SCC에서 온프레미스 매니지드 FMC로 유니버설 ZTNA에 대한 보안 액세스 구성

목차

소개

이 문서에서는 온프레미스 가상 FMC에서 관리하는 보안 액세스 및 가상 FTD를 사용하여 Universal ZTNA를 구성하는 방법에 대해 설명합니다.

사전 요구 사항

- FMC(Firewall Management Center) 및 FTD(Firewall Threat Defense)는 7.7.10 이상의 소프트웨어 버전을 사용하여 구축해야 합니다.
- FTD(Firewall Threat Defense)는 FMC(Firewall Management Center)에서 관리해야 함
- FTD(Firewall Threat Defense)는 보안 제어에 필요한 암호화, IPS 및 위협 라이센스와 함께 라

이센스가 있어야 합니다(내보내기 기능을 활성화하면 강력한 암호화를 활성화해야 함).
- FTD(Firewall Threat Defense)의 기본 컨피그레이션은 인터페이스, 라우팅 등 FMC(Firewall Management Center)에서 수행해야 합니다.
- 앱의 FQDN을 확인하기 위해 FMC의 디바이스에 DNS 컨피그레이션을 적용해야 함
- Cisco Secure Client 버전은 5.1.10 이상이어야 합니다.
- 방화벽 및 Secure Access Micro Apps, UZTNA 기능 플래그가 활성화된 고객에게 보안 클라우드 제어가 프로비저닝됨

요구 사항

- cdFMC 및 FTD(Firewall Threat Defense) 디바이스를 포함한 모든 FMC(Secure Firewall Management Center)는 소프트웨어 버전 7.7.10 이상을 실행해야 합니다.
- FTD(Firewall Threat Defense)는 Firewall Management Center에서 관리해야 합니다. 로컬 관리자 FDM(Firewall Defense Manager)은 지원되지 않습니다.
- 모든 FTD(Firewall Threat Defense) 디바이스는 라우팅 모드로 구성해야 합니다. 투명 모드는 지원되지 않습니다.
- 클러스터링된 디바이스는 지원되지 않습니다.
- HA(High Availability) 디바이스 지원 하나의 엔티티로 표시됩니다.
- Secure Client 버전 5.1.10 이상

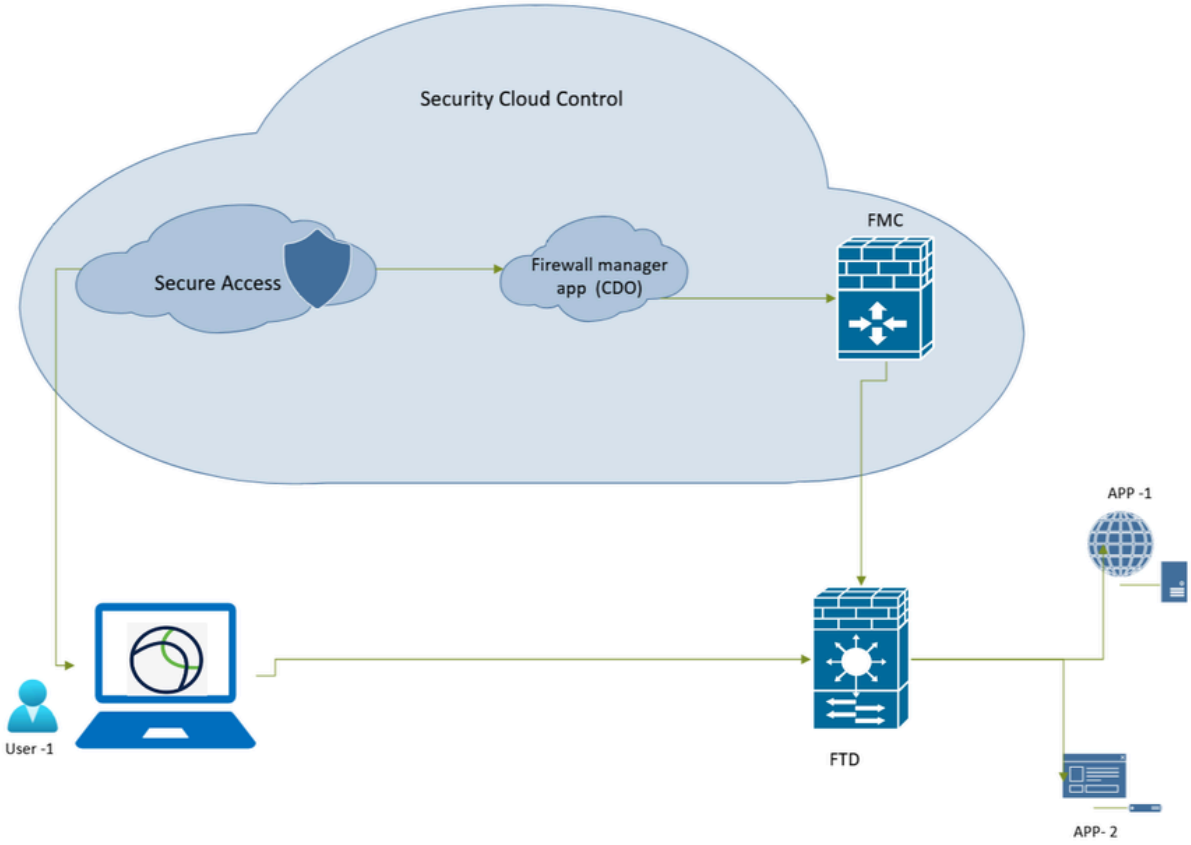
사용되는 구성 요소

이 문서의 정보는

- 보안 클라우드 제어(SCC)
- FMC(Secure Firewall Management Center) 버전 7.7.10
- FTD(Secure Firewall Threat Defense) 가상 -100 버전 7.7.10
- Secure Client for Windows 버전 5.1.10
- 보안 액세스

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.

