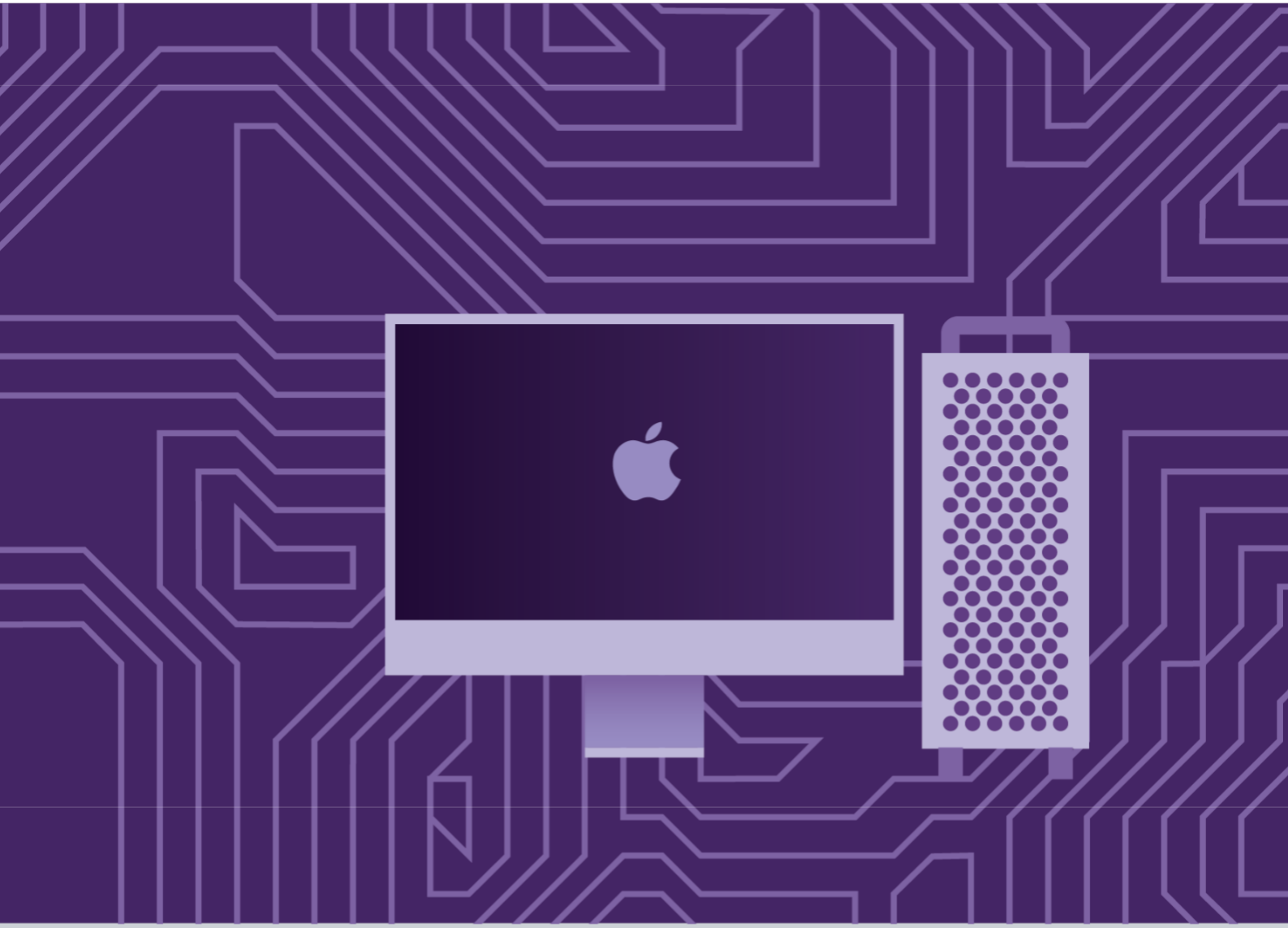
ENDPOINT PROTECTOR | by CoSoSys

JAMF

배포 가이드



버전: 3.0

날짜: 2022 년 11 월 11 일

목 차

변경 내역

버전	날짜	비고
1.0	2019	문서 만들어짐
2.0	2022.02.16	문서 업데이트됨
3.0	2022.11.11	VPN 설정 섹션 업데이트, 문서에 추가됨 로그 섹션 변경 및 현재 템플릿 적용됨

1. 개요

macOS 11.0 (Big Sur) 출시 이후 커널 레벨 엑세스 없이 엔드포인트 보안 솔루션 배포를 현재 허용하는 시스템 확장과 관련하여 많은 변화가 있었습니다.

이는 11.0 이상의 운영 체제를 사용하는 모든 Mac 의 Endpoint Protector 클라이언트 배포에 영향을 줍니다. 기업은 JAMF 뿐만 아니라 대안 도구와 같은 제 3 업체 배포 도구를 사용할 수 있습니다.

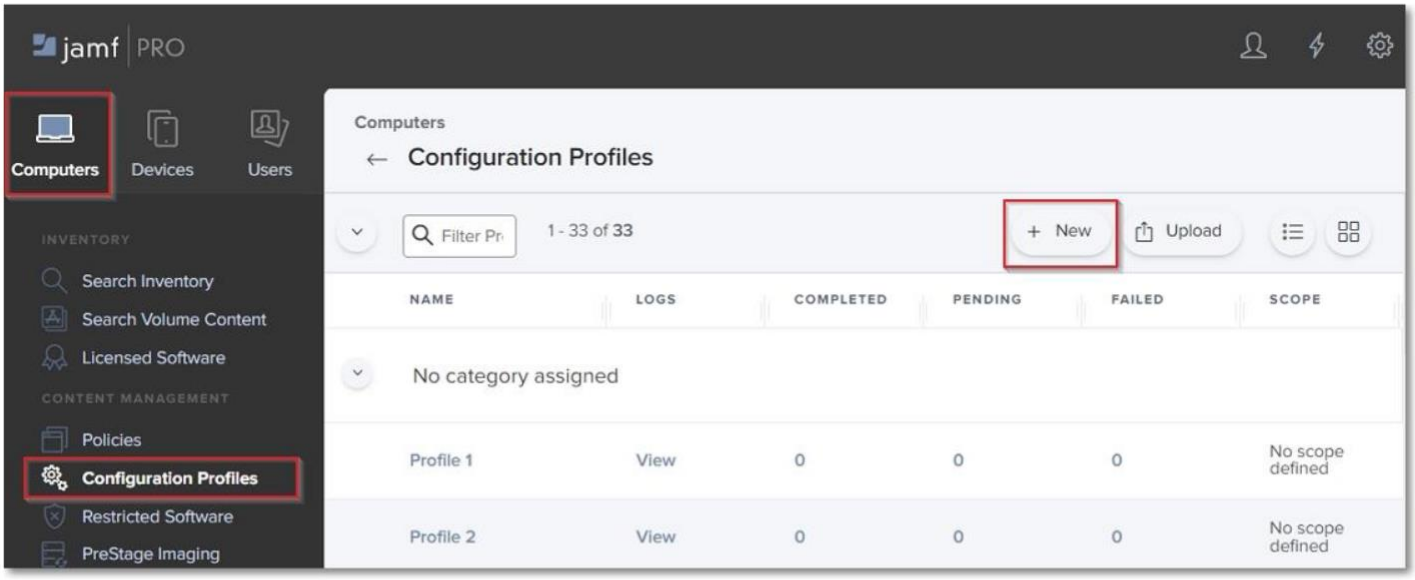
이 사용자 매뉴얼은 여러 엔드포인트에 Endpoint Protector 를 배포하기 위한 JAMF 사용 방법을 설명하는 것이 목적입니다.

2. 구성 프로파일 만들기

JAMF 를 사용하려면 첫 번째로 새로운 구성 프로파일을 만들어야 합니다.

구성 프로파일을 만들려면 아래 단계를 따르시기 바랍니다:

1. **JAMF Pro account** 를 열고 여러분의 계정으로 로그인합니다;
2. **JAMF** 계정의 메인 네비게이션 바의 **Computer** 클릭 후 왼쪽 사이드 메뉴에서 **Configuration Profiles** 을 선택합니다;
3. 새로운 구성 프로파일을 만들기 위해서 가능한 구성 프로파일의 우측 상단의 **+New** 클릭합니다.



New macOS Configuration Profile 섹션에서 프로파일 설정을 관리하고 프로파일 배포를 원하는 장치와 사용자를 선택할 수 있습니다.

