인증서 인증 구성 & DUO SAML 인증

목차

소개

이 문서에서는 인증서 기반 인증 및 듀오 SAML 인증 구현의 예를 설명합니다.

사전 요구 사항

이 가이드에서 사용하는 도구 및 장치는 다음과 같습니다.

- Cisco FTD(Firepower 위협 방어)
- FMC(Firepower Management Center)
- 내부 CA(인증 기관)
- Cisco DUO Premier 어카운트
- Cisco DUO 인증 프록시
- CSC(Cisco Secure Client)

요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- 기본 VPN,
- SSL/TLS
- 공개 키 인프라

- FMC 경험
- Cisco 보안 클라이언트
- FTD 코드 7.2.0 이상
- Cisco DUO 인증 프록시

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- Cisco FTD(7.3.1)
- Cisco FMC(7.3.1)
- Cisco Secure Client(5.0.02075)
- Cisco DUO 인증 프록시(6.0.1)
- Mac OS(13.4.1)
- 액티브 디렉토리

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.

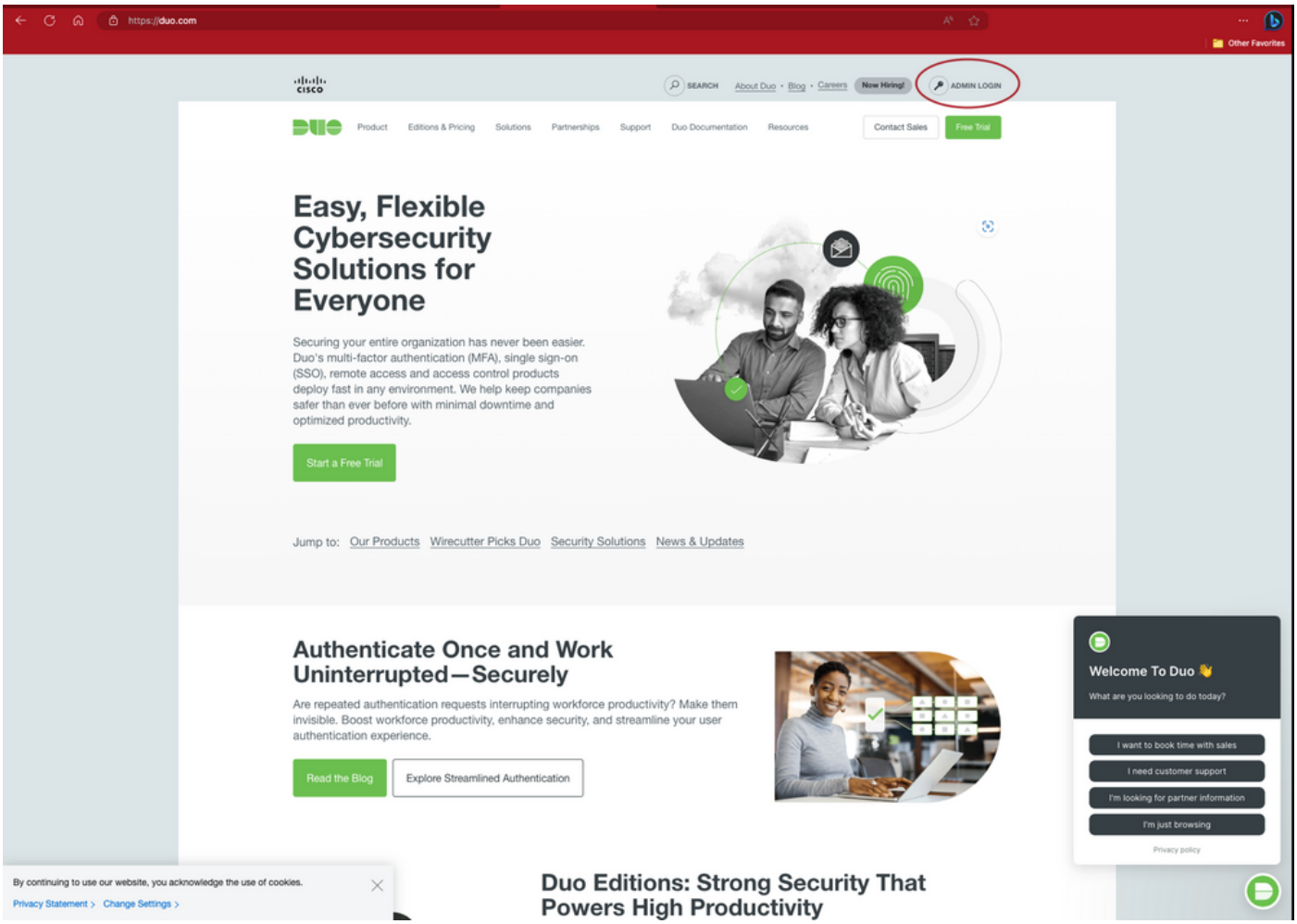
DUO에서 단계 구성

이 섹션에서는 Cisco DUO SSO(Single Sign-On)를 구성하는 단계에 대해 설명합니다. 시작하기 전에 인증 프록시를 구현해야 합니다.

경고: 인증 프록시가 구현되지 않은 경우 이 링크에는 이 작업에 대한 지침이 있습니다. DUO 인증 프록시 설명서

애플리케이션 보호 정책 생성

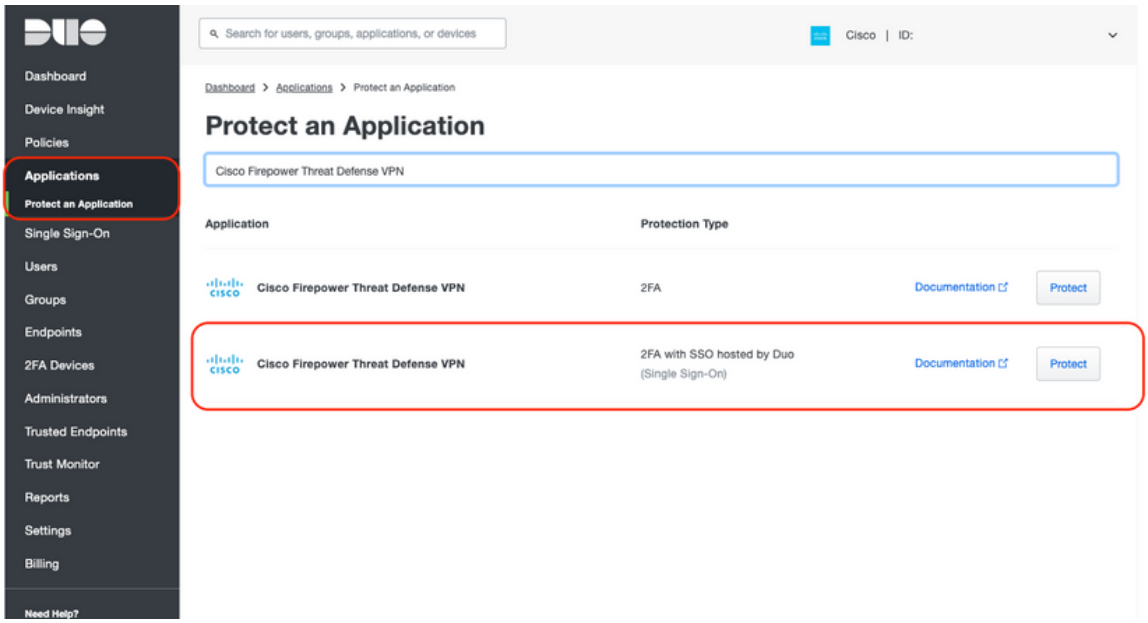
1단계. Cisco Duo 링크를 통해 관리자 패널에 로그인합니다.



Cisco DUO 홈페이지

2단계. Dashboard(대시보드) > Applications(애플리케이션) > Protect an Application(애플리케이션 보호)으로 이동합니다.

검색 표시줄에서 "Cisco Firepower Threat Defense VPN"을 입력하고 "Protect"를 선택합니다.



애플리케이션 스크린샷 보호

Protection Type(보호 유형)이 "2FA with SSO with Duo hosted(Duo가 호스팅하는 SSO가 있는 2FA)"인 옵션을 선택합니다.

3단계: 메타데이터 아래에서 이 URL 정보를 복사합니다.

- ID 공급자 엔티티 ID
- SSO URL
- 로그아웃 URL

복사할 정보의 예

참고: 스크린샷에서 링크가 생략되었습니다.

4단계. Downloads(다운로드) 아래에서 ID 공급자 인증서를 다운로드하려면 "Download certificate(인증서 다운로드)"를 선택합니다.

