증서)에서 Cisco Umbrella Root Certificate(Cisco Umbrella 루트 인증서)를 다운로드합니다.

2. JAMF에서 Computers(컴퓨터) > Configuration Profiles(컨피그레이션 프로파일) > Cisco Secure Client(Cisco Secure Client) > Edit(수정)로 이동합니다.

3. 인증서 검색 > 구성. 고유한 이름을 지정합니다.

4. Select Certificate Option(인증서 선택 옵션)에서 Upload(업로드)를 선택하고 1단계에서 이전에 다운로드한 Cisco Umbrella Root Certificate(Cisco Umbrella 루트 인증서)를 업로드합니다.

5. 여기에서 비밀번호를 구성하지 않는지 확인하고 저장을 선택합니다.



6. 재배포 옵션을 입력하라는 메시지가 표시되면 전체 배포를 선택하여 변경 사항을 원하는 macOS 장치에 즉시 적용합니다.

확인

Umbrella 모듈이 있는 Cisco Secure Client가 작동하는지 확인하려면 https://policy-debug.checkumbrella.com으로 이동하거나 다음 명령을 실행합니다.

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

각 출력에는 OrgID와 같은 Umbrella 조직에 대한 고유한 관련 정보가 포함되어야 합니다.

macOS 14.3의 해결 방법

Cisco Secure Client 5.1.x를 사용하는 macOS 14.3 이상의 경우, "VPN 클라이언트 에이전트가 프로세스 간 통신 데포를 생성할 수 없습니다"라는 메시지가 나타나면

1. JAMF에서 설정 > 컴퓨터 관리 > 스크립트 > 새로 만들기로 이동합니다.

2. 고유한 이름을 지정하고 범주를 정의합니다.

3. 스크립트 탭으로 이동하여 다음을 추가합니다.

```
#!/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. 옵션에서 우선순위가 다음으로 설정되었는지 확인합니다. 이 bash 스크립트는 pgrep -fl에서 프로세스 ID로 예상 출력을 반환하여 Cisco Secure Client - AnyConnect VPN service.app이 실행 중인지 확인합니다.

- 빈 출력이 반환되면 `Cisco Secure Client - AnyConnect VPN service.app`이 실행되고 있지 않으며 Umbrella 모듈이 올바르게 실행되는 데 필요한 Cisco Secure Client 코어 서비스를 시작하는 스크립트가 실행됩니다.

자동 업데이트

Cisco는 Secure Client 5.1.6.103(MR6)부터 시작하는 Secure Client를 포함하도록 Umbrella 대시보드에서 자동 업데이트 지원을 확장하기로 결정했습니다. 앞으로 Umbrella 대시보드에서 자동 업데이트가 구성된 경우 최소 Cisco Secure Client 5.1.6 MR6로 업그레이드한 고객은 최신 버전으로 자동 업데이트할 수 있습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.