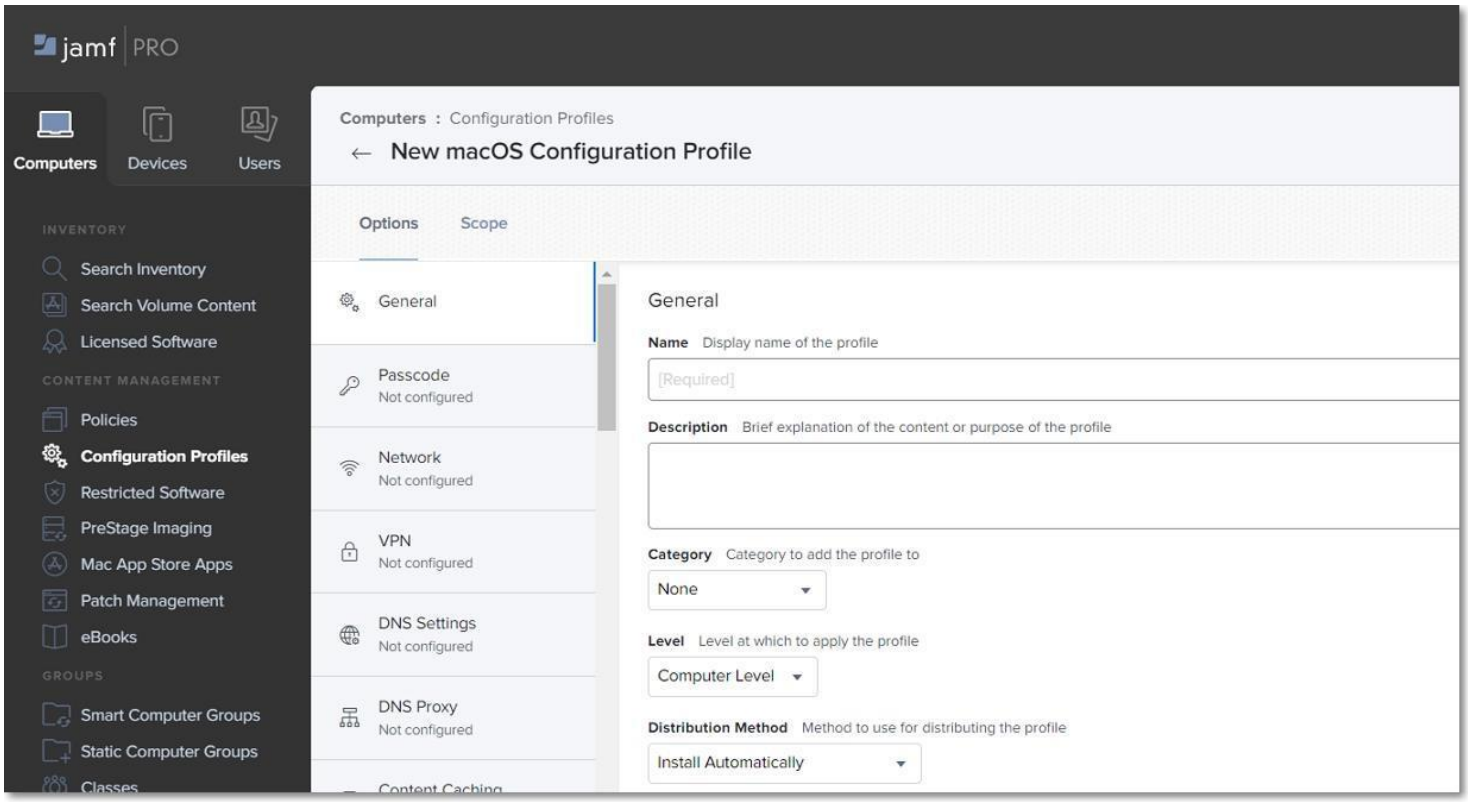
참고: 모든 설정과 프로파일 범위가 설정된 경우에만 **Save** 를 클릭하시기 바랍니다.

2.1. 일반 설정

기본 **General** 섹션에서 아래 정보를 입력합니다.:

- **Name** – 구성 프로파일 사용을 위한 이름 입력
- **Description** (선택) – 구성 프로파일 목적의 상세한 설명 추가

category, **level**, **distribution method** 필드는 기본 설정으로 계속 진행할 수 있습니다.

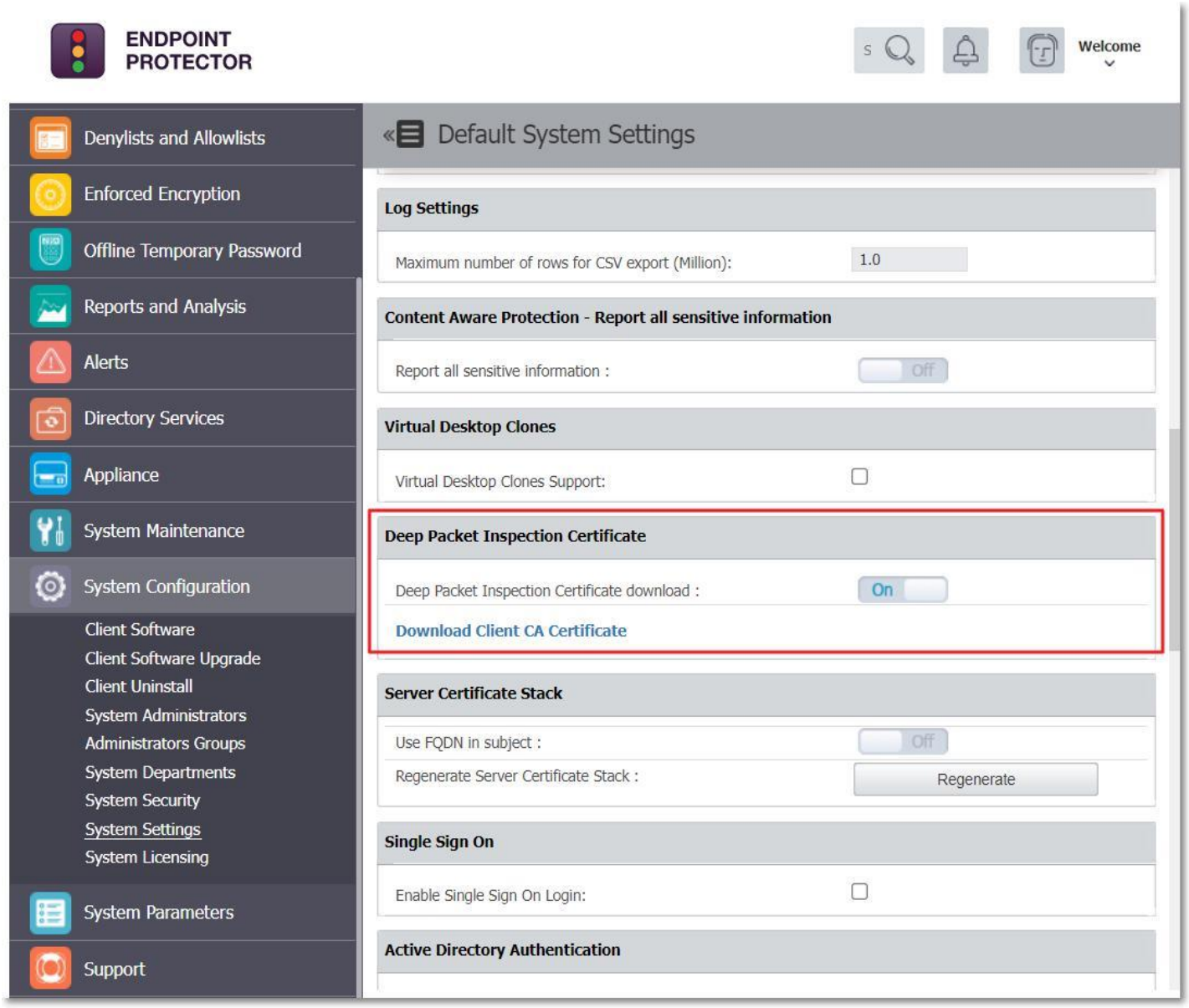


2.2. 인증서 설정

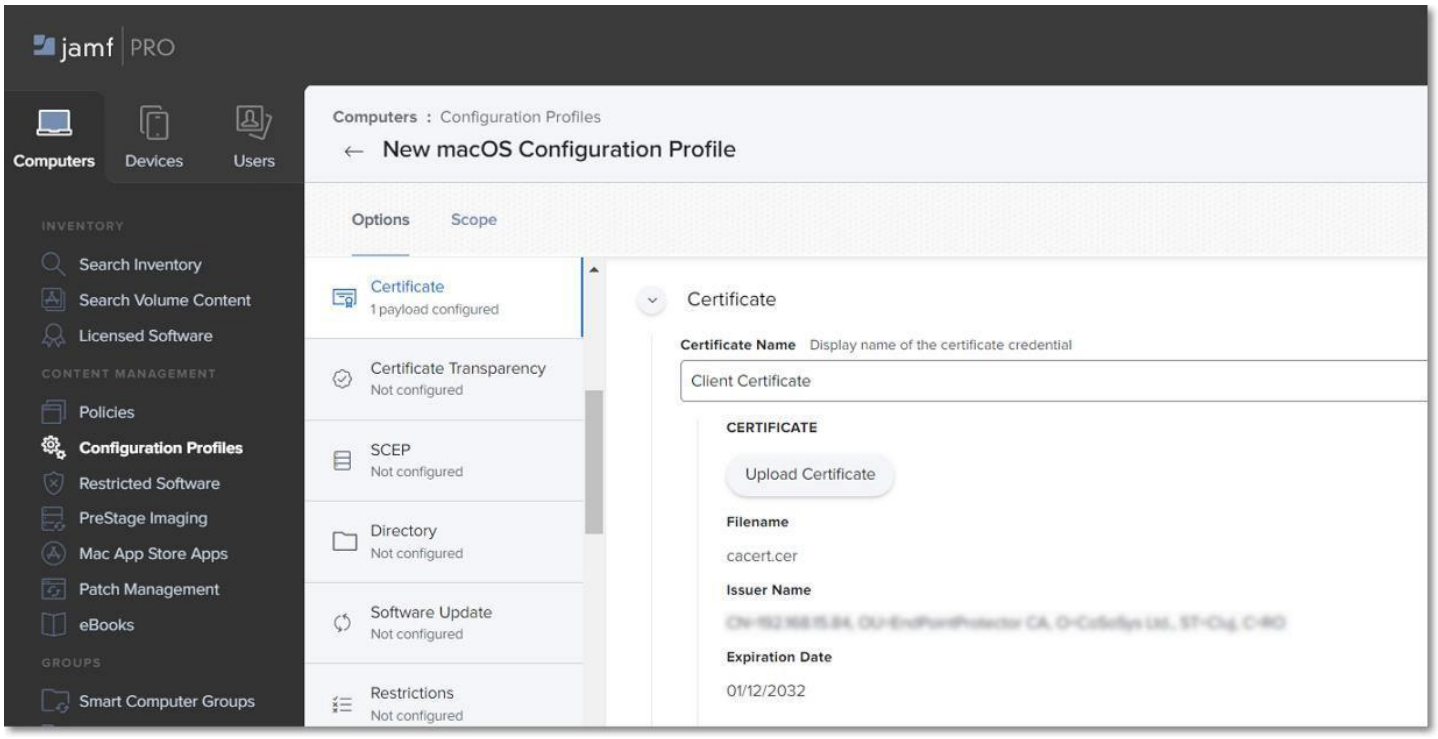
인증서 설정 섹션에서 .cer 포맷의 클라이언트 CA 인증서를 추가합니다.

참고: 이 단계는 심층 패킷 검사(DPI)를 사용하지 않으면 필요하지 않습니다. 계속 진행하려면 **Privacy Preferences Policy Control** 섹션으로 이동합니다.