네트워크 다이어그램



보안 액세스 - 네트워크 토폴로지

배경 정보

지원되는 디바이스

지원되는 보안 방화벽 위협 방어 모델:

- FPR 1150
- FPR 3105, 3110,3120,3130,3140
- FPR4115,4125,4145,4112
- FPR4215,4225,4245
- FTD(Firewall Threat Defense) 가상, 최소 16개의 CPU 코어

제한 사항

- 객체 공유
- IPv6는 지원되지 않습니다.
- 전역 VRF만 지원됩니다.
- 범용 ZTNA 정책은 디바이스에 대한 사이트 대 사이트 터널 트래픽에 적용되지 않습니다.
- 클러스터링된 디바이스는 지원되지 않습니다.
- 4K 및 9K firepower 시리즈에 컨테이너로 구축된 FTD는 지원되지 않습니다

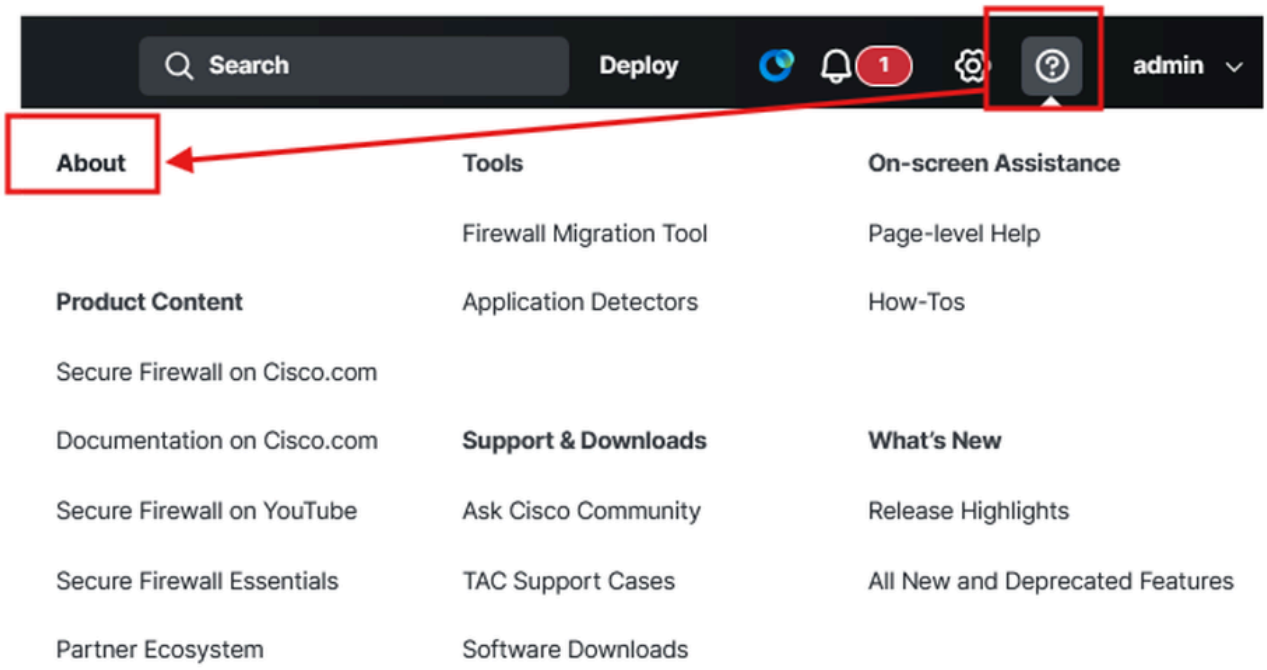
- 범용 ZTNA 세션은 점보 프레임을 지원하지 않습니다

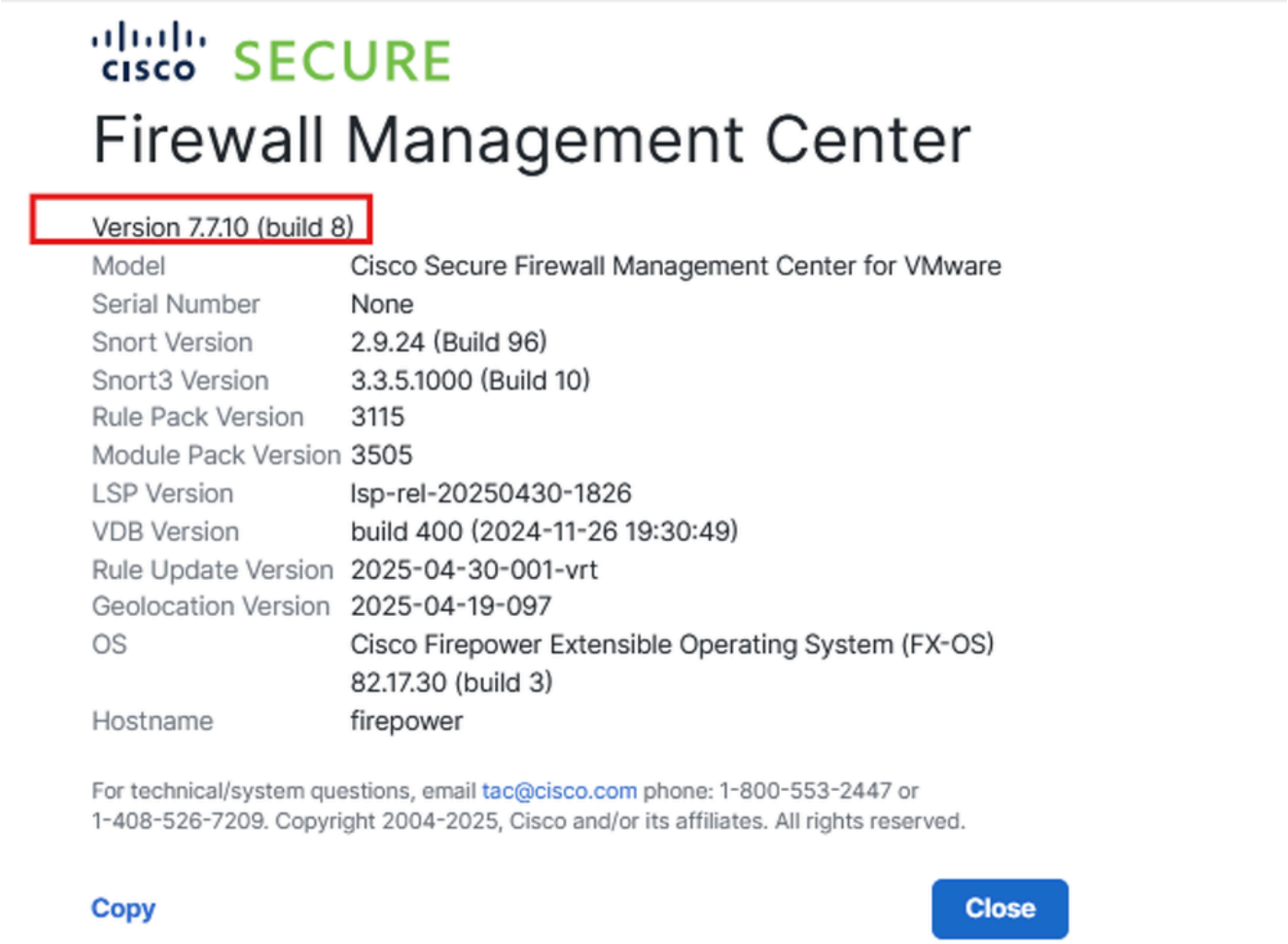
구성

FMC 버전 확인

범용 ZTNA에 대해 지원되는 소프트웨어 버전(7.7.10 이상일 수 있음)에서 실행 중인 방화벽 관리 센터 및 방화벽 FTD를 확인합니다.