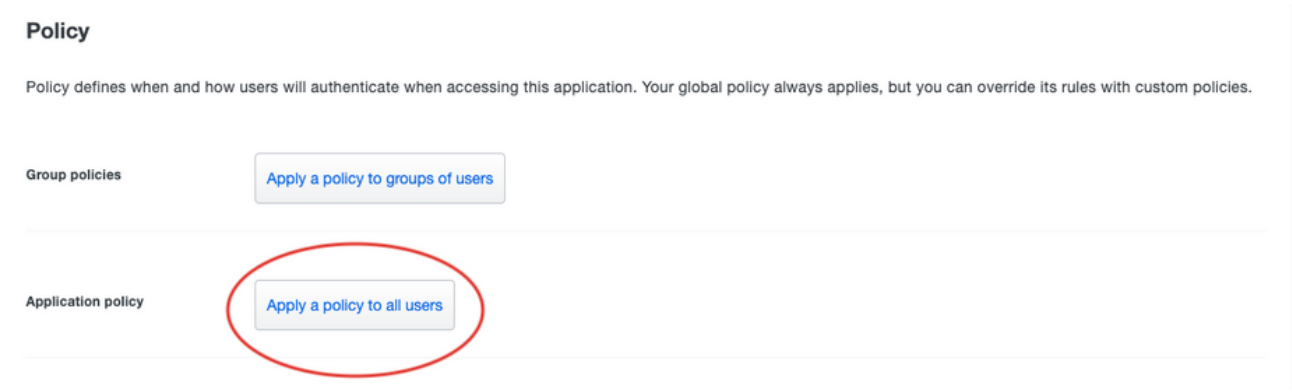
5단계. 서비스 공급자 정보 입력

Cisco Firepower Base URL - FTD에 연결하는 데 사용되는 FQDN

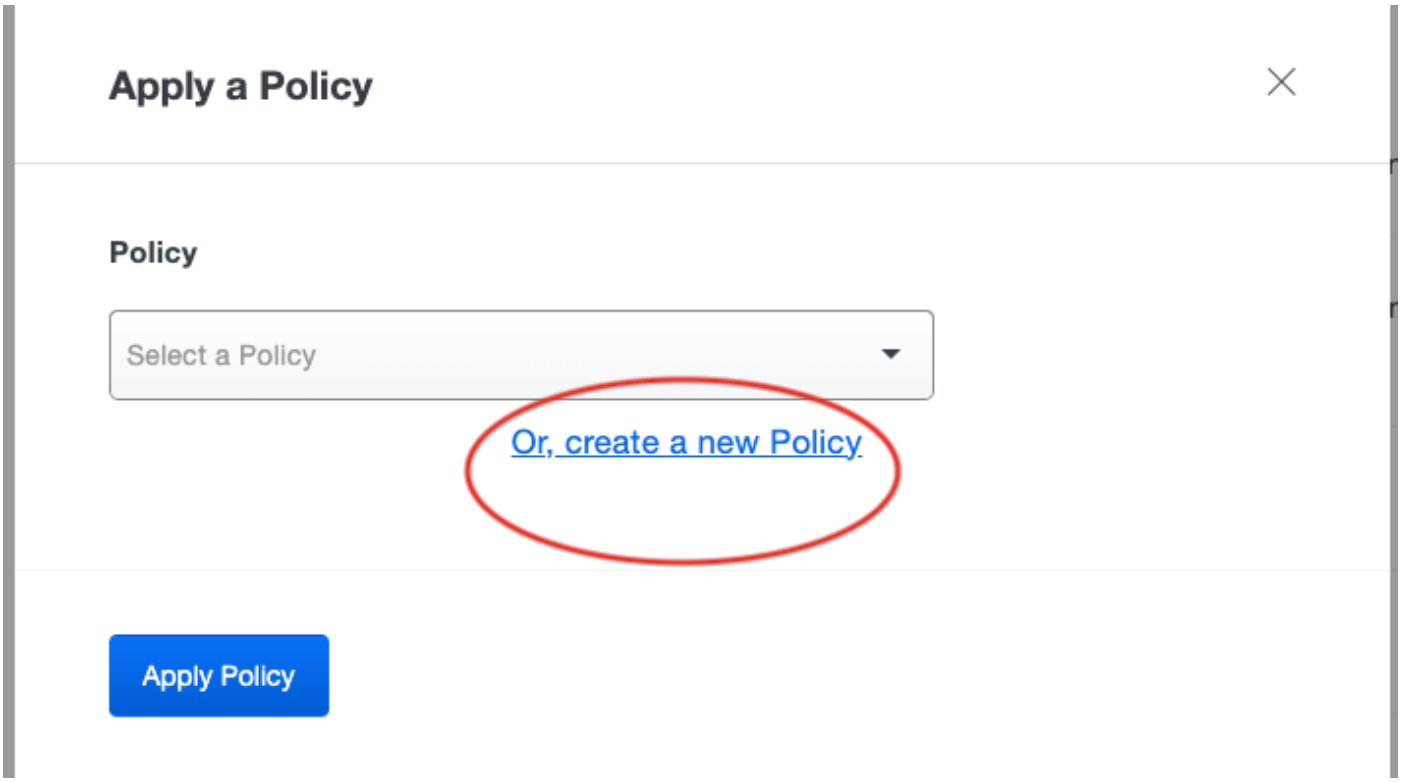
Connection Profile Name(연결 프로파일 이름) - 터널 그룹 이름

애플리케이션 정책 생성

1단계: Policy(정책)에서 Application Policy(애플리케이션 정책)를 생성하려면 "Apply a policy to all users(모든 사용자에게 정책 적용)"를 선택한 다음 이미지와 같이 "Or, create a new Policy(또는 새 정책 생성)"를 선택합니다.

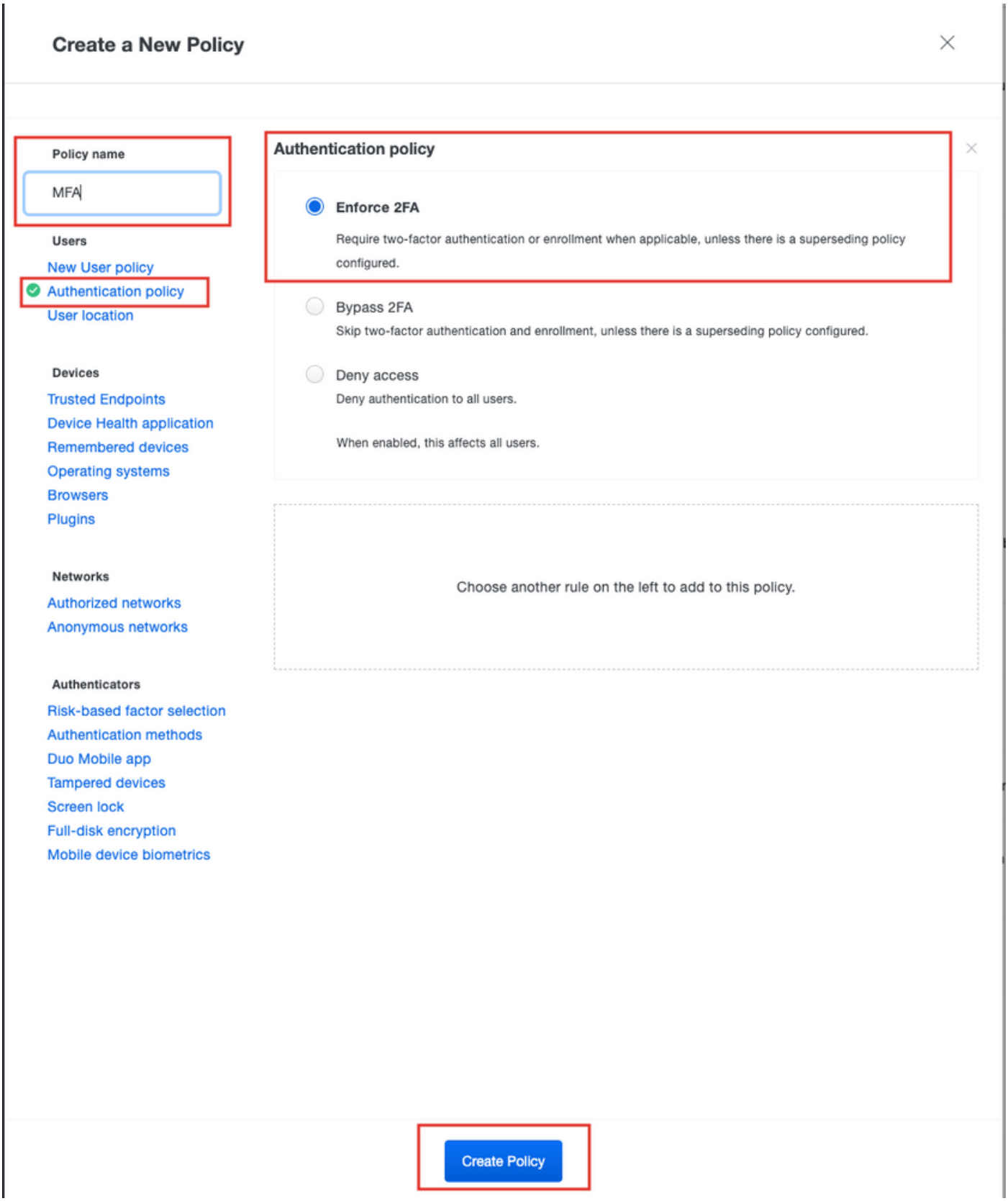


애플리케이션 정책 생성의 예



애플리케이션 정책 생성의 예

2단계. Policy name(정책 이름)에서 원하는 이름을 입력하고 Users(사용자) 아래에서 "Authentication policy(인증 정책)"를 선택한 다음 "2FA 시행." 그런 다음 "Create Policy(정책 생성)"를 사용하여 저장합니다.



애플리케이션 정책 생성의 예

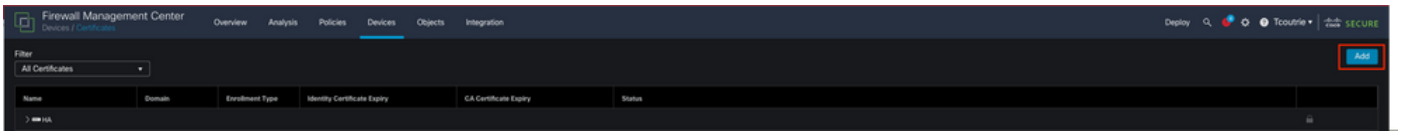
3단계. 다음 창에 "Apply Policy(정책 적용)"로 정책을 적용합니다. 그런 다음 페이지 아래쪽으로 스크롤하고 "저장"을 선택하여 DUO 컨피그레이션을 완료합니다