1. **Endpoint Protector 서버**에 로그 인 후 **시스템 구성** 섹션의 **시스템 설정**을 선택합니다;
2. **기본 시스템 설정** 섹션에서 **심층 패킷 검사(DPI) 인증서**를 활성화하고 클라이언트 CA 인증서를 다운로드 합니다 – 다운로드한 .zip 파일은 .cer 과 .crt 클라이언트 인증서를 포함합니다.



3. JAMF 로 이동 후 **Certificate** 섹션의 **Configure** 를 클릭합니다;
4. **Certificate name** 을 입력하고 **.cer** 포맷으로 다운로드된 **클라이언트 CA 인증서**를 선택하고 업로드합니다.



2.3. Privacy Preferences Policy Control 설정

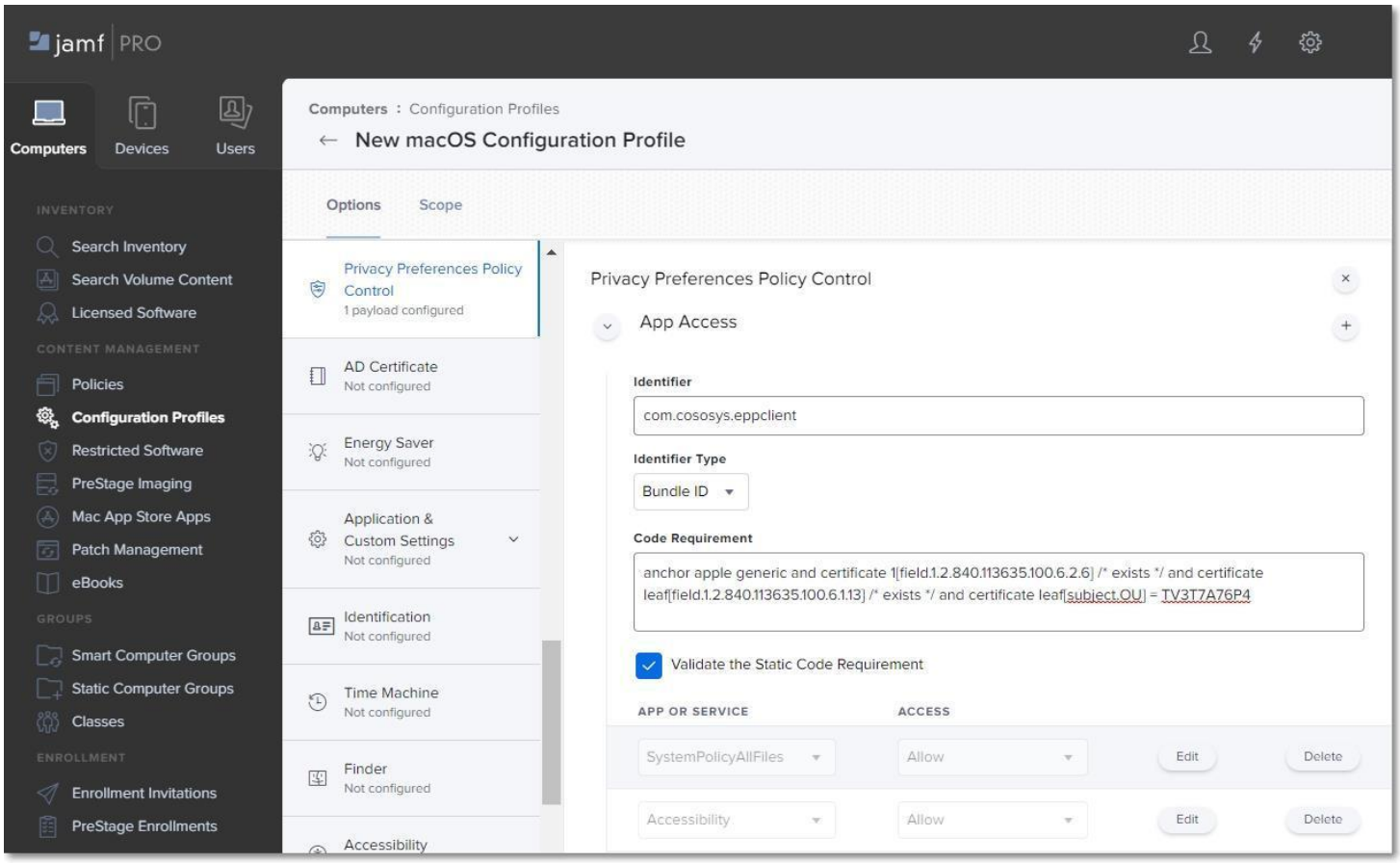
Privacy Preferences Policy Control 섹션에서 **Configure** 클릭 후 아래 정보를 입력합니다:

- **Identifier** - com.cososys.eppclient
- **Identifier Type** – 기본 **Bundle ID** 유형 사용
- **Code Requirement**

  anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

참고: 이 커맨드 라인을 실행하기 전에 서식 변경이 없는지 터미널 편집기를 사용하여 확인하시기 바랍니다.

- **Validate the Static Code Requirement** 체크박스 선택
- **Add** 클릭 후 **SystemPolicyAllFiles** 및 **Accessibility** 서비스 허용 후 **Save** 를 클릭



2.4. EppNotifier 설정 허용

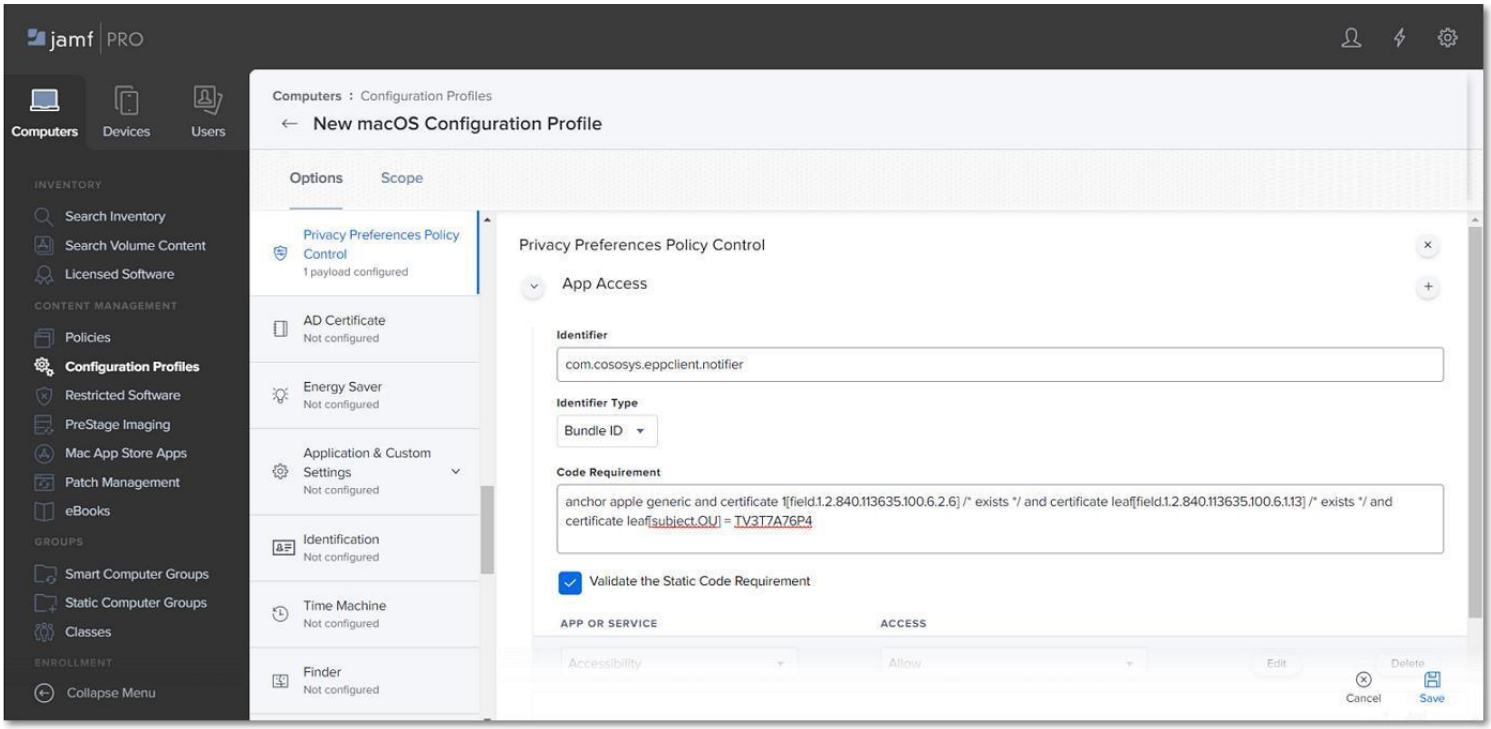
Privacy Preferences Policy Control 섹션에서 새로운 정책 추가를 위해서 **+** 아이콘을 클릭하고 아래 정보를 입력합니다:

- **Identifier** - com.cososys.eppclient.notifier
- **Identifier Type** – 기본 **Bundle ID** 유형 사용
- **Code Requirement**

  anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

참고: 이 커맨드 라인을 실행하기 전에 서식 변경이 없는지 터미널 편집기를 사용하여 확인하시기 바랍니다.