- 을?클릭하고(오른쪽 상단 모서리) About



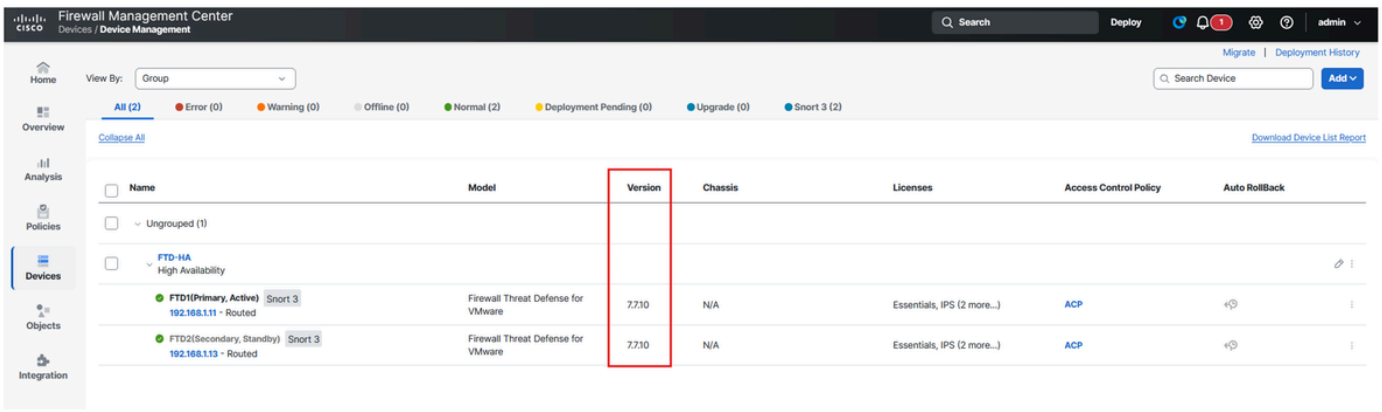


Secure Firewall Management Center - 소프트웨어 버전

FTD 버전 확인

FMC UI로 이동합니다.