FMC 구성 단계

FTD에 ID 인증서 구축

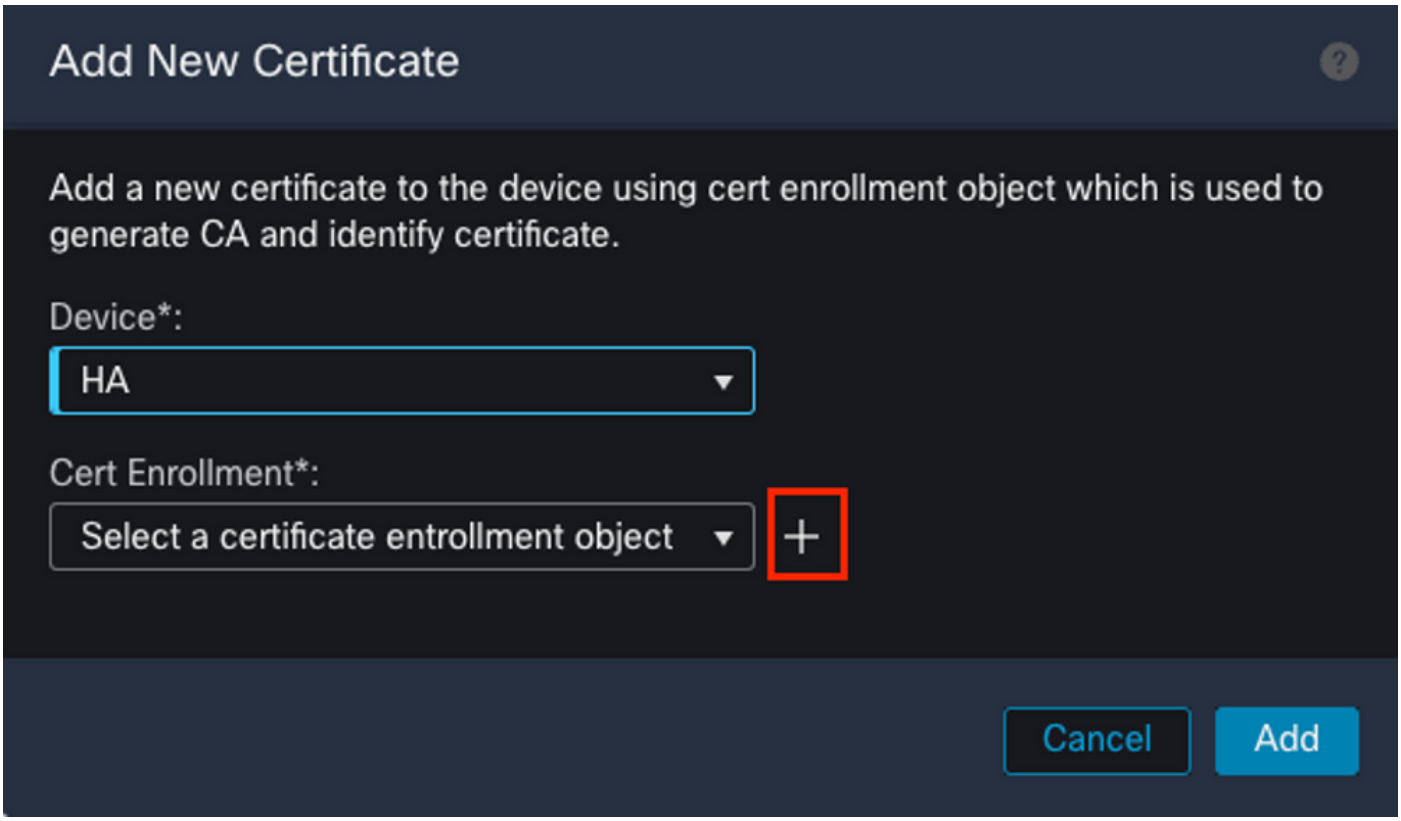
이 섹션에서는 인증서 인증에 필요한 FTD에 ID 인증서를 구성하고 배포하는 방법에 대해 설명합니다. 시작하기 전에 모든 구성을 배포해야 합니다.

1단계. 이미지에 표시된 대로 Devices(디바이스) > Certificate(인증서)로 이동하고 Add(추가)를 선택합니다.



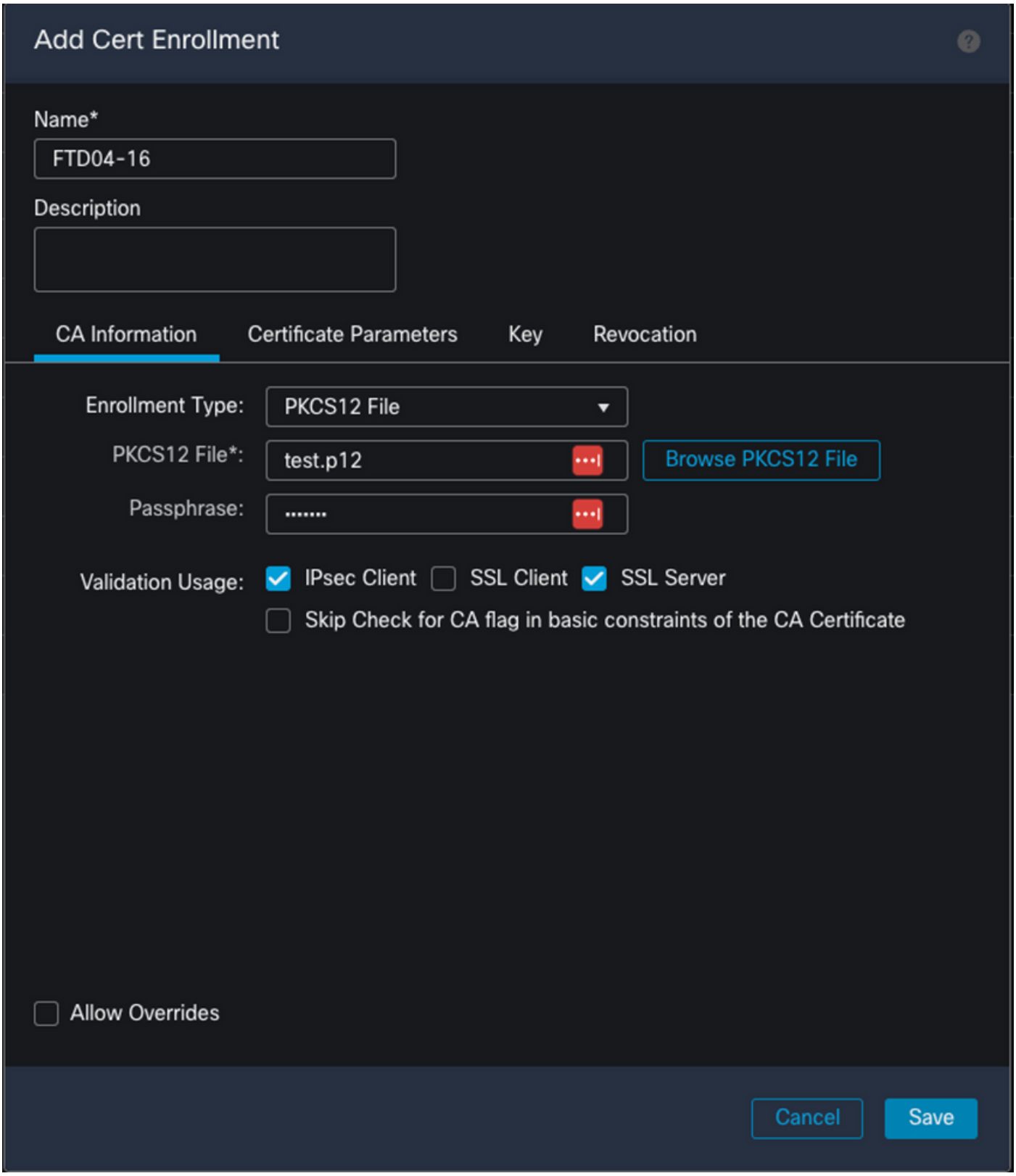
디바이스/인증서 스크린샷

2단계: 디바이스 드롭다운에서 FTD 어플라이언스를 선택합니다. 새 인증서 등록 방법을 추가하려면 + 아이콘을 클릭합니다.



Add New Certificate(새 인증서 추가)의 스크린 샷

3단계: 이미지에 표시된 대로 "Enrollment Type"(등록 유형)을 통해 환경에서 인증서를 얻기 위해 선호하는 방법인 옵션을 선택합니다.



새 인증서 등록 페이지의 스크린샷

팁: 사용 가능한 옵션은 다음과 같습니다. 자체 서명 인증서 - 로컬에서 새 인증서 생성, SCEP - Simple Certificate Enrollment Protocol을 사용하여 CA에서 인증서 가져오기, 수동 - 루트 및 ID 인증서 수동 설치, PKCS12 - 루트, ID 및 개인 키로 암호화된 인증서 번들 업로드

IDP 인증서를 FTD에 구축

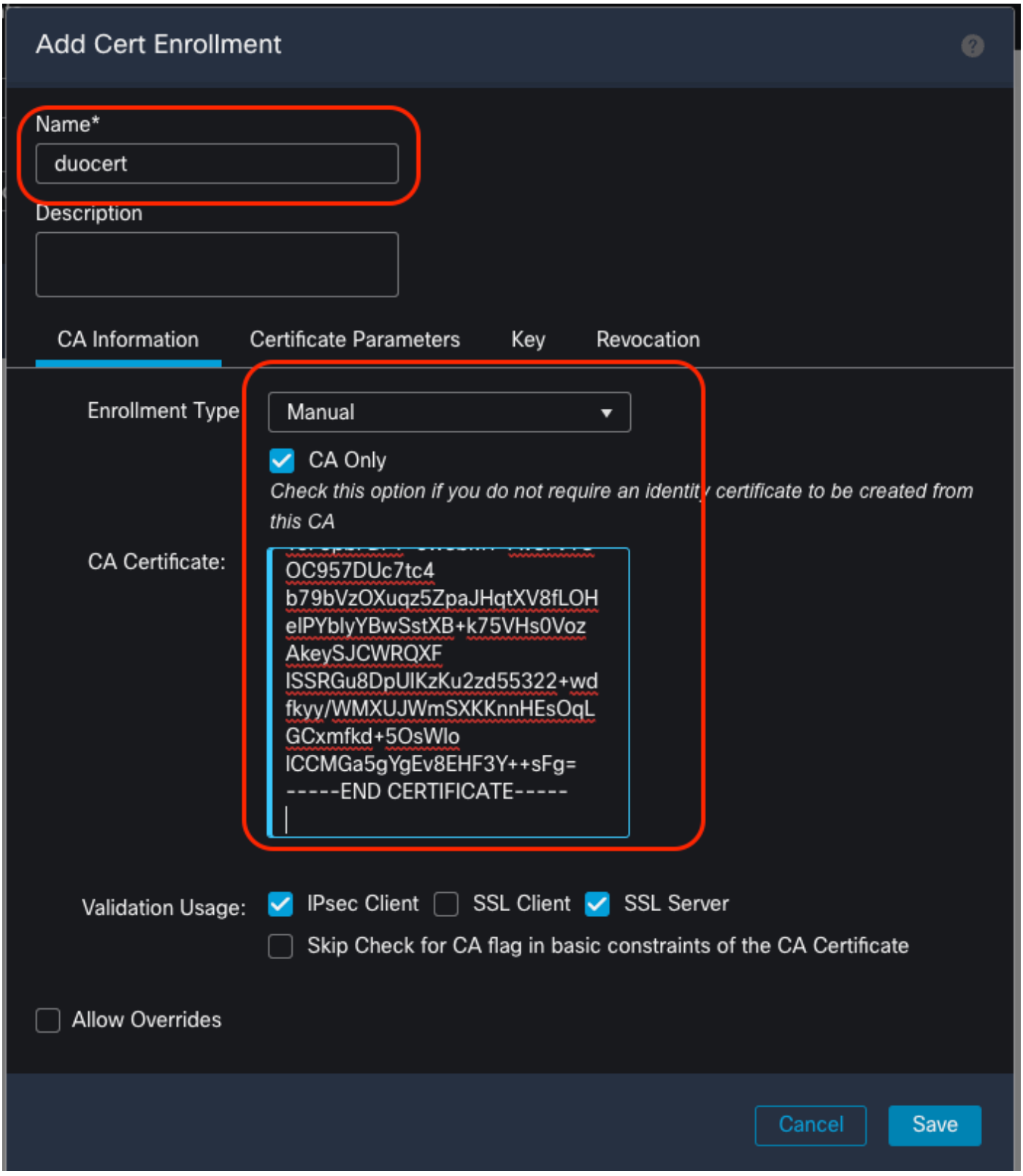
이 섹션에서는 IDP 인증서를 구성하고 FTD에 배포하는 방법에 대해 설명합니다. 시작하기 전에 모든 구성을 배포해야 합니다.