- **Validate the Static Code Requirement** 체크박스를 선택
- **Add** 클릭 후 **Accessibility** 서비스 허용 후 **Save** 클릭



2.5. EasyLock 암호화 정책 설정

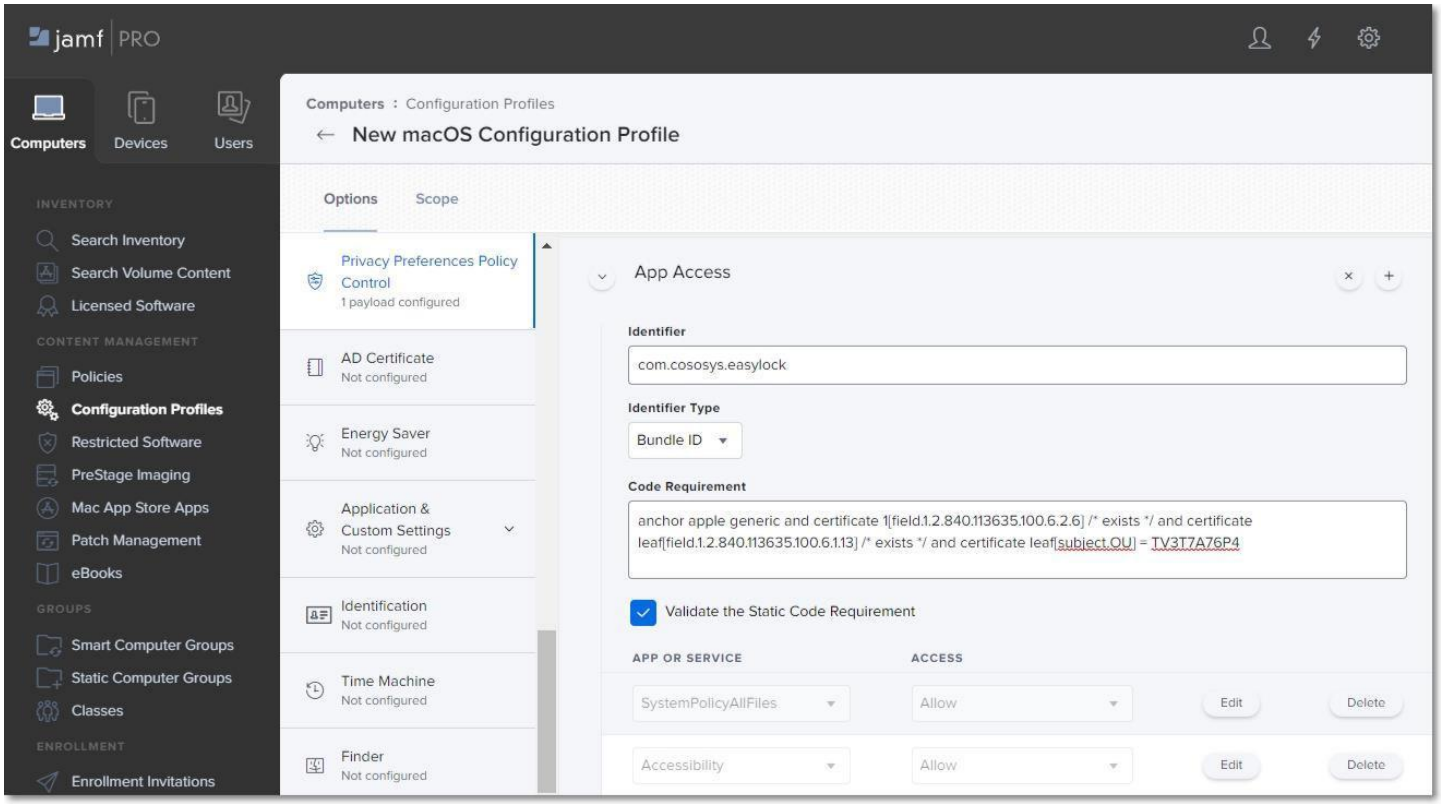
Privacy Preferences Policy Control 섹션에서 새로운 정책 추가를 위해서 **+** 아이콘을 클릭하고 아래 정보를 입력합니다:

- **Identifier** – com.cososys.easylock
- **Identifier Type** – 기본 **Bundle ID** 유형 사용
- **Code Requirement**

  anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

참고: 이 커맨드 라인을 실행하기 전에 서식 변경이 없는지 터미널 편집기를 사용하여 확인하시기 바랍니다.

- **Validate the Static Code Requirement** 체크박스 선택
- **Add** 클릭 후 **SystemPolicyAllFiles** 및 **Accessibility** 서비스 허용 후 **Save** 클릭

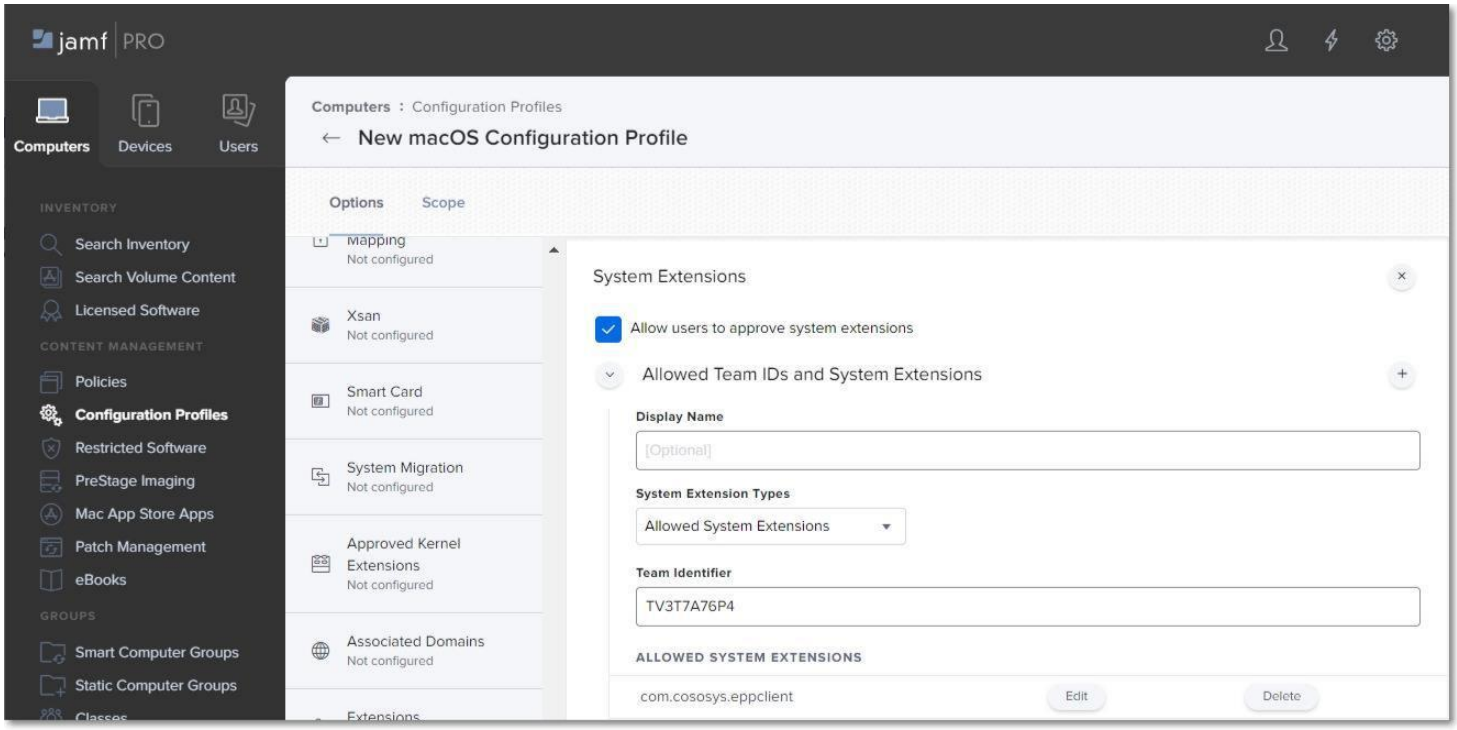


2.6. 시스템 확장 설정

2.6.1. 시스템 확장 허용

System Extension 섹션에서 **Configure** 클릭 후 아래 정보를 입력합니다:

- **Display Name** (선택) – 이 구성에 사용되는 이름 입력
- **System Extension Type - Allow System Extension** 유형 선택
- **Team Identifier -** TV3T7A76P4
- **Allowed System Extensions** – **Add** 클릭 후 com.cososys.eppclient 입력 후 변경 사항 **Save**



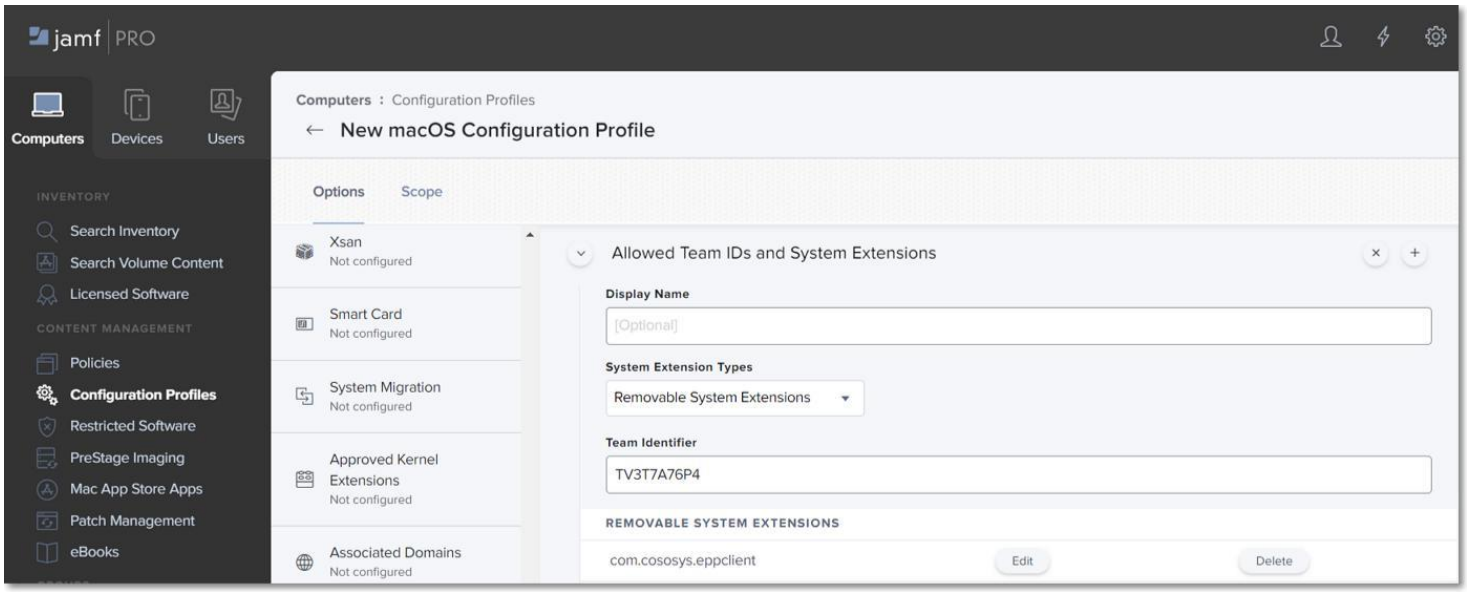
참고: macOS 11 (Big Sur) 이하 버전의 운영 체제에서는 시스템 확장 대신에 **Approved Kernel Extensions** 섹션에서 설정을 관리합니다. **Team ID (TV3T7A76P4)** 입력 후 다음 단계를 진행합니다.