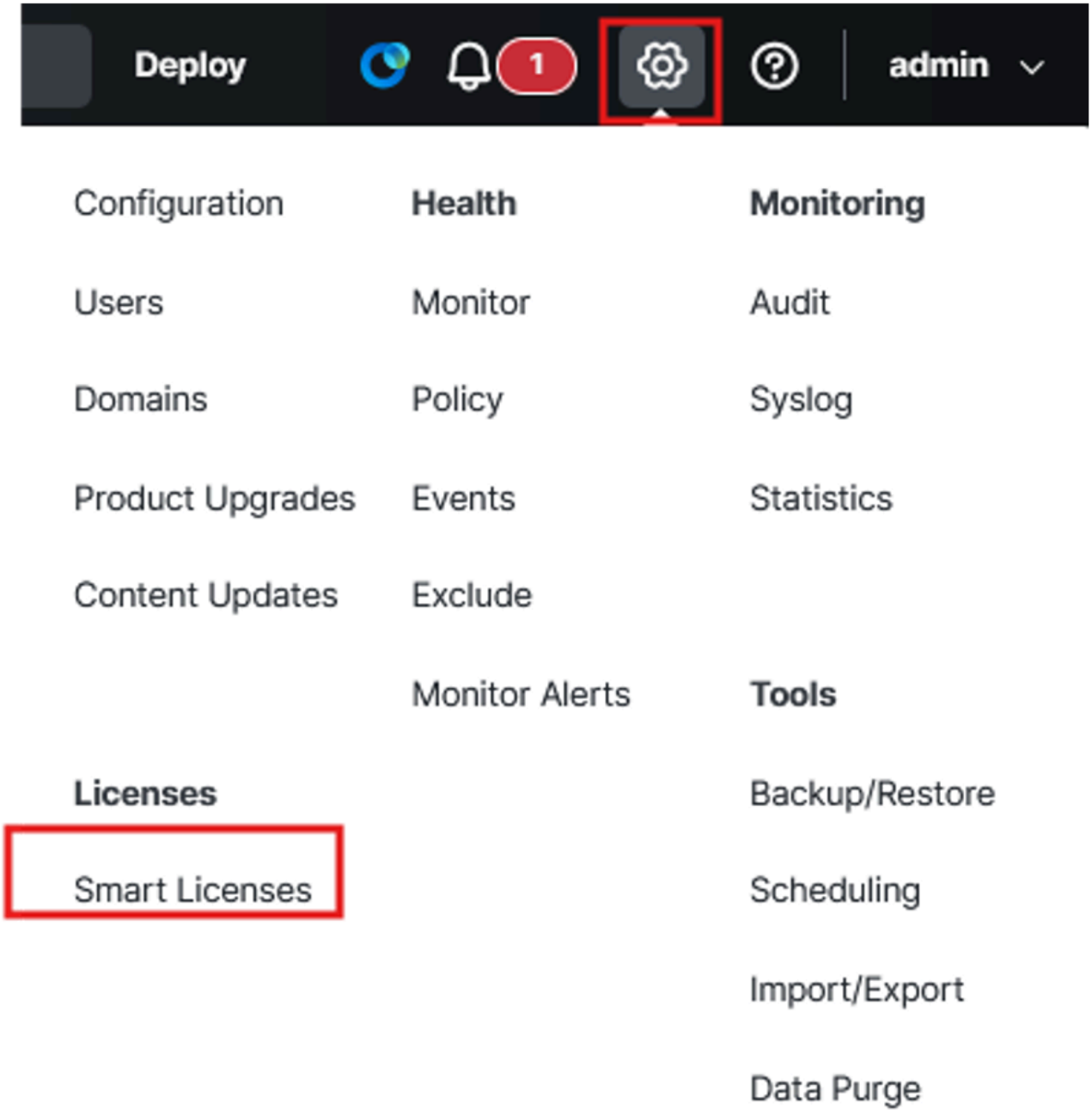
- 클릭Devices> Device Management

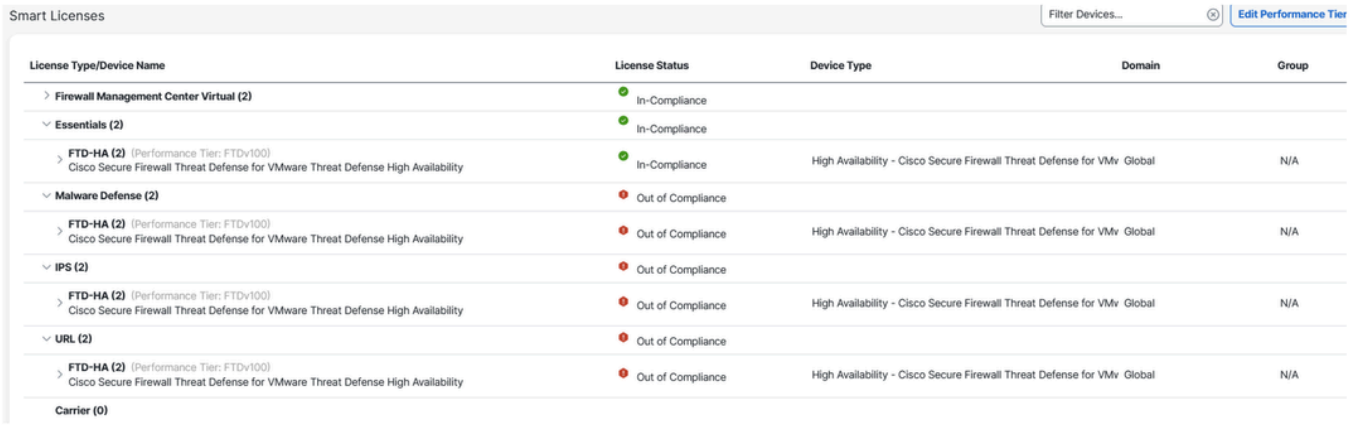


보안 방화벽 위협 방어 - 소프트웨어 버전

FTD 라이센스 확인

- Setting Icon> Licenses를 클릭합니다. Smart Licenses





보안 방화벽 위협 방어 - 스마트 라이센스

플랫폼 설정 및 DNS가 올바르게 구성되었는지 확인

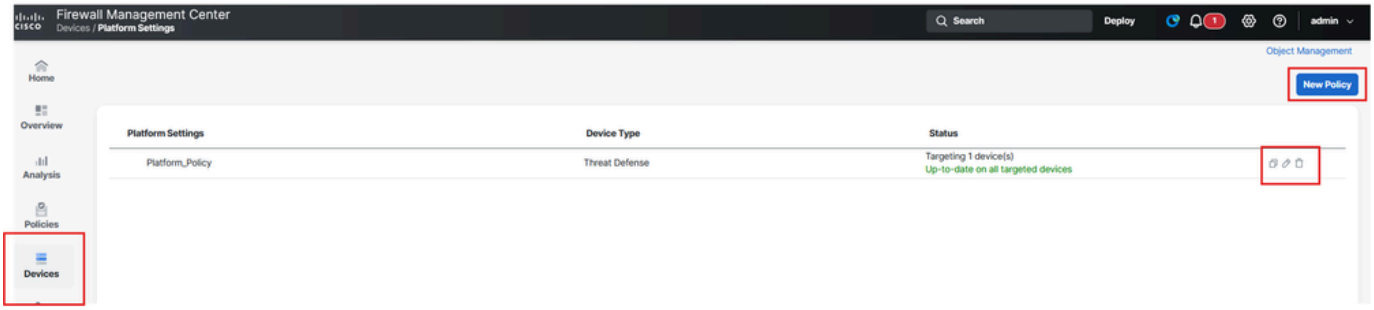
CLI를 통해 FTD에 로깅:

- 명령을 실행하여 DNS가 구성되었는지 확인합니다.

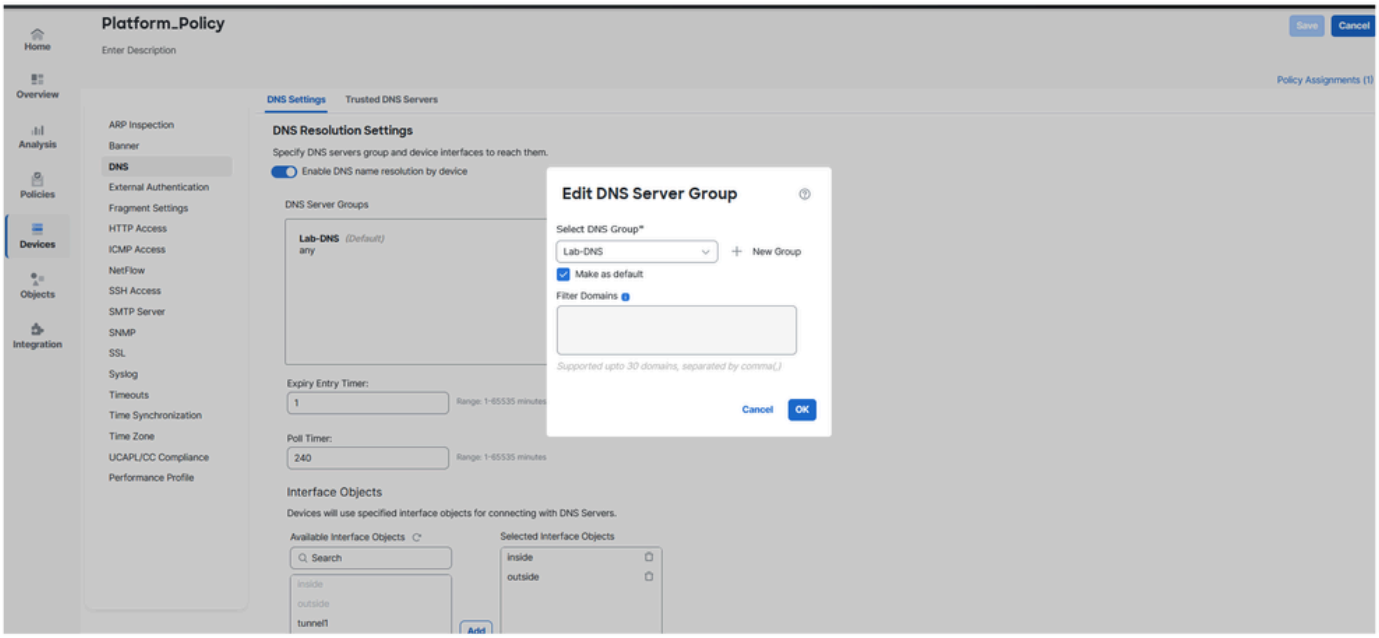
```
show run dns
```

FMC에서:

- Devices>Platform Settings를 클릭하여 새 정책을 수정하거나 생성합니다.



보안 방화벽 위협 방어 - 플랫폼 정책



보안 방화벽 위협 방어 - DNS 컨피그레이션

FTD cli를 통해 프라이빗 리소스 IP 주소 및 FQDN을 ping할 수 있는지 확인합니다(FQDN을 사용하여 PR에 액세스하려는 경우).