1단계: Devices(디바이스) > Certificate(인증서)로 이동하고 Add(추가)를 선택합니다."

2단계: 디바이스 드롭다운에서 FTD 어플라이언스를 선택합니다. 새 인증서 등록 방법을 추가하려면 + 아이콘을 클릭합니다.

3단계: Add Cert Enrollment(인증서 등록 추가) 창에서 이미지에 표시된 대로 필요한 정보를 입력한 다음 이미지에 표시된 대로 "Save(저장)"를 입력합니다.

- 이름: 객체의 이름
- 등록 유형: 수동
- 확인란 활성화: CA만
- CA 인증서: 인증서의 PEM 형식

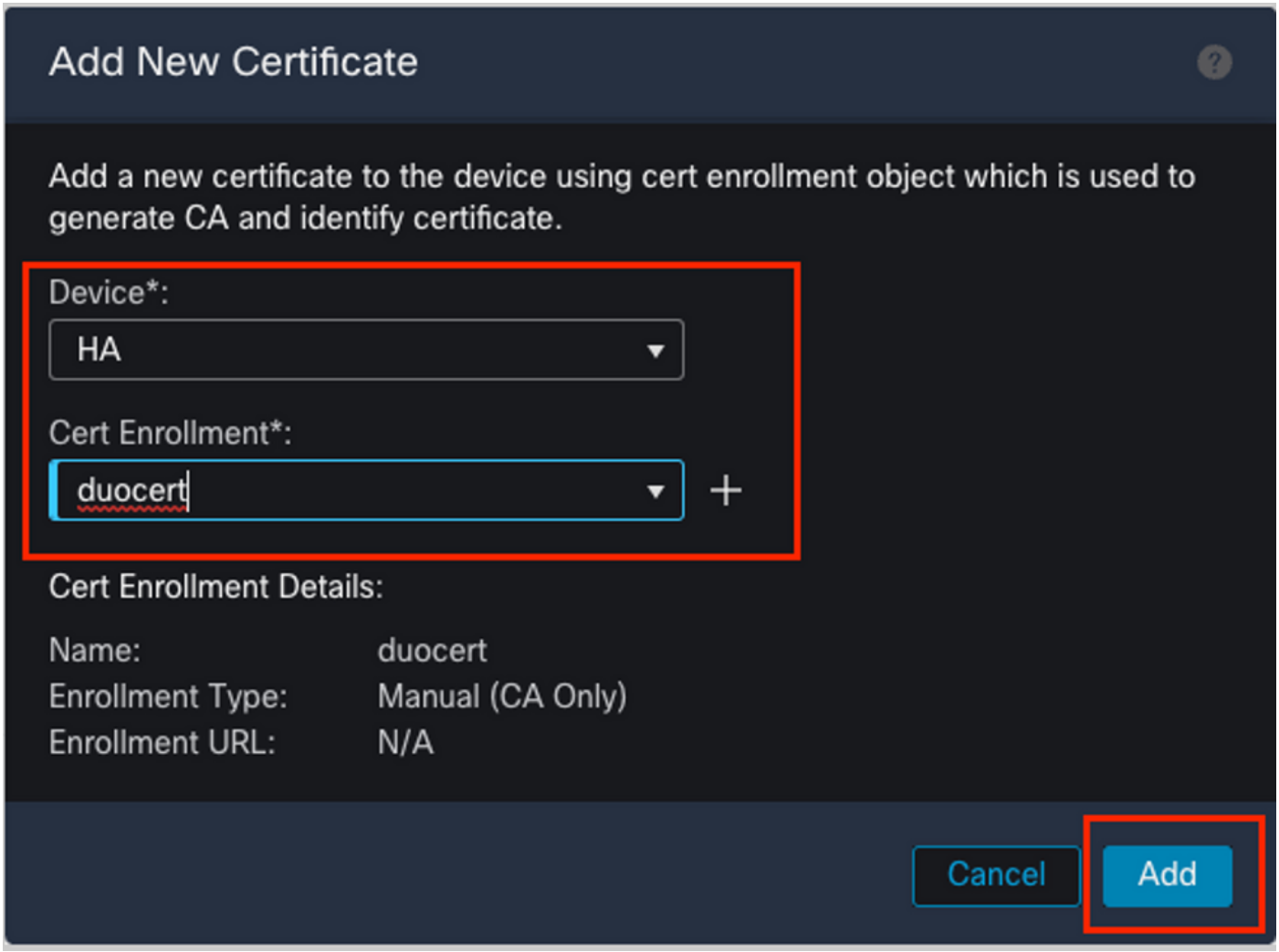


인증서 등록 객체를 만드는 예

⚠ 주의: 필요한 경우 "CA 인증서의 기본 제약 조건에서 CA 플래그에 대한 검사 건너뛰기"를 사용할 수 있습니다. 이 옵션은 주의하여 사용하십시오.

4단계: "Cert Enrollment*:" 아래에서 새로 생성된 인증서 등록 객체를 선택한 다음 그림과 같이

"Add"를 선택합니다.



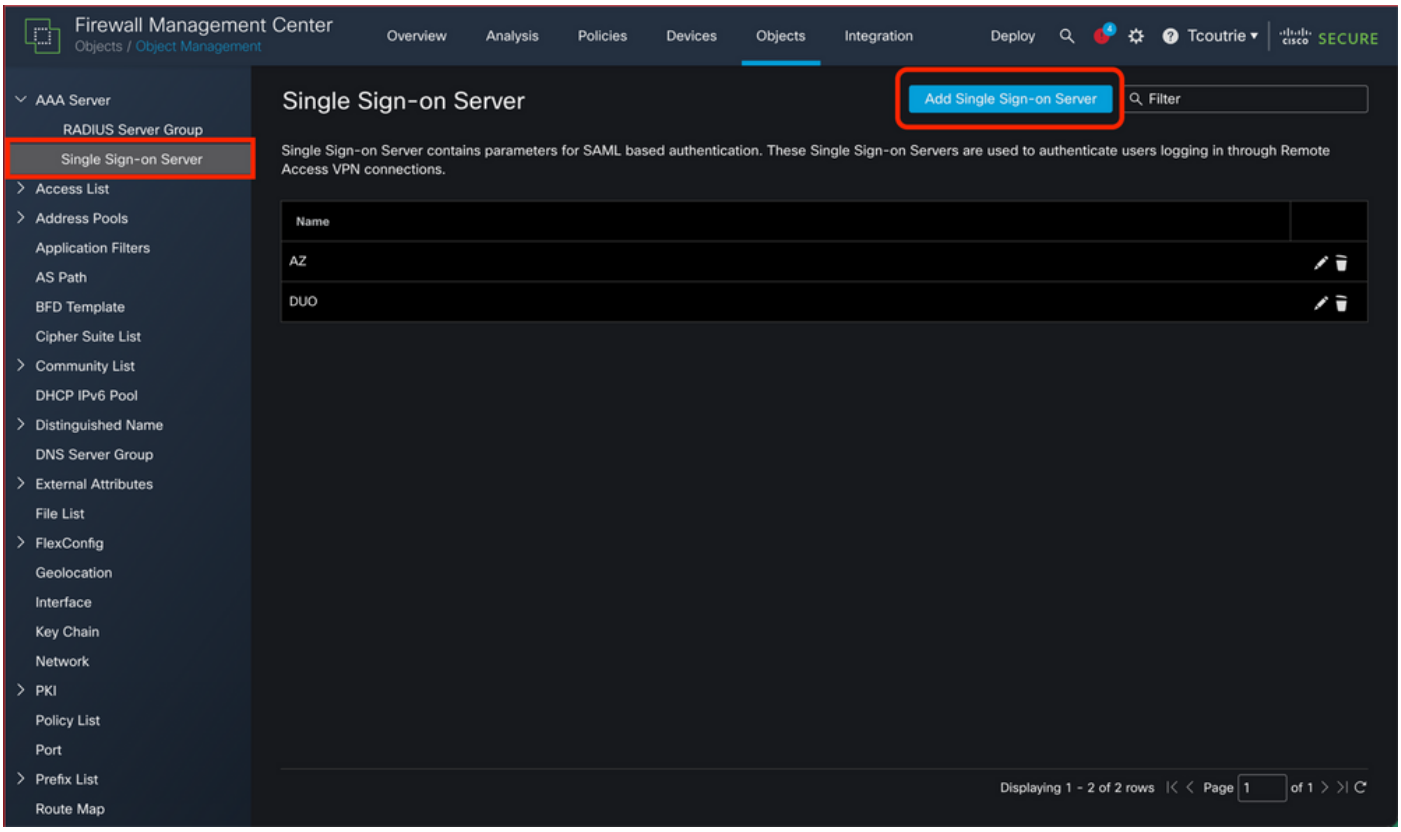
추가된 인증서 등록 개체 및 장치의 스크린샷

참고: 인증서가 추가되면 즉시 ' 구축됩니다.