2.6.2. 제거 가능한 시스템 확장

System Extension 섹션에서 팝업 없이 시스템을 확장 제거를 허용하는 새로운 정책을 추가하기 위해 + 아이콘 클릭 후 아래 정보를 입력합니다:

- **Display Name** (선택) – 이 구성 사용을 위한 이름을 입력
- **System Extension Type - Removable System Extensions** 유형 선택
- **Team Identifier -** TV3T7A76P4
- **Allowed System Extensions** – **Add** 클릭 후 com.cososys.eppclient 입력하고 변경 사항 **Save**

참고: 이 설정은 macOS 12 버전 (Monterey)을 시작으로 적용됩니다.



2.7. VPN 설정

참고: 이 단계는 **VPN** 서비스를 사용하지 않으면 필요 없습니다. 계속 진행하려면 **Scope** 섹션으로 이동하시기 바랍니다.

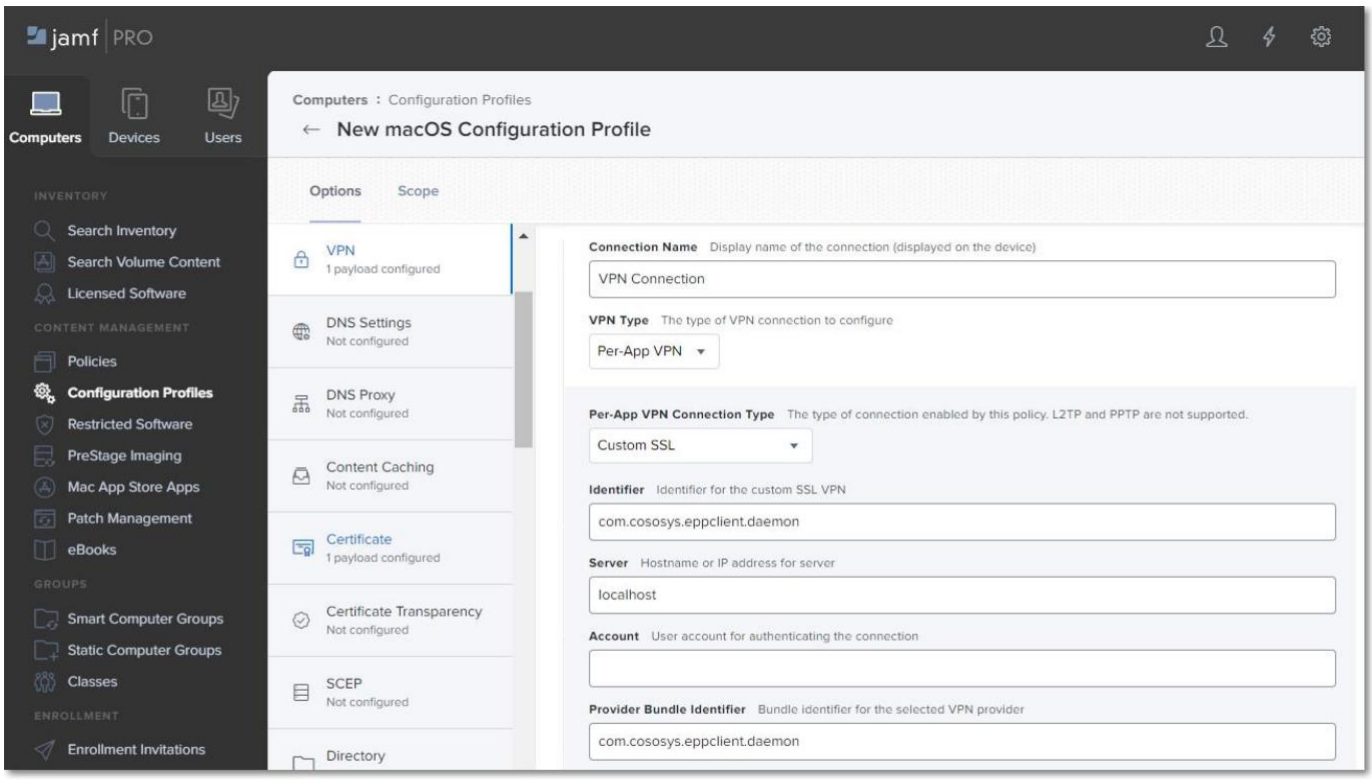
VPN 섹션에서 **Configure** 을 클릭 후 아래 정보를 입력합니다:

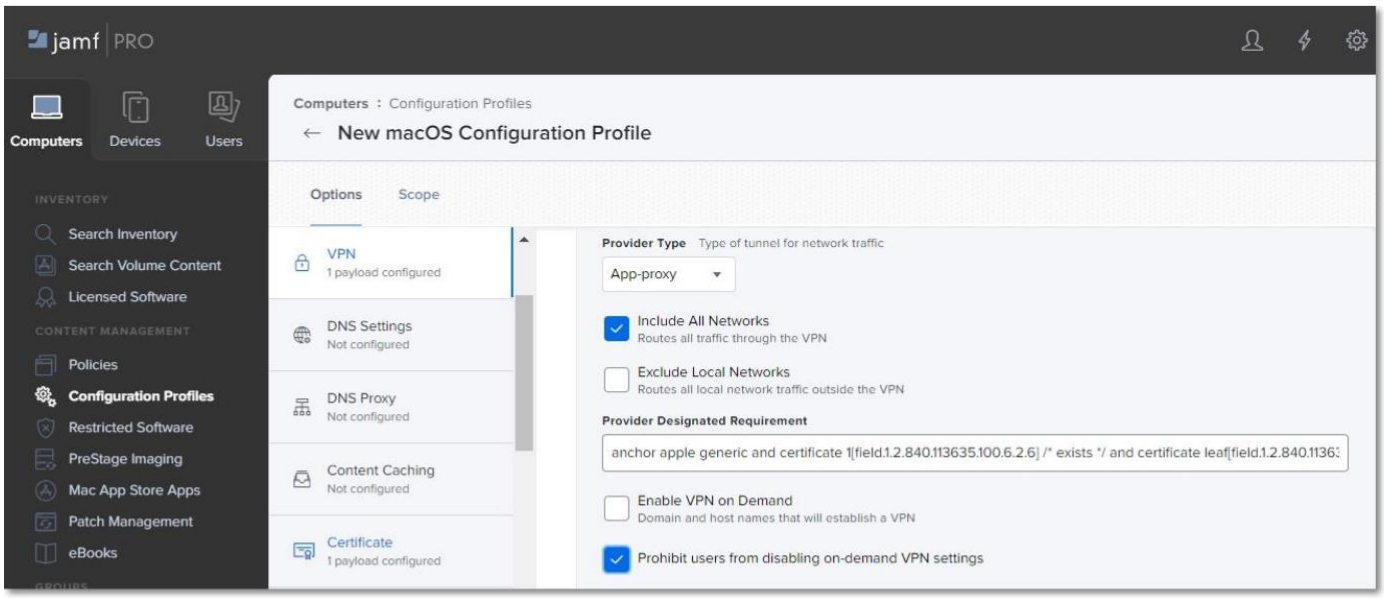
- **Connection Name** – 기기에 표시되는 통신 이름 입력
- **VPN Type** – **Per-App VPN** 유형 선택
- **Per-App VPN Connection Type** – **Custom SSL** 통신 유형 선택
- **Identifier** – com.cososys.eppclient.daemon
- **Server** – localhost
- **Provider Bundle Identifier** – com.cososys.eppclient.daemon
- **Provider Type** – **App-proxy** 유형 선택
- **Include All Networks** 체크박스 선택
- **Provider Designated Requirement**

  anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = TV3T7A76P4

참고: 이 커맨드 라인을 실행하기 전에 서식 변경이 없는지 터미널 편집기를 사용하여 확인하시기 바랍니다.