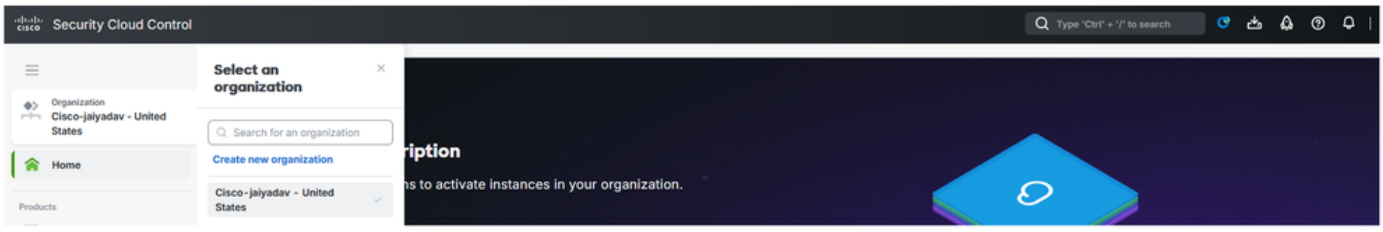
```
dns-group Lab-DNS
ftd1# ping ise.taclab.com
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.50, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ftd1#
```

CDO에서 보안 클라우드 제어 테넌트 만들기

참고: 이미 SCC 테넌트가 구성된 경우 새 테넌트를 생성할 필요가 없습니다.

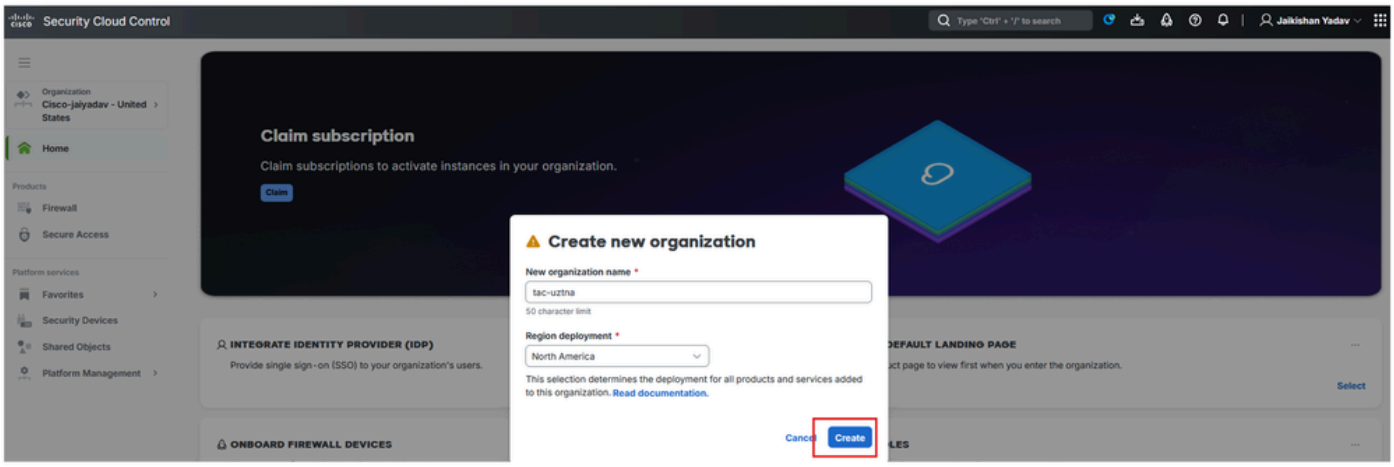
Security Cloud Control(보안 클라우드 제어)로 이동합니다.

- 클릭Organization> Create new organization



보안 클라우드 제어 - 조직

- 클릭 Create



보안 클라우드 제어 - 조직 생성

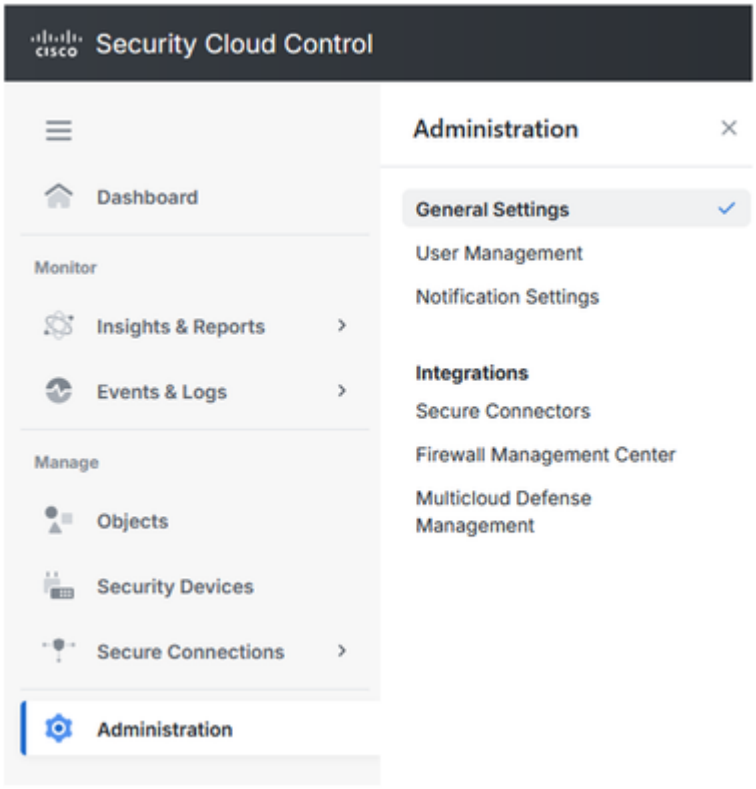
SCC 테넌트가 생성되면 테넌트 정보를 수집하여 방화벽 및 Secure Access 마이크로앱을 활성화하고 uZTNA를 활성화합니다.