SAML SSO 객체 생성

이 섹션에서는 FMC를 통해 SAML SSO를 구성하는 단계를 설명합니다. 시작하기 전에 모든 구성을 배포해야 합니다.

1단계. Objects(개체) > AAA Server(AAA 서버) > Single Sign-on Server(단일 로그인 서버)로 이동하고 "Add Single Sign-on Server(단일 로그인 서버 추가)"를 선택합니다.

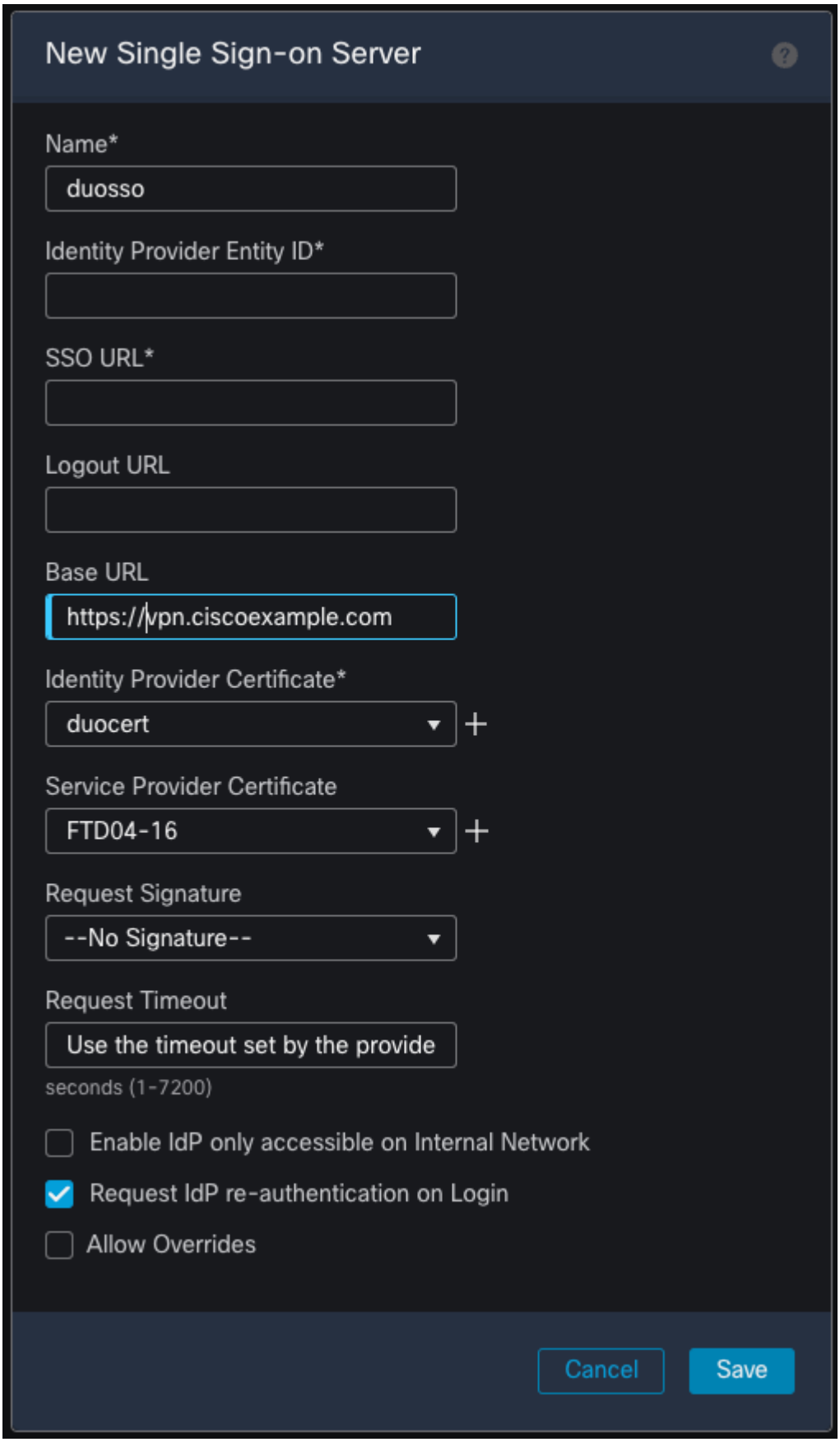


새 SSO 객체 생성 예

2단계. "Create an Application Protection Policy(애플리케이션 보호 정책 생성)"에서 필요한 정보 입력

". 완료되면 계속하려면 "저장"을 선택하십시오."

- 이름*: 개체 이름
- ID 공급자 엔티티 ID*: 3단계의 엔티티 ID
- SSO URL*: 3단계에서 복사한 로그인 URL
- 로그아웃 URL: 3단계에서 복사한 로그아웃 URL
- 기본 URL: 5단계에서 "Cisco Firepower Base URL"과 동일한 FQDN 사용
- ID 공급자 인증서*: 배포된 IDP 인증서
- 서비스 공급자 인증서: FTD 외부 인터페이스의 인증서



새 SSO 객체의 예

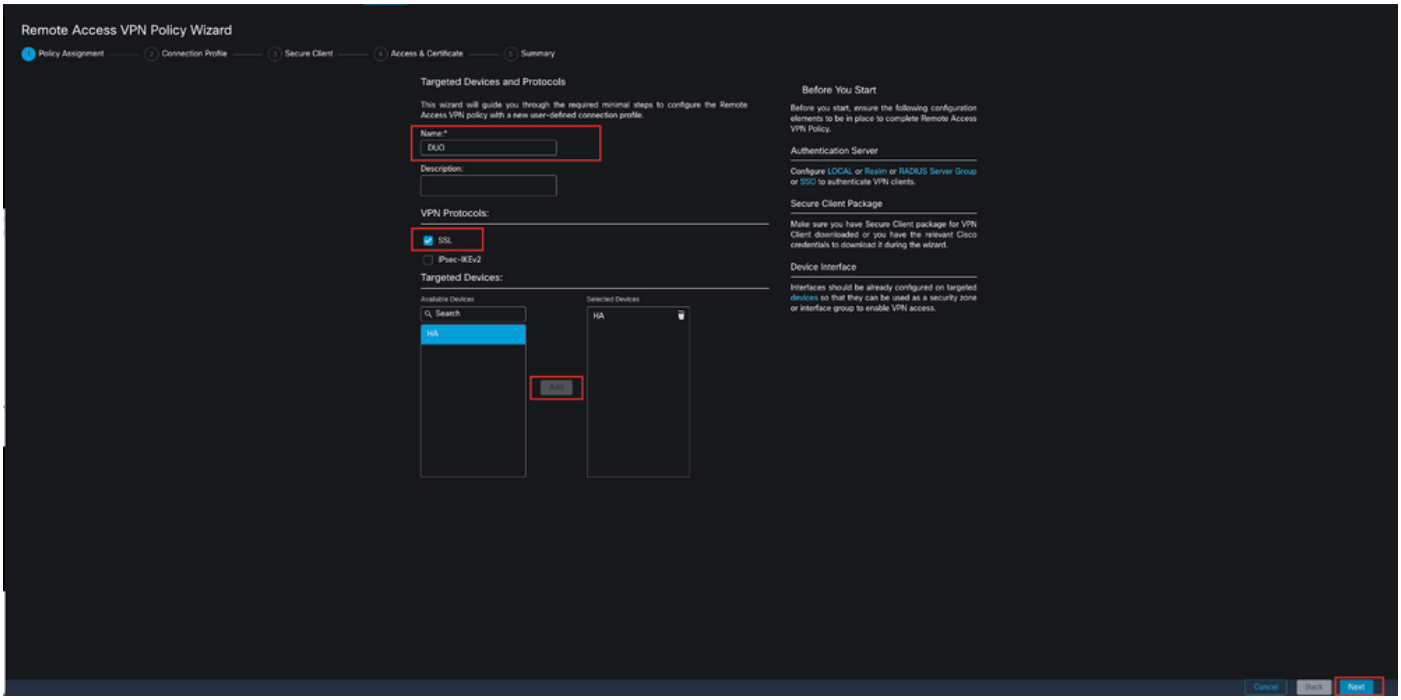
참고: 엔터티 ID, SSO URL 및 로그아웃 URL 링크가 스크린샷에서 생략되었습니다

RAVPN(Remote Access Virtual Private Network) 컨피그레이션 생성

이 섹션에서는 마법사를 사용하여 RAVPN을 구성하는 단계를 설명합니다.

1단계. Devices(디바이스) > Remote Access(원격 액세스)로 이동하여 "Add(추가)"를 선택합니다.

2단계. 마법사에서 새 RAVPN 정책 마법사의 이름을 입력하고 VPN Protocols: Add the Targeted Devices(VPN 프로토콜: 대상 장치 추가)에서 SSL을 선택합니다. 완료되면 "Next(다음)"를 선택합니다.



RAVPN 마법사의 1단계

2단계. Connect Profile(연결 프로파일)에서 옵션을 설정합니다(여기에 표시됨). 완료되면 "Next(다음)"를 선택합니다.