- **Prohibit users from disabling on-demand VPN settings** 체크박스 선택



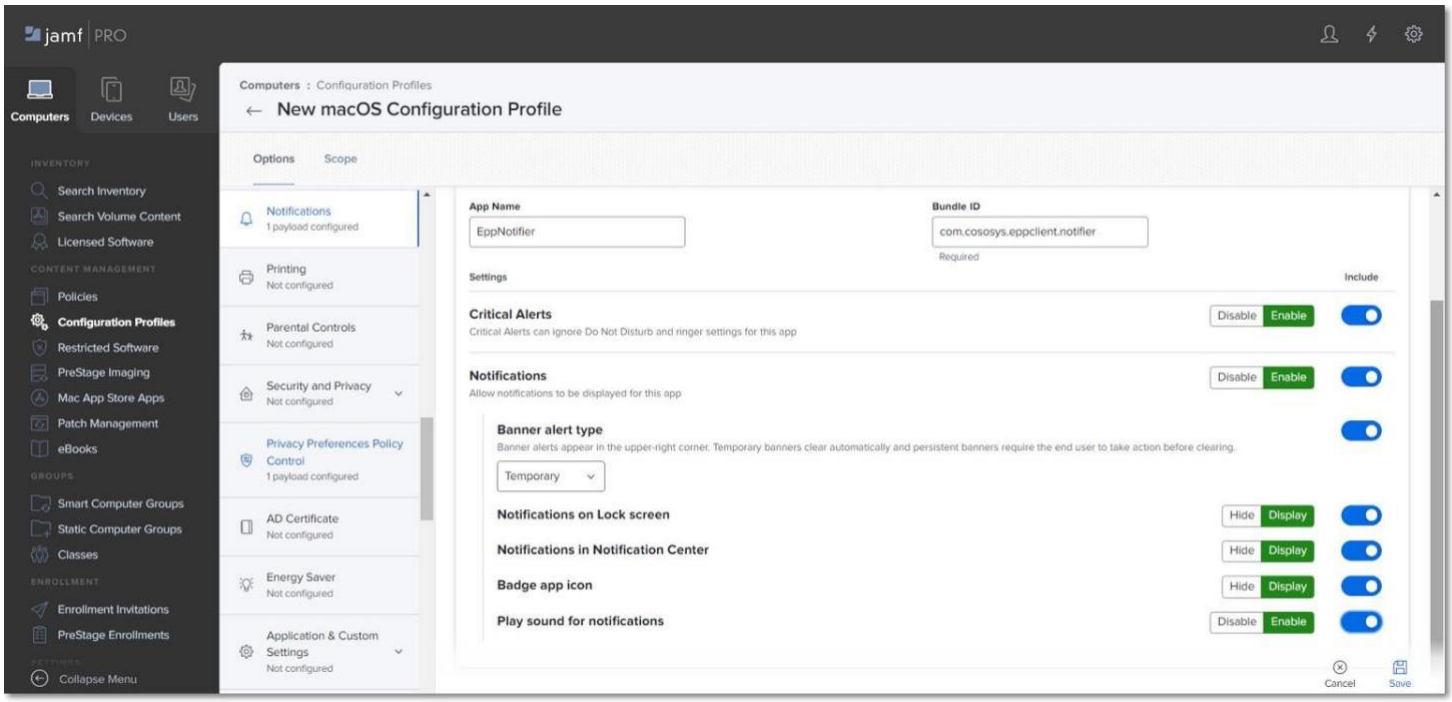


2.8. 알림 설정

참고: 이 단계는 선택 사항입니다. 계속 진행하려면 **Scope** 세션으로 이동합니다.

Notifications 섹션에서 **Configure** 클릭 후 아래 정보를 입력합니다:

- **App Name** - EppNotifier
- **Bundle ID** - com.cososys.eppclient.notifier
- 설정 유형을 포함하기 위해서 스위치를 토글하고 각 알림 옵션 관리를 위해서 disable/enable 합니다.

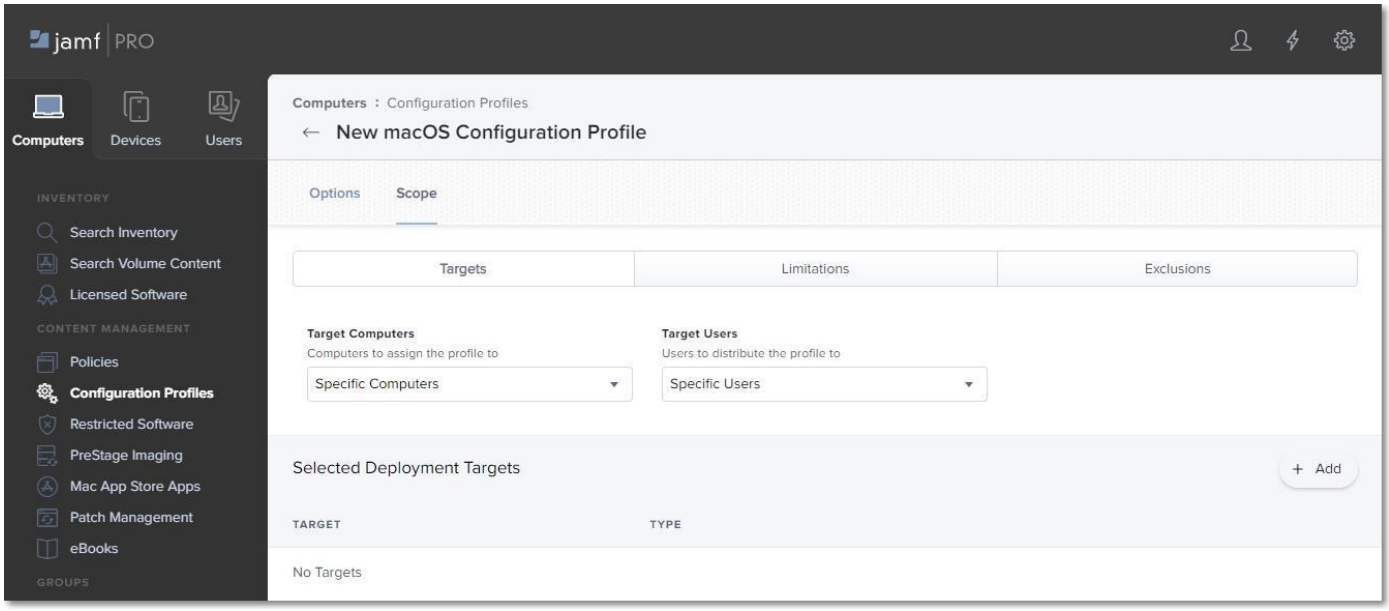


2.9. 범위

모든 설정을 관리하기 위해서 Scope 탭으로 이동 후 새로운 프로파일을 배포하는 기기와 사용자를 선택합니다.

새로운 구성 프로파일에 모든 설정을 적용하기 위해서 **Save** 를 클릭합니다.

참고: 새로운 구성 프로파일이 성공적으로 저장된 것을 확인하기 위해서 이 시점에 컴퓨터를 재부팅합니다.



3. 스크립트 및 패키지 업로드

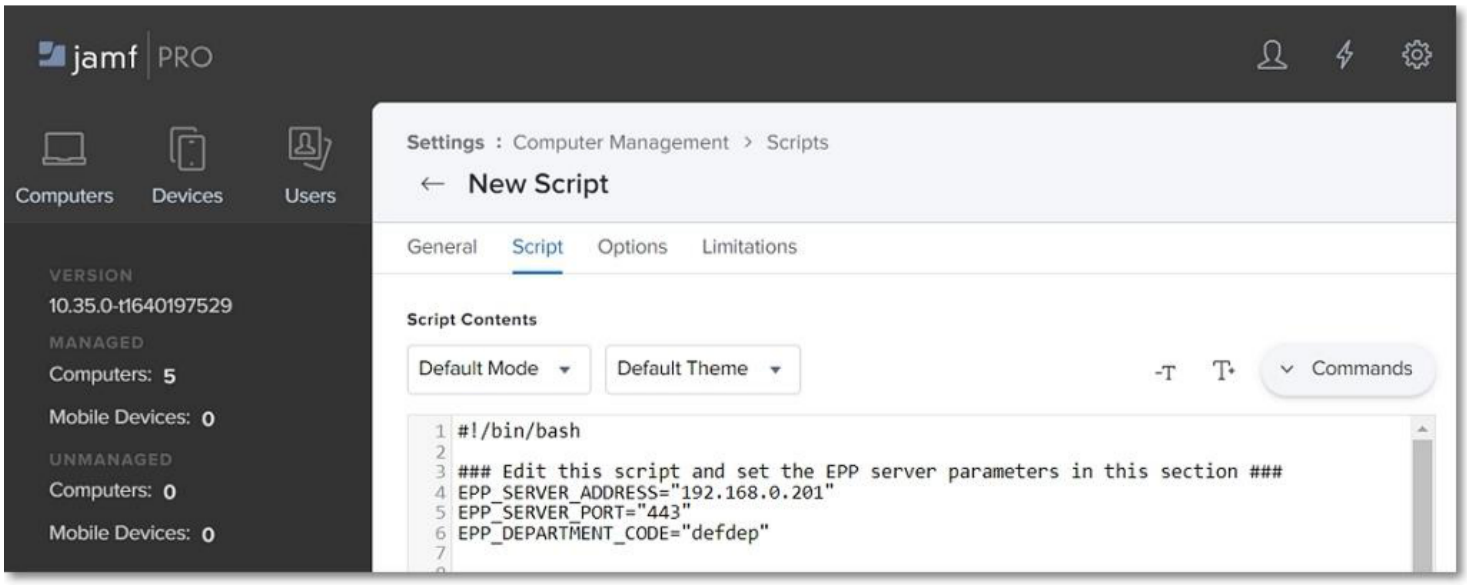
Endpoint Protector 클라이언트를 배포하기 위해서 **EndpointProtector.pkg** 패키지와 **epp_change_ip.sh** 스크립트를 업로드해야 합니다.

중요: 스크립트는 담당 총판사로 문의 주시기 바랍니다.

스크립트와 패키지를 업로드 하려면 아래 단계를 진행하시기 바랍니다:

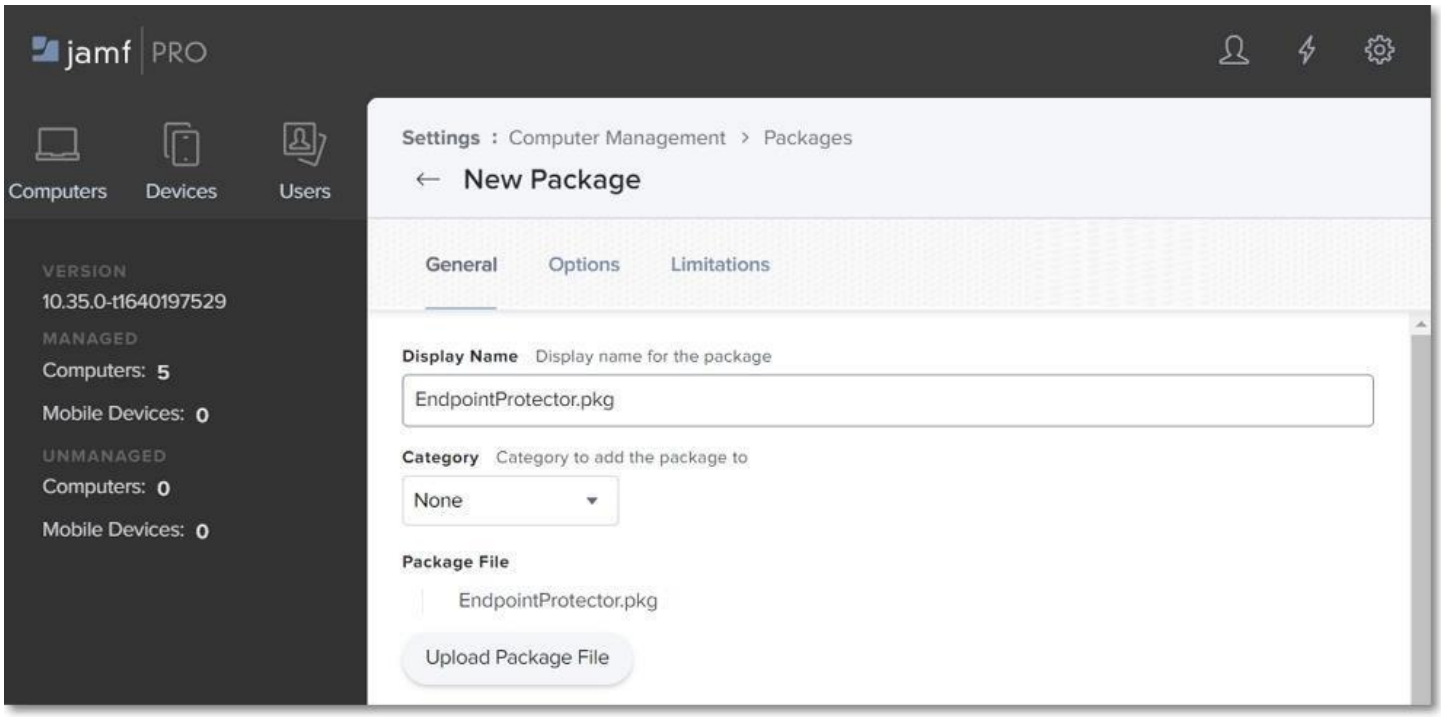
1. **JAMF** 계정의 메인 네비게이션 바에서 **Computer** 클릭 후 좌측 메뉴에서 **Management Settings** 를 선택합니다;
2. **Computer Management** 섹션에서 **Scripts** 선택 후에 우측 상단의 **+ New** 를 클릭합니다;
3. **General** 섹션에서 프로파일 이름 추가 후 **Script** 탭을 선택하고 **epp_change_ip.sh** 스크립트를 추가합니다;
4. **EPP_SERVER_ADDRESS** 영역에서 서버 IP 를 추가합니다;

참고: 특정 구분 또는 사용자 정의 포트로 배포하려면 **EPP_DEPARTMET CODE** 및 **EPP_SERVER_PORT** 필드를 편집할 수 있습니다.



5. **Computer Management** 섹션에서 **Package** 선택한 후 우측 상단의 **+ New** 를 클릭합니다;

6. **General** 탭에서 이름을 추가한 후 **EndpointProtector.pkg** 를 업로드 합니다.

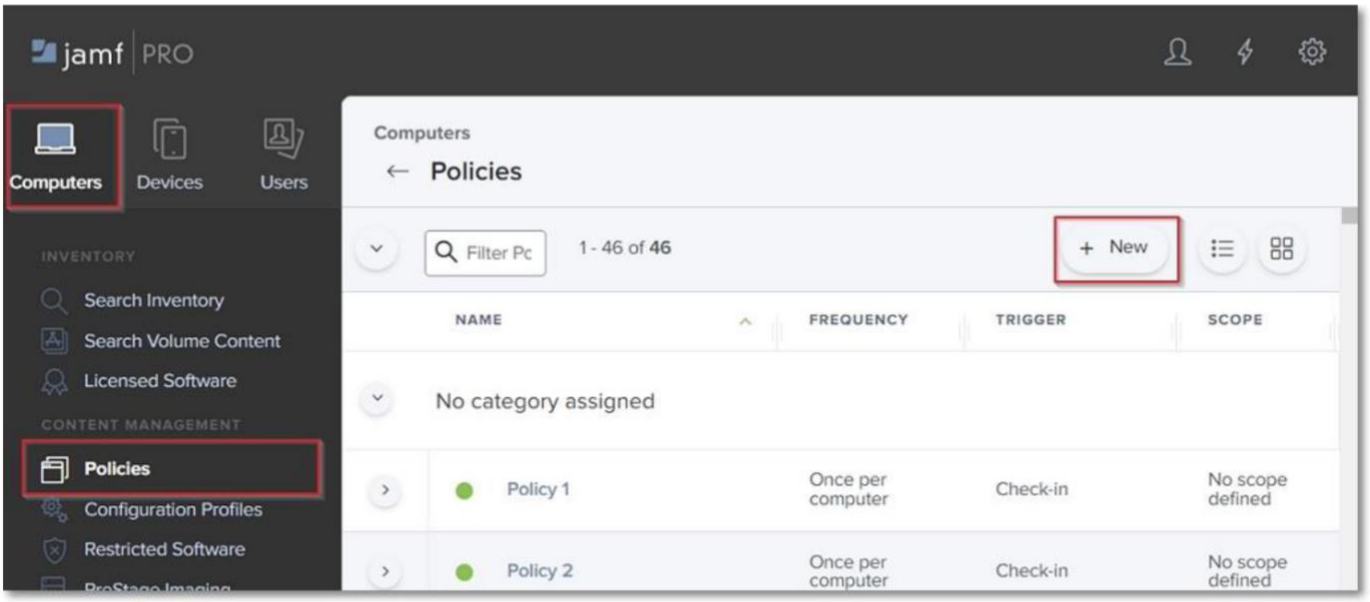


4. 정책 만들기

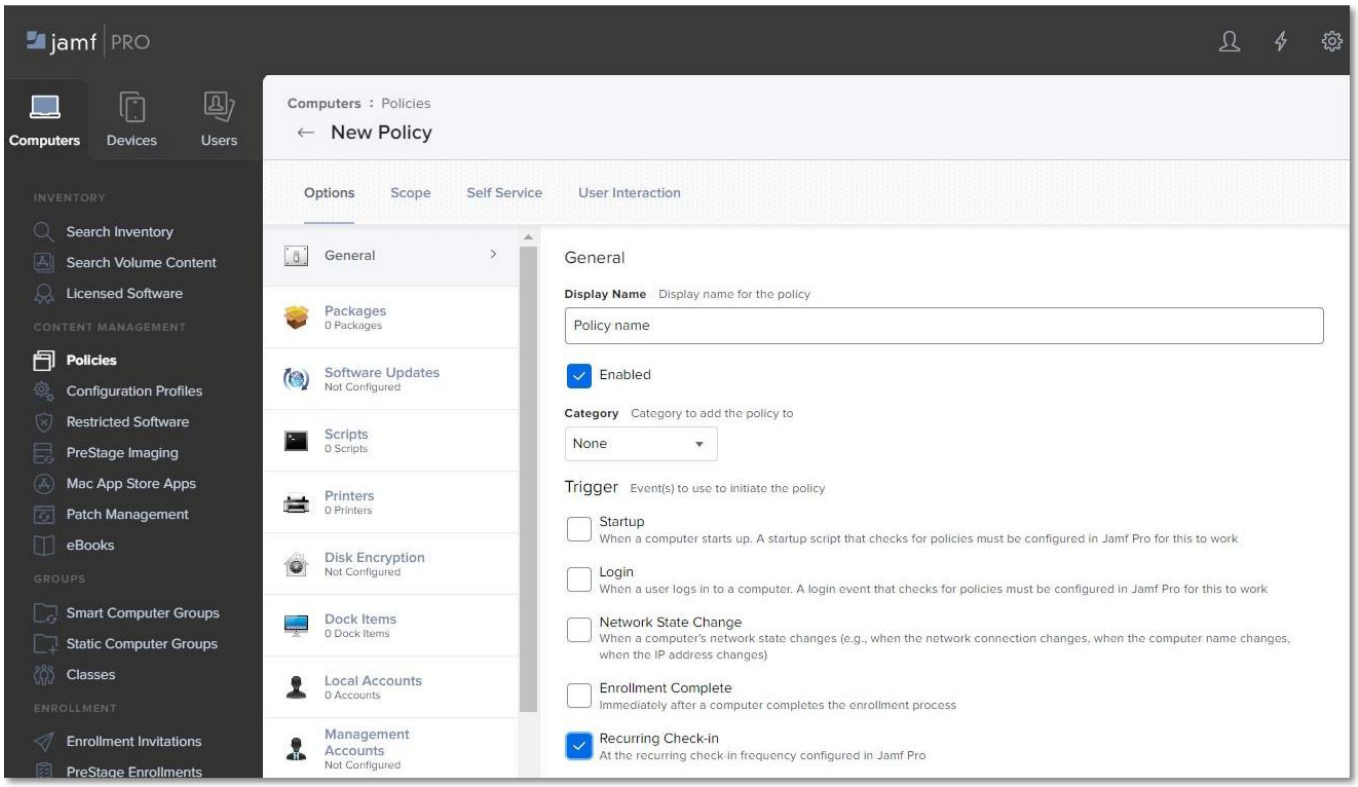
스크립트와 패키지가 성공적으로 업로드 되면 새로운 JAMF 정책을 만들어야 합니다.