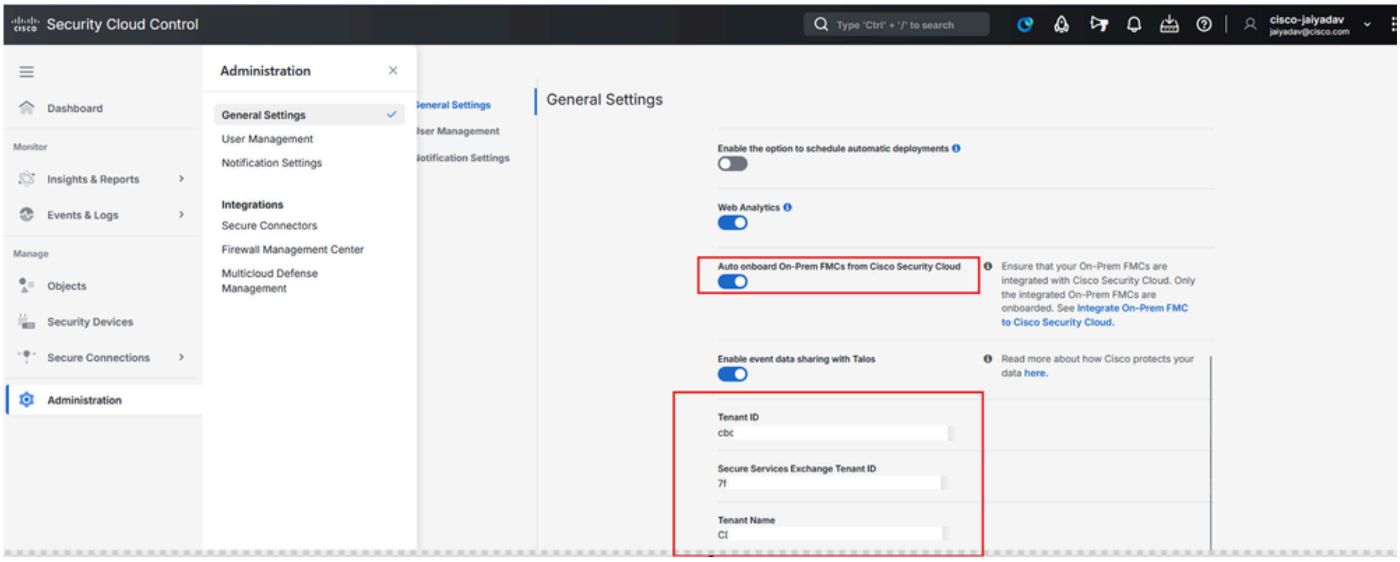
SCC 방화벽 일반 설정이 구성되었는지 확인

CDO/SCC로 이동합니다.

- 클릭Administration> General Settings
- 옵션Auto onboard On-Prem FMCs from Cisco Security Cloud이 활성화되었는지 확인합니다.

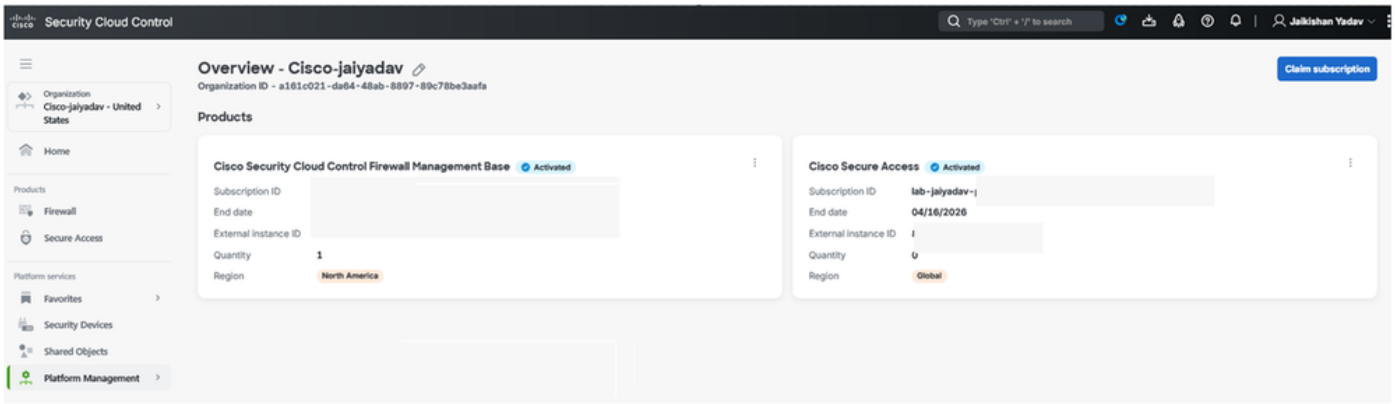
참고: Secure Access MicroApp에 액세스하려는 사용자에게는Secure Access및 관리자 역할 Security Cloud Control이 있어야 합니다.





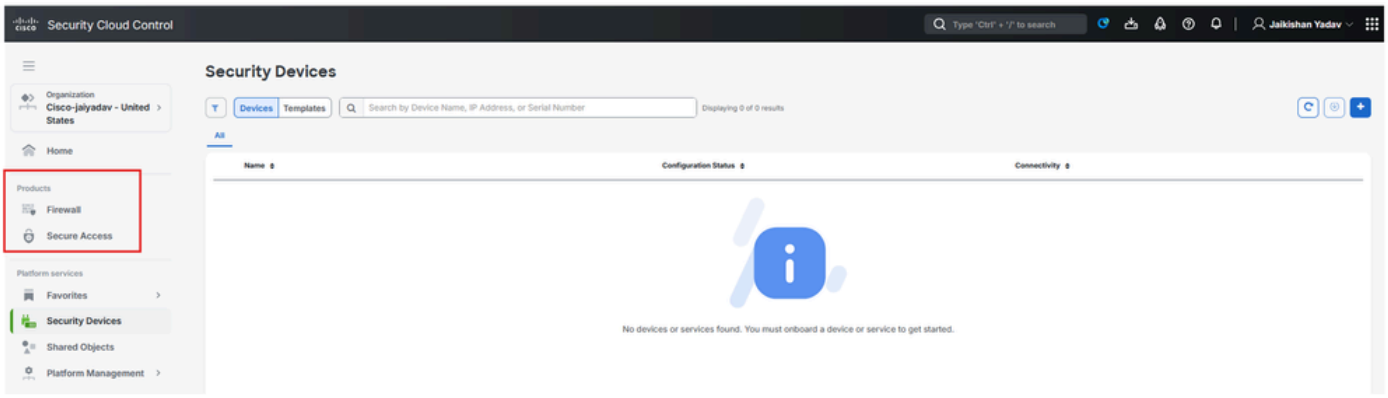
보안 클라우드 제어 - 조직 세부사항

Secure Access Tenant 및 Security Control Firewall Management Base 통합 확인



보안 클라우드 제어 - 보안 액세스 활성화

CDO에서 보안 클라우드 제어 테넌트 만들기 및 CDO에서 보안 클라우드 제어 테넌트 만들기를 완료하면 SCC 대시보드에서 방화벽 및 Secure Access 마이크로 앱을 볼 수 있습니다.



보안 클라우드 제어 - 마이크로 애플리케이션

FTD(Firewall Threat Defense) CA 서명 인증서 생성

참고: 또한 FTD 자체 서명 인증서 FTD 인증서를 사용할 수 있습니다(자체 서명 내부 및 내부 CA 인증서 생성 섹션 참조). 인증서는 PKCS12 형식이어야 하며 사용자 시스템 저장소에 신뢰할 수 있는 루트 CA 아래에 있어야 합니다.