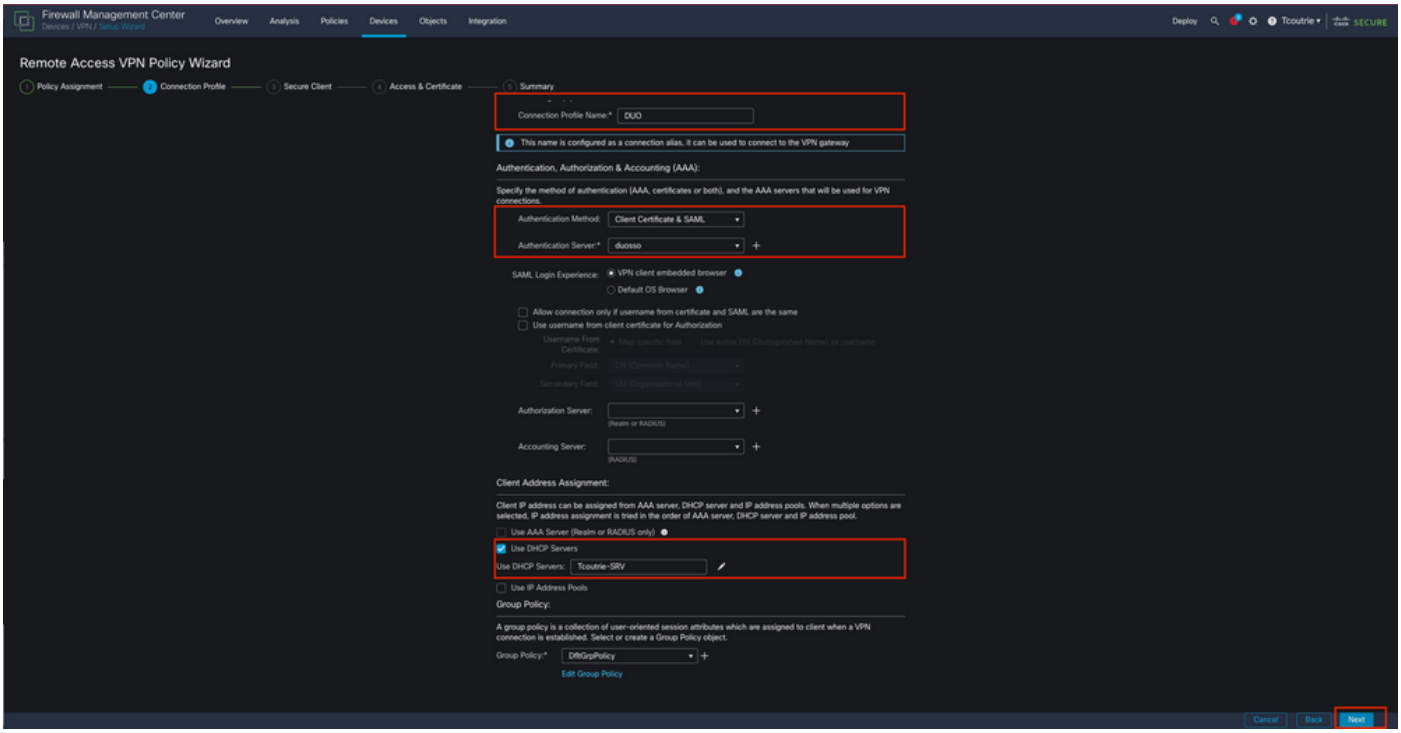
- 연결 프로파일 이름: "애플리케이션 보호 정책 생성"의 5단계에서 터널 그룹 이름을 사용합니다.

인증, 권한 부여 및 계정 관리(AAA):

- 인증 방법: 클라이언트 인증서 및 SAML
- 인증 서버:* "SAML SSO 객체 생성" 중에 생성된 SSO 객체를 선택합니다.

클라이언트 주소 할당:

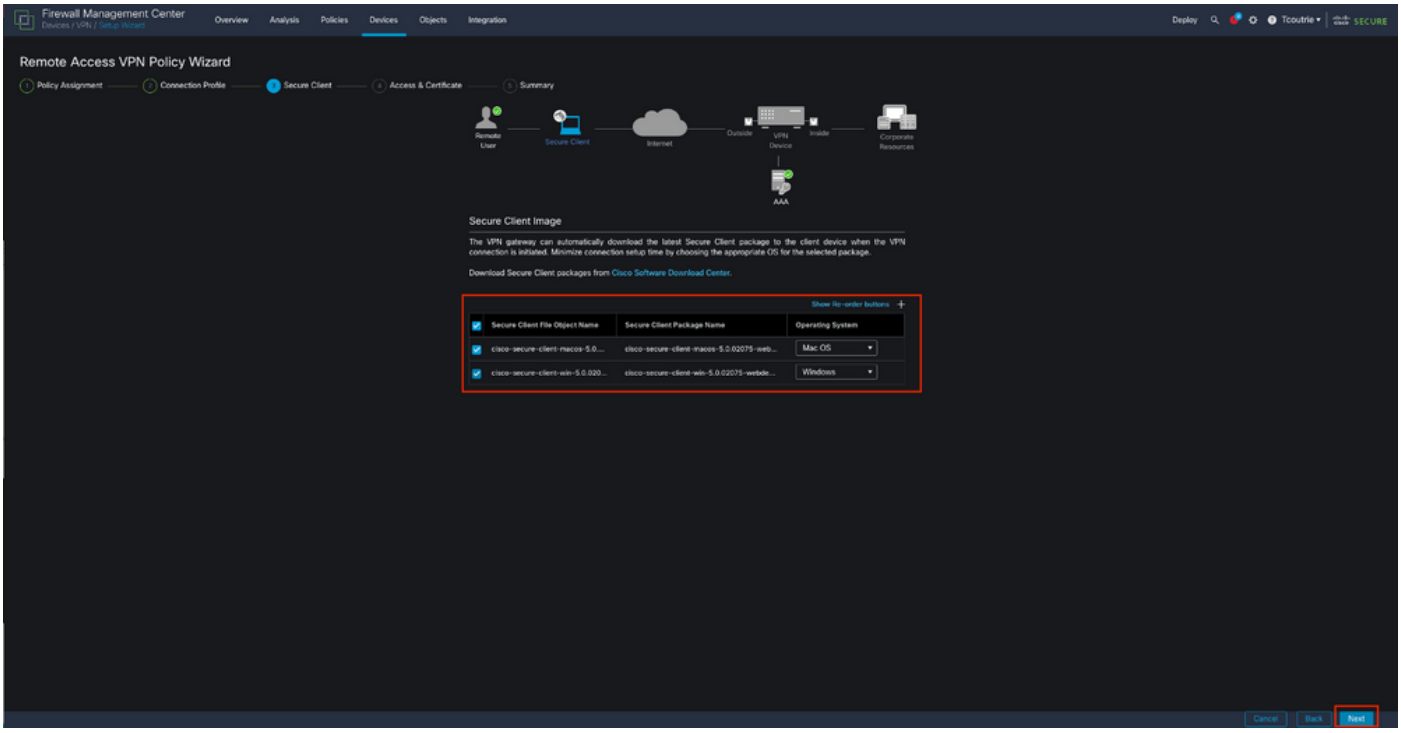
- Use AAA Server(AAA 서버 사용)(Realm(영역) 또는 RADIUS에만 해당) - Radius 또는 LDAP
- DHCP 서버 사용 - DHCP 서버
- FTD에서 IP 주소 풀 사용 - 로컬 풀



RAVPN 마법사의 2단계

팁: 이 실습에서는 DHCP 서버가 사용됩니다.

3단계. 구축할 Cisco Secure Client의 웹 구축 이미지를 업로드하려면 "+"를 선택합니다. 그런 다음 구축할 CSC 이미지의 확인란을 선택합니다. 그림과 같이. 완료되면 "다음"을 선택합니다.

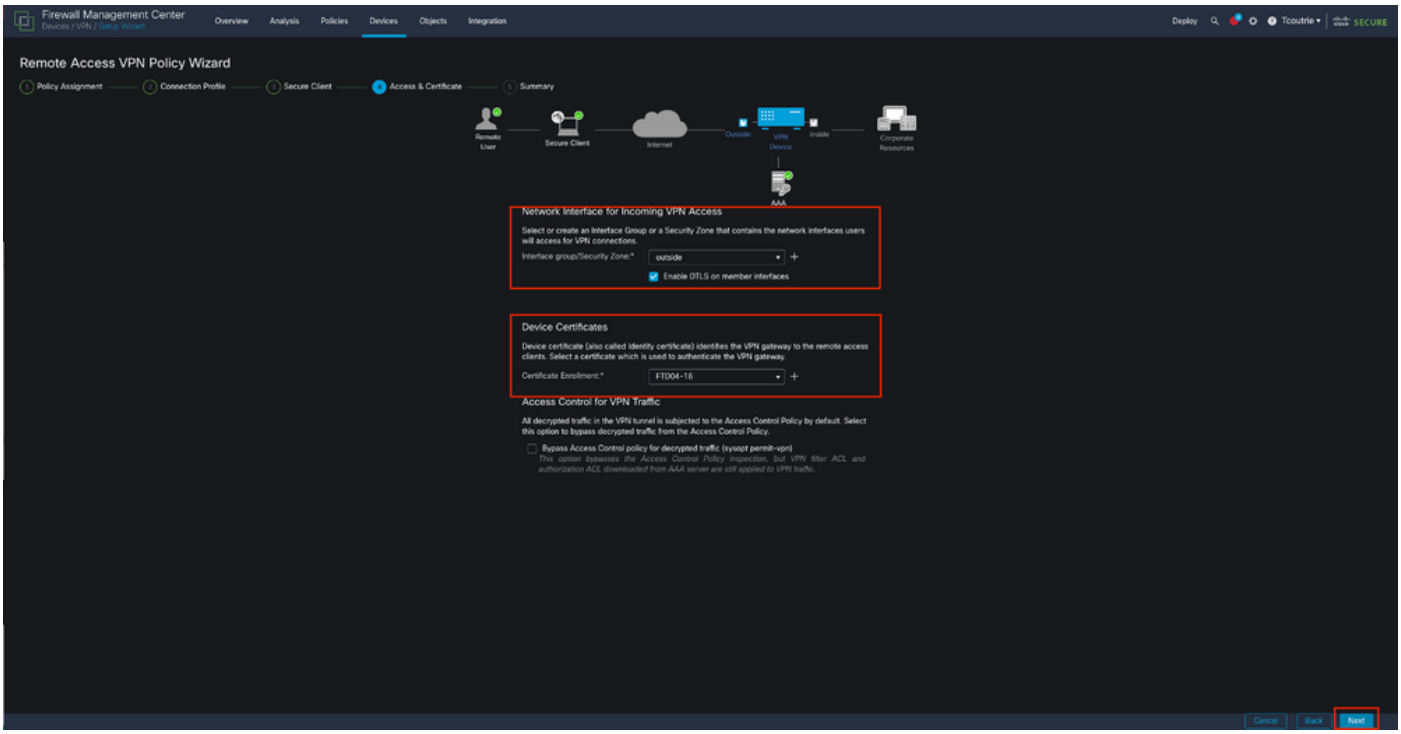


3단계 RAVPN 마법사

4단계. 이 개체를 설정합니다(그림에 표시된 대로). 완료되면 "다음"을 선택합니다.