새로운 정책을 만들려면 다음 단계를 따르시기 바랍니다:

1. **JAMF** 계정의 메인 네비게이션 바에서 **Computer** 클릭 후 좌측 메뉴에서 **Policies** 선택 후 **+ New** 클릭합니다;

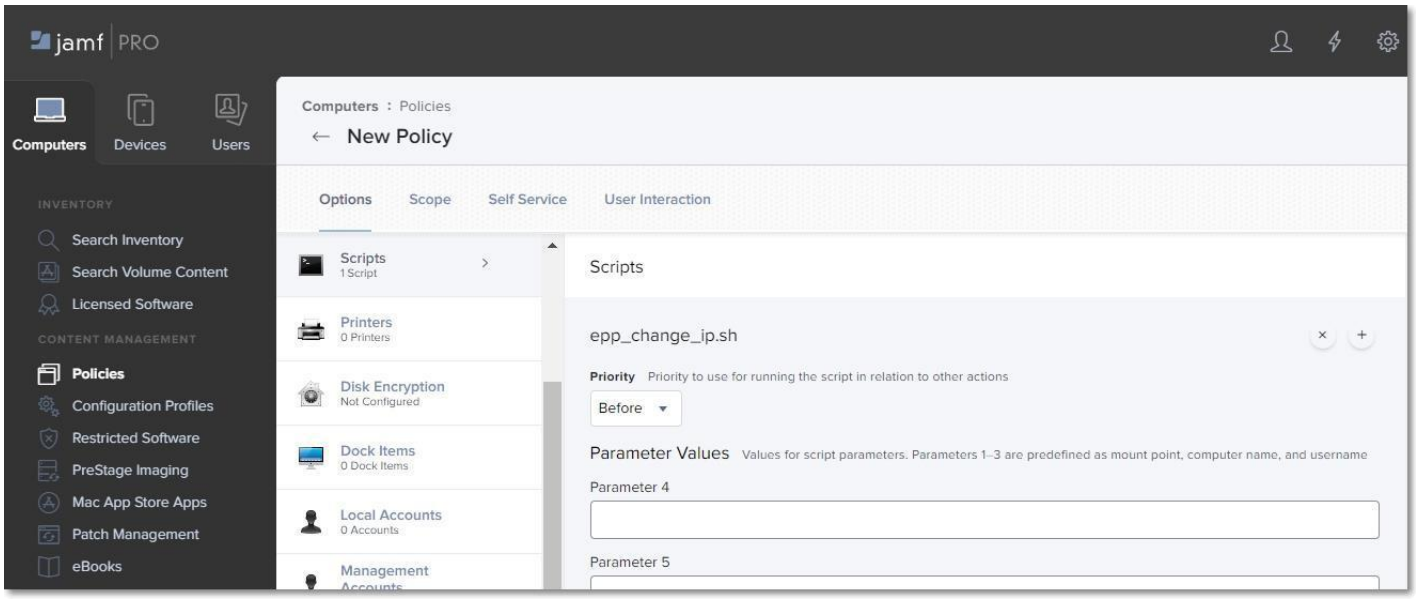


2. 기본 **General** 섹션에서 아래 정보를 입력합니다:
   - **Display Name** – 이 정책을 사용하는 이름 입력
   - **Recurring Check-in** 체크박스 선택

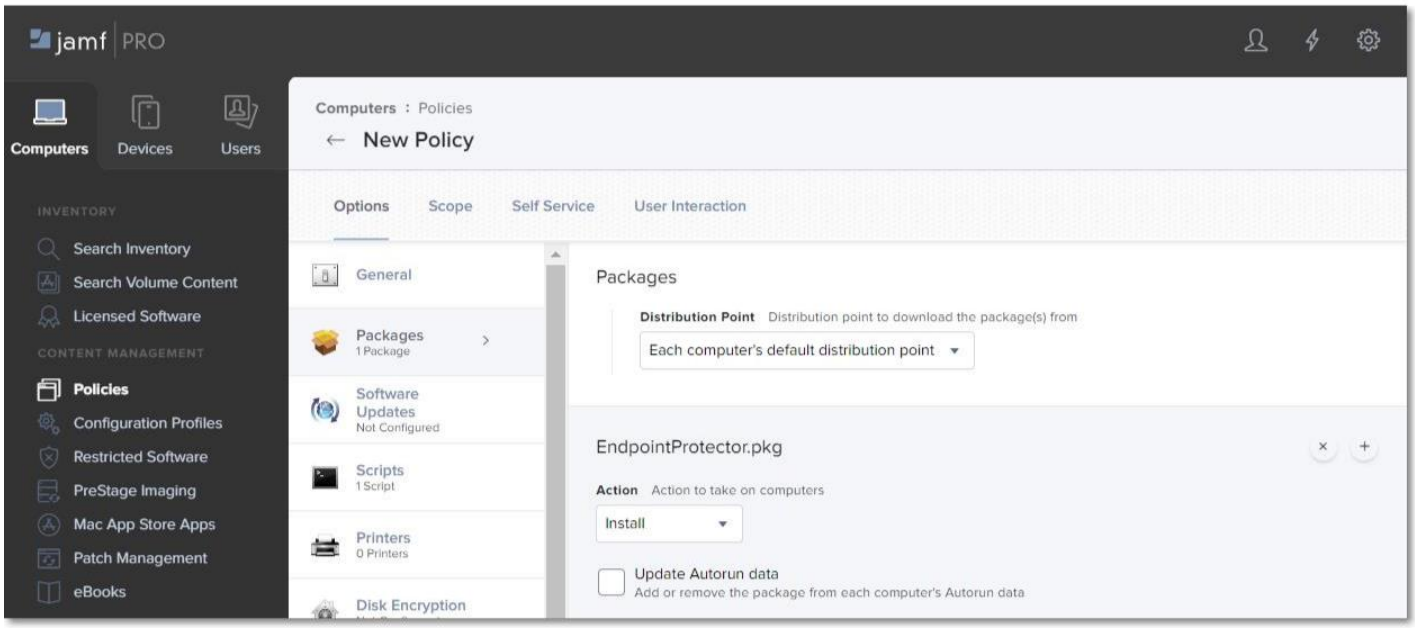


3. **Scripts** 섹션에서 **Configure** 클릭 후 아래 정보를 입력합니다:

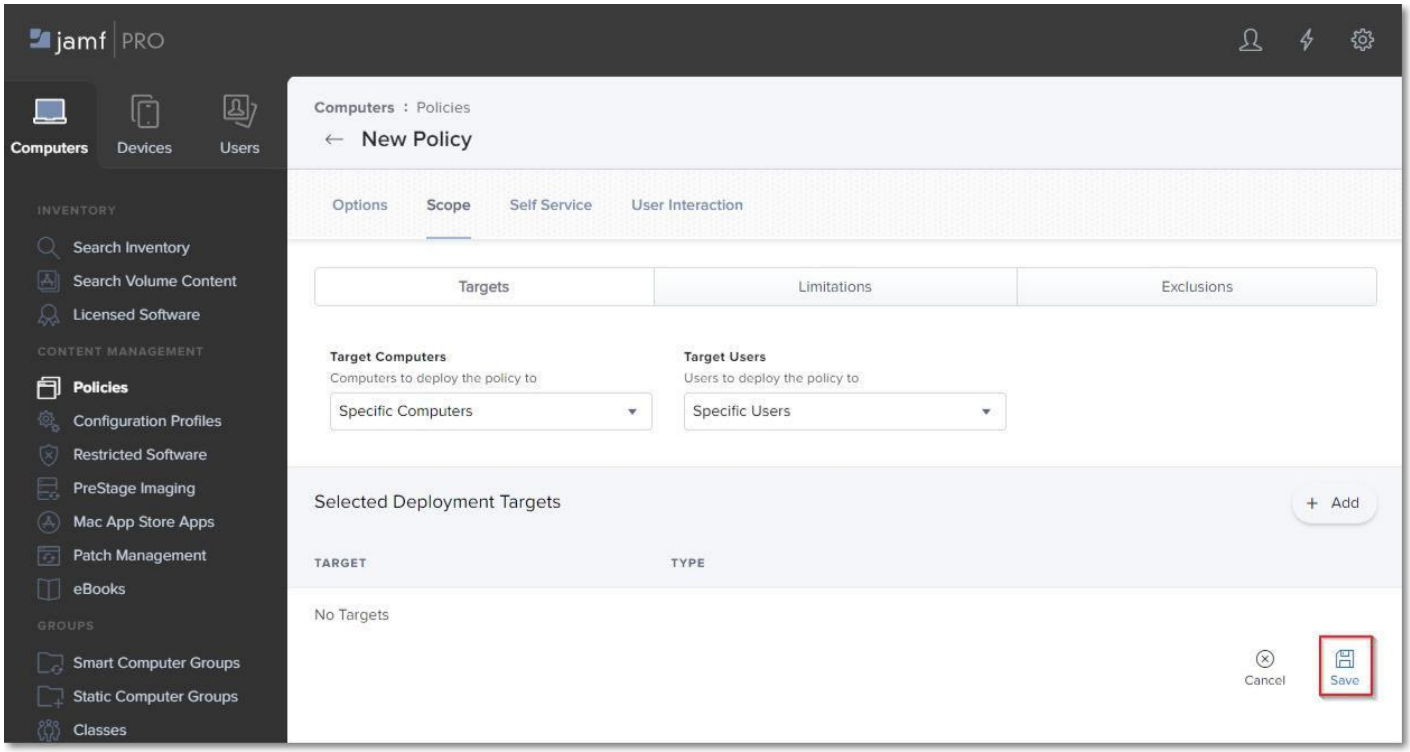
   - **epp_change_ip.sh** 스크립트를 추가
   - **Priority** – **Before** 우선순위 설정, 다음 단계 전에 스크립트는 설치가 되어야 함



4. **Packages** 섹션에서 **Configure** 클릭 후 **EndpointProtector.pkg** 패키지를 추가합니다;



5. **Scope** 탭으로 이동 후 새로운 정책 적용을 위해 기기와 사용자를 추가합니다;
6. 새로운 정책에 모든 설정을 적용하기 위해서 **Save** 를 클릭합니다;



Endpoint Protector 클라이언트가 성공적으로 배포되고 서버-클라이언트 통신이 예상대로 동작하는지 확인하기 위해서 Endpoint Protector UI 의 **컴퓨터 목록**에서 엔드포인트를 볼 수 있습니다. Endpoint Protector 클라이언트는 메뉴 바에 표시됩니다.

5. 면책

These instructions are provided on an “AS IS” basis. To the maximum extent permitted by law, CoSoSys disclaims all liability, as well as any and all representations and warranties, whether express or implied, as to the fitness for a particular purpose, title, non-infringement, merchantability, interoperability, and performance in relation with these instructions. Furthermore, CoSoSys makes no warranty and disclaims any and all liability with regards to third-party software, which the Customer uses at its own risk and expense.

Nothing herein shall be deemed to constitute any warranty, representation, or commitment in addition to those expressly provided in the terms and conditions that apply to the Customer’s use of the CoSoSys Products.

EndpointProtector.com