인터페이스 그룹/보안 영역:*: 외부 인터페이스

"인증서 등록:*": 이 설명서의 "FTD에 ID 인증서 구축" 과정에서 생성된 ID 인증서

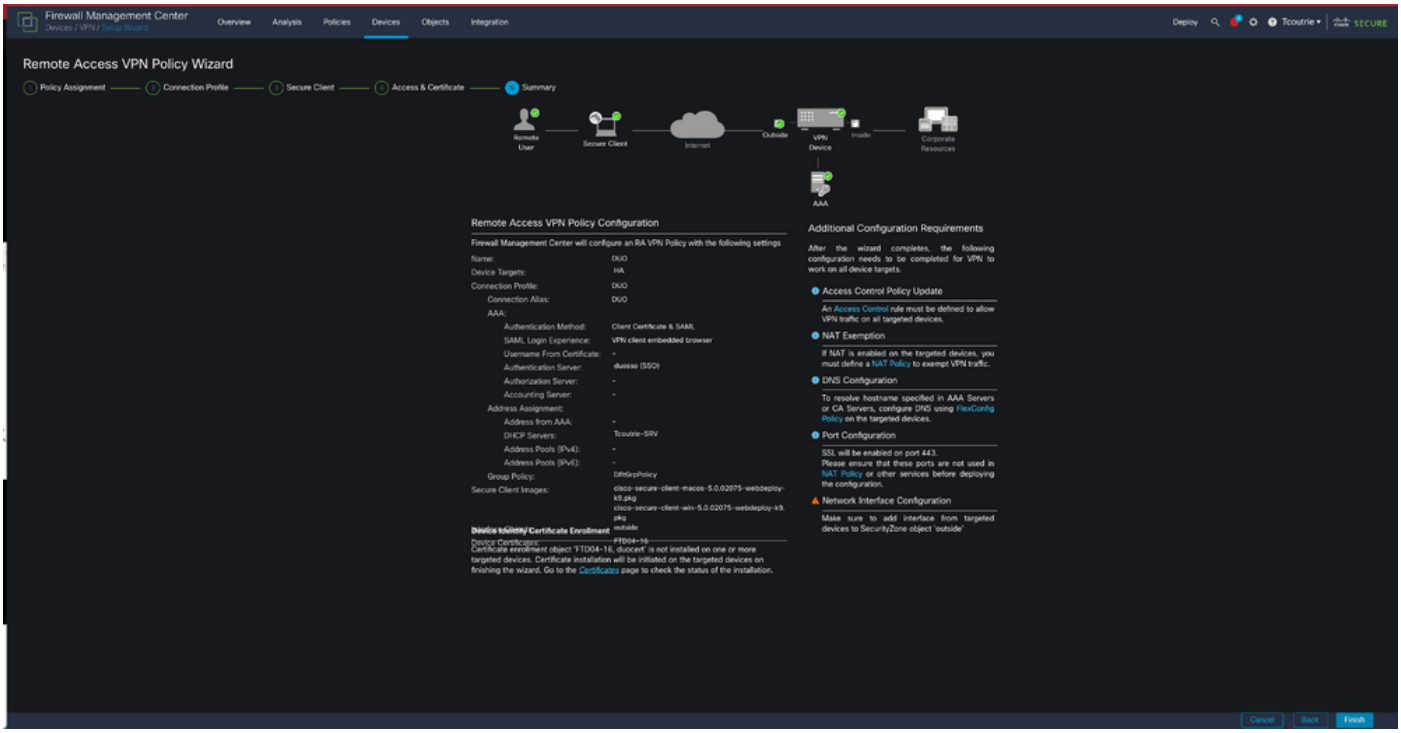


RAVPN 마법사의 4단계

팁: 아직 만들지 않은 경우 "+"를 선택하여 새 인증서 등록 객체를 추가합니다.

6단계. 요약

모든 정보를 확인합니다. 모든 것이 올바르면 '마침'을 계속하십시오.



요약 페이지

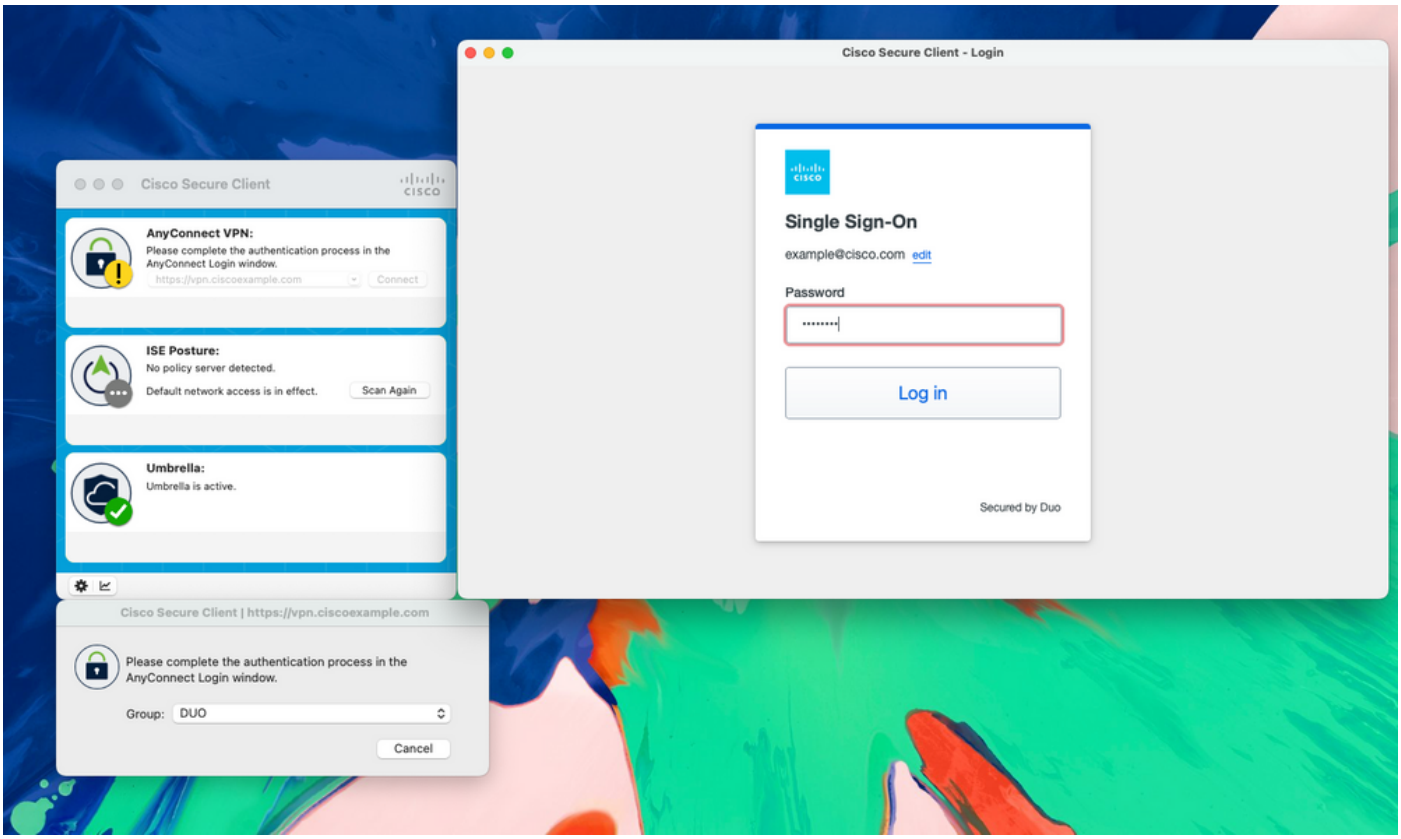
7단계. 새로 추가된 컨피그레이션을 구축합니다.

다음을 확인합니다.

이 섹션에서는 성공적인 연결 시도 확인에 대해 설명합니다.

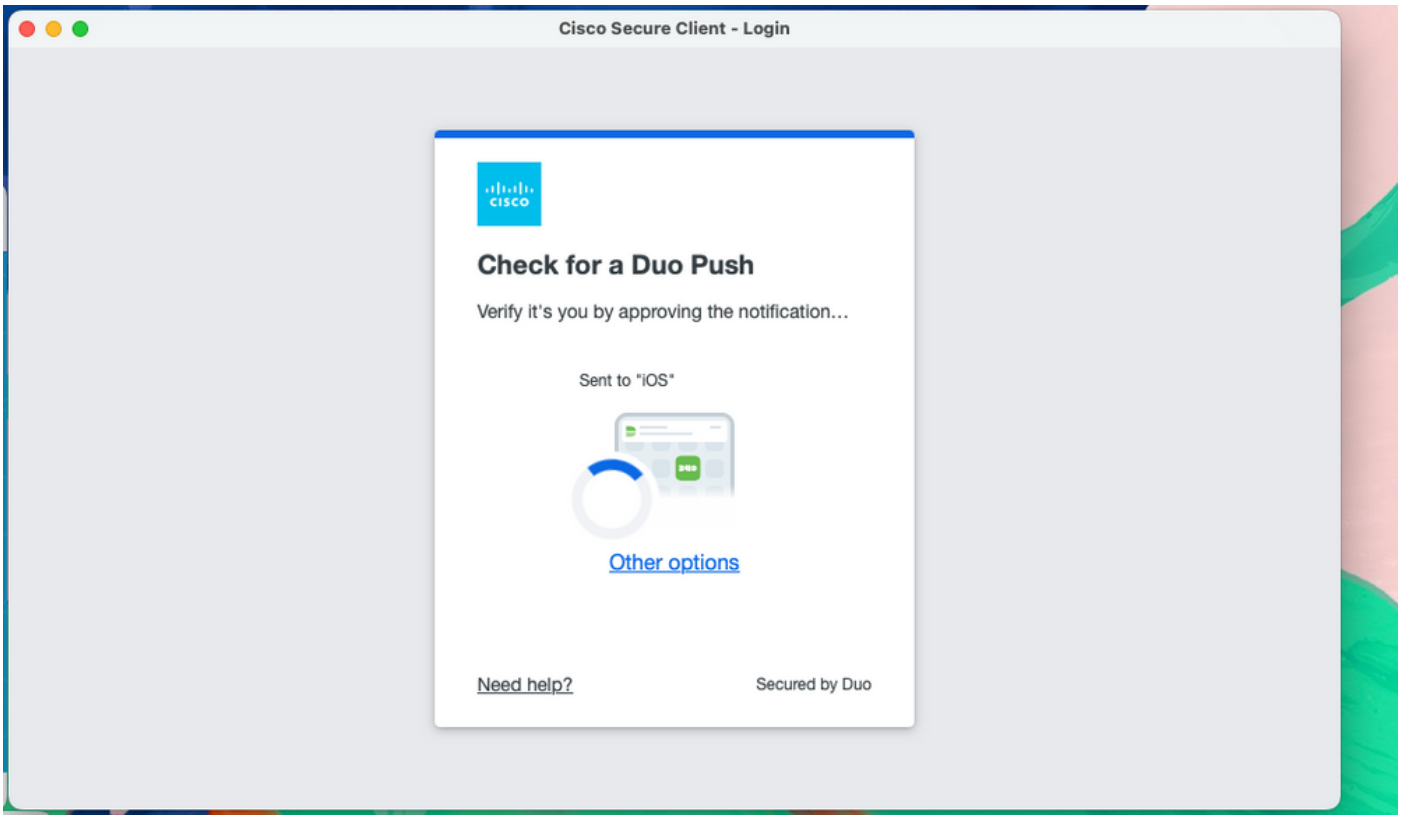
Cisco Secure Client를 열고 FTD의 FQDN을 입력하고 연결합니다.

SSO 페이지에서 자격 증명을 입력합니다.



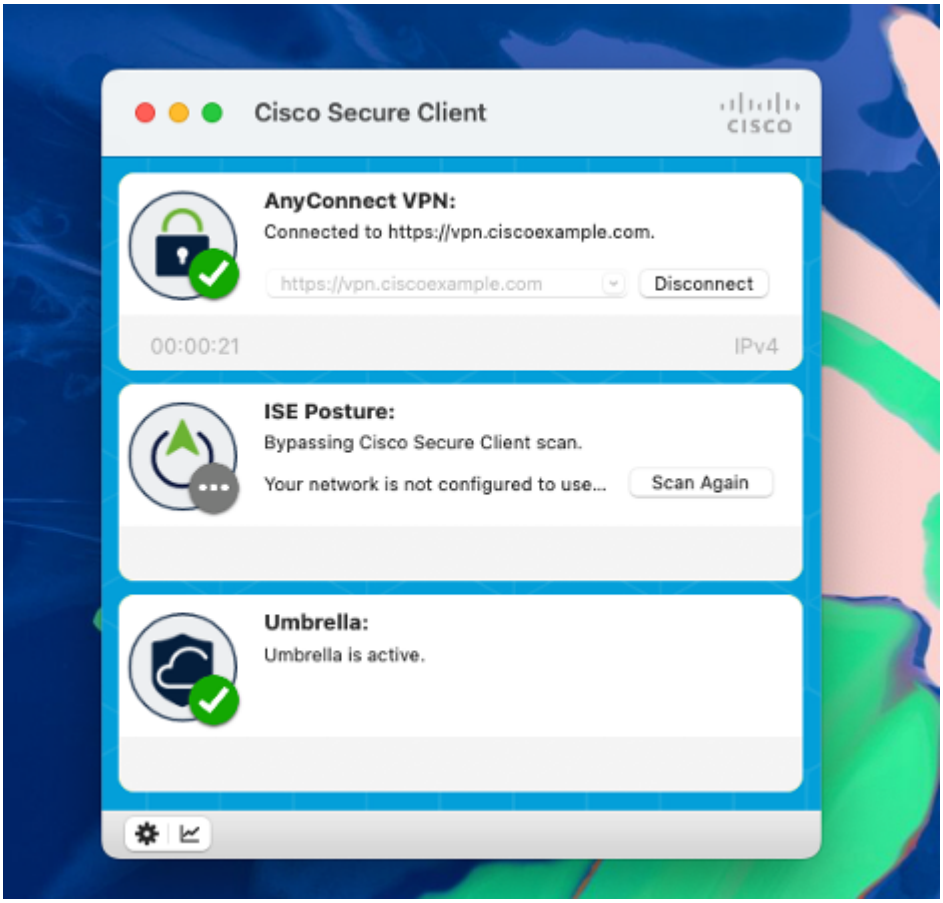
Cisco Secure Client를 통한 SSO 페이지

등록된 디바이스에 대한 DUO 푸시를 수락합니다.



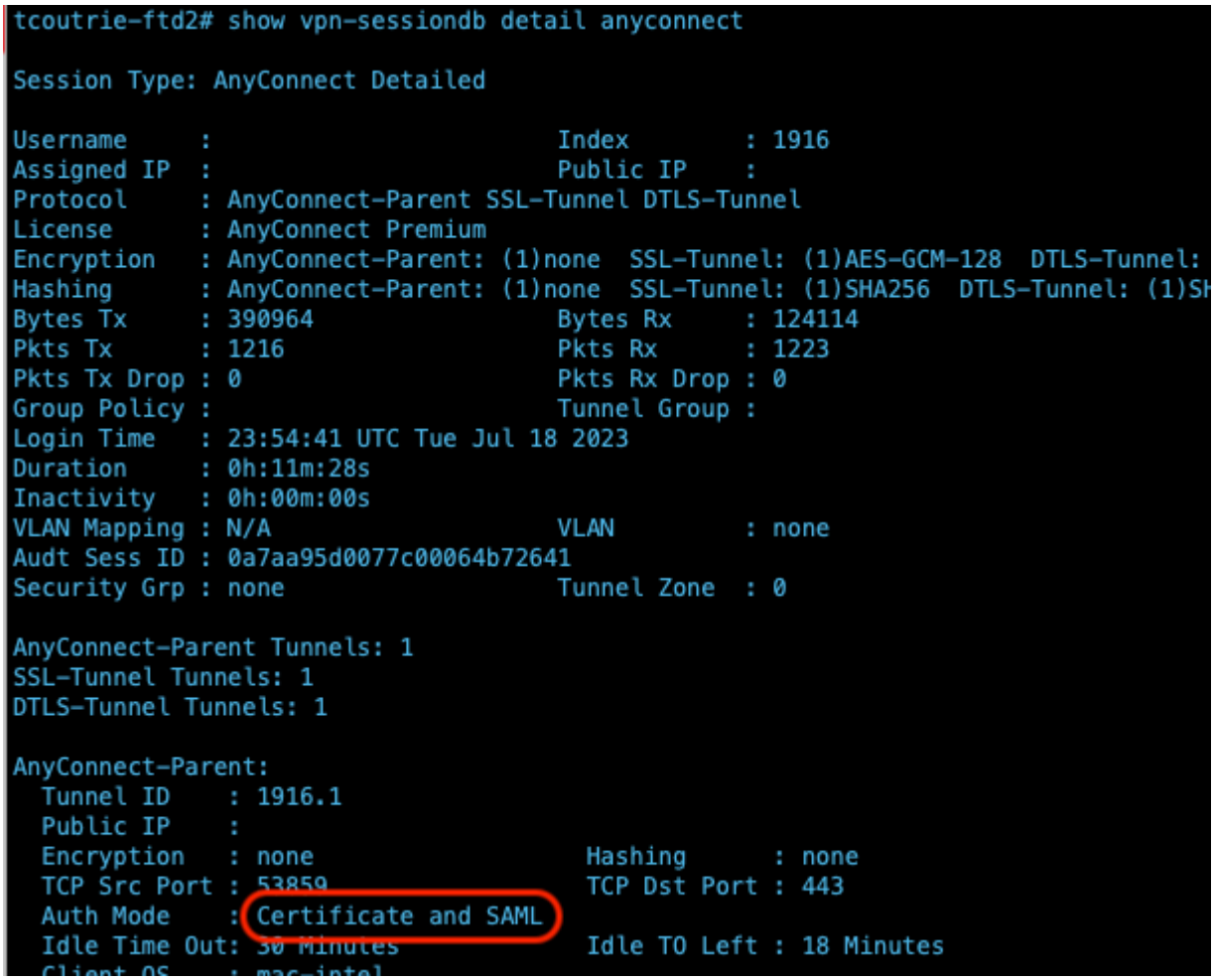
듀오 푸시

연결에 성공했습니다.



FTD에 연결됨

다음 명령을 사용하여 FTD의 연결을 확인합니다. show vpn-sessiondb detail anyconnect



출력 예제에서 일부 정보가 생략되었습니다.

문제 해결

이는 구현 이후에 발생할 수 있는 문제일 수 있다.

문제 1: 인증서 인증에 실패했습니다.

루트 인증서가 FTD에 설치되었는지 확인합니다.

다음 디버그를 사용합니다.

debug crypto ca 14

debug aaa shim 128

debug aaa common 128

문제 2: SAML 실패

이러한 디버그를 사용하여 문제를 해결할 수 있습니다.

debug aaa shim 128

debug aaa common 128

webvpn anyconnect 128 디버그

디버그 webvpn saml 255

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.