OpenSSL 빌드 기능에서 FTD를 사용하여 CA 서명 인증서를 생성하려면

- FTD로 이동
- 명령expert실행

- openssl을 사용하여 CSR 및 키 생성
  - OpenSSL 명령:

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
```

```
openssl req -newkey rsa:2048 -nodes -keyout cert.key -out cert.csr
Generating a RSA private key
.........................+++++
.....................+++++
writing new private key to 'cert.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:NC
Locality Name (eg, city) []:RTP
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:TAC
Common Name (e.g. server FQDN or YOUR name) []:ftd.taclab.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
```

인증서 서명 요청

- CSR을 복사하고 CA 서명 인증서를 가져옵니다.
- FTD CA 서명 인증서와 키를 사용하고 인증서를 PKCS12 형식으로 변환합니다.
    - OpenSSL 명령:

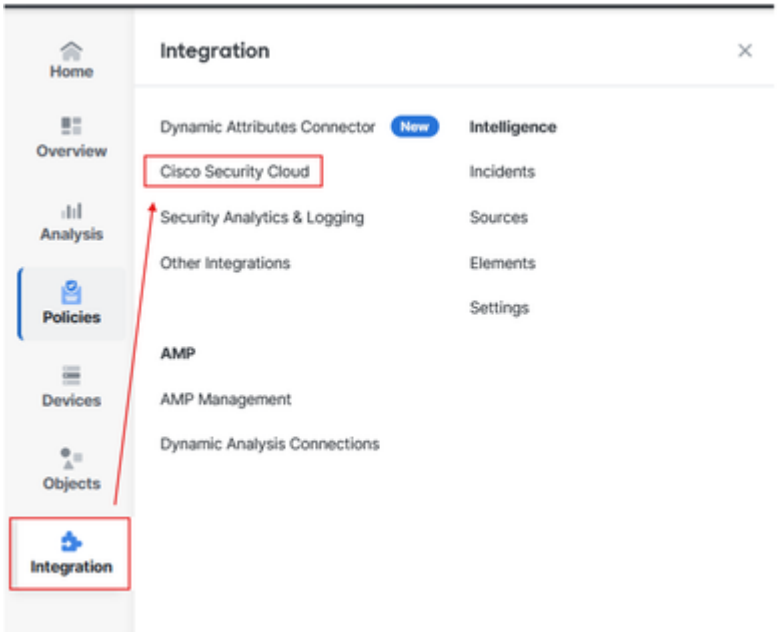
```
openssl pkcs12 -export -out ftdcert.p12 -in cert.crt -inkey cert.key
```

- SCP 또는 기타 툴을 사용하여 인증서를 내보냅니다.

온보드 온프레미스 방화벽 관리 센터에서 보안 클라우드 제어로

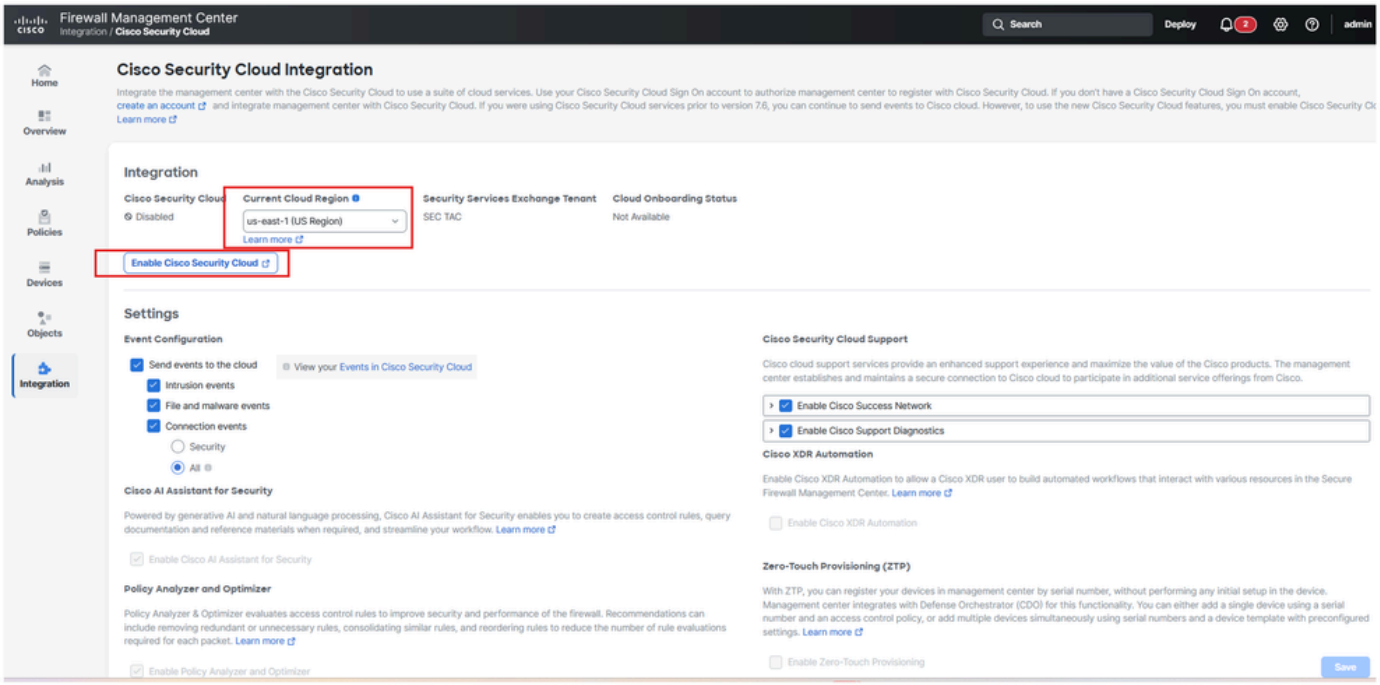
FMC로 이동합니다.

- 클릭Integration> Cisco Security Cloud



방화벽 관리 센터 및 SCC 통합

- Cloud Region(클라우드 지역)을 선택한 다음 Enable Cisco Security Cloud

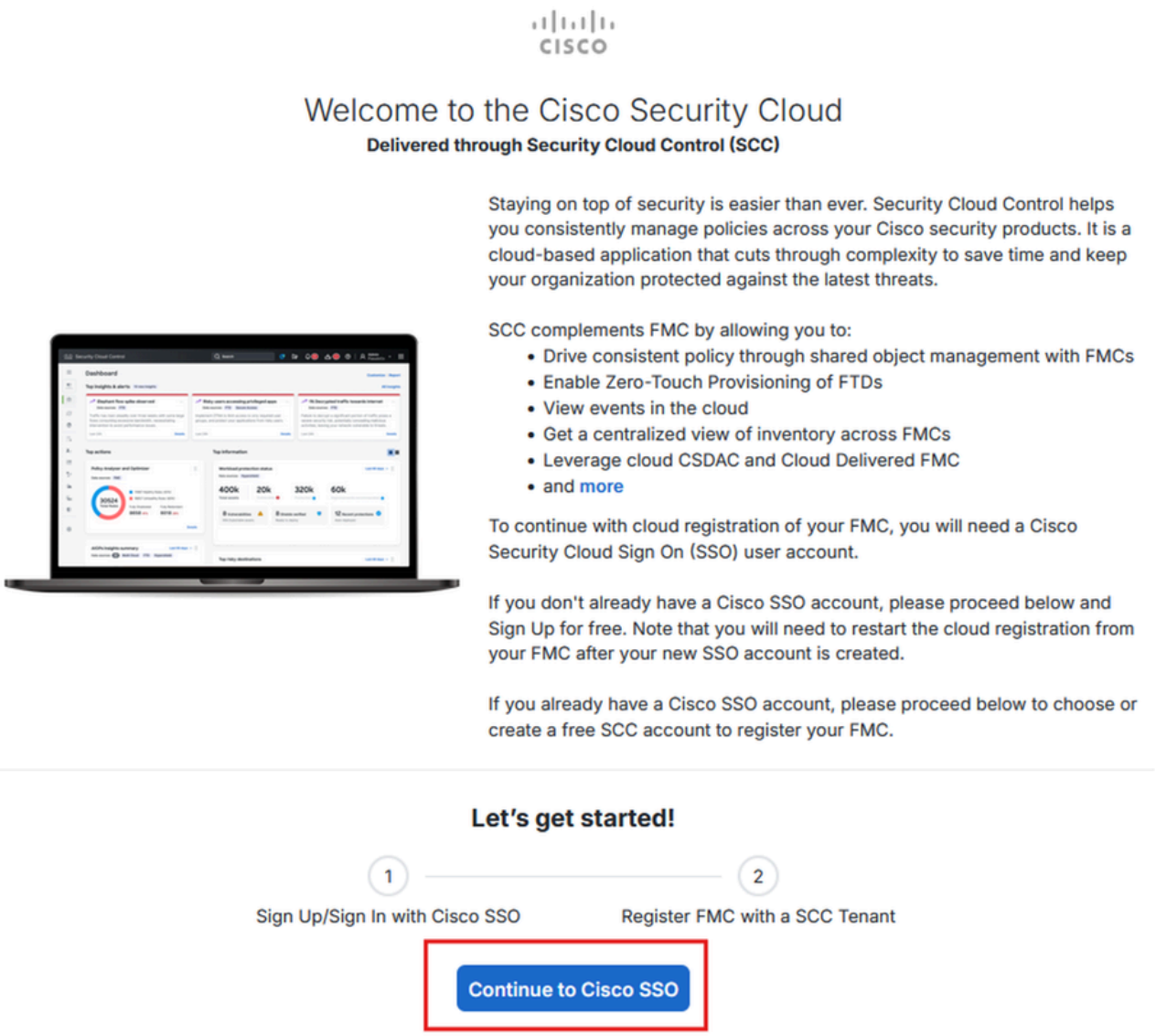


SCC에 대한 방화벽 관리 센터 온보딩

새 탭에서 새 브라우저 탭이 열립니다.

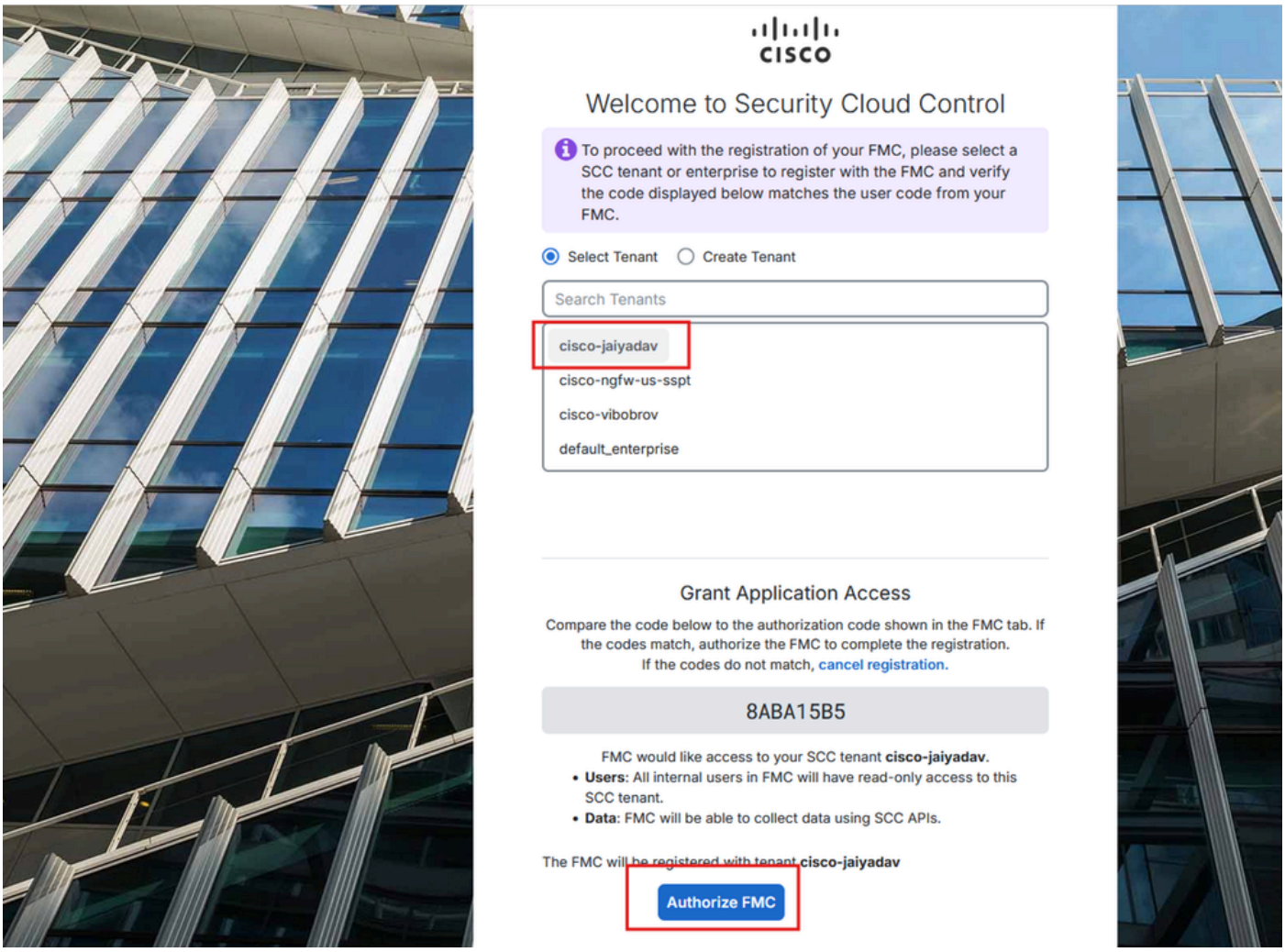
- 클릭 Continue to Cisco SSO

참고: SCC에서 로그아웃했으며 다른 탭이 열려 있지 않은지 확인하십시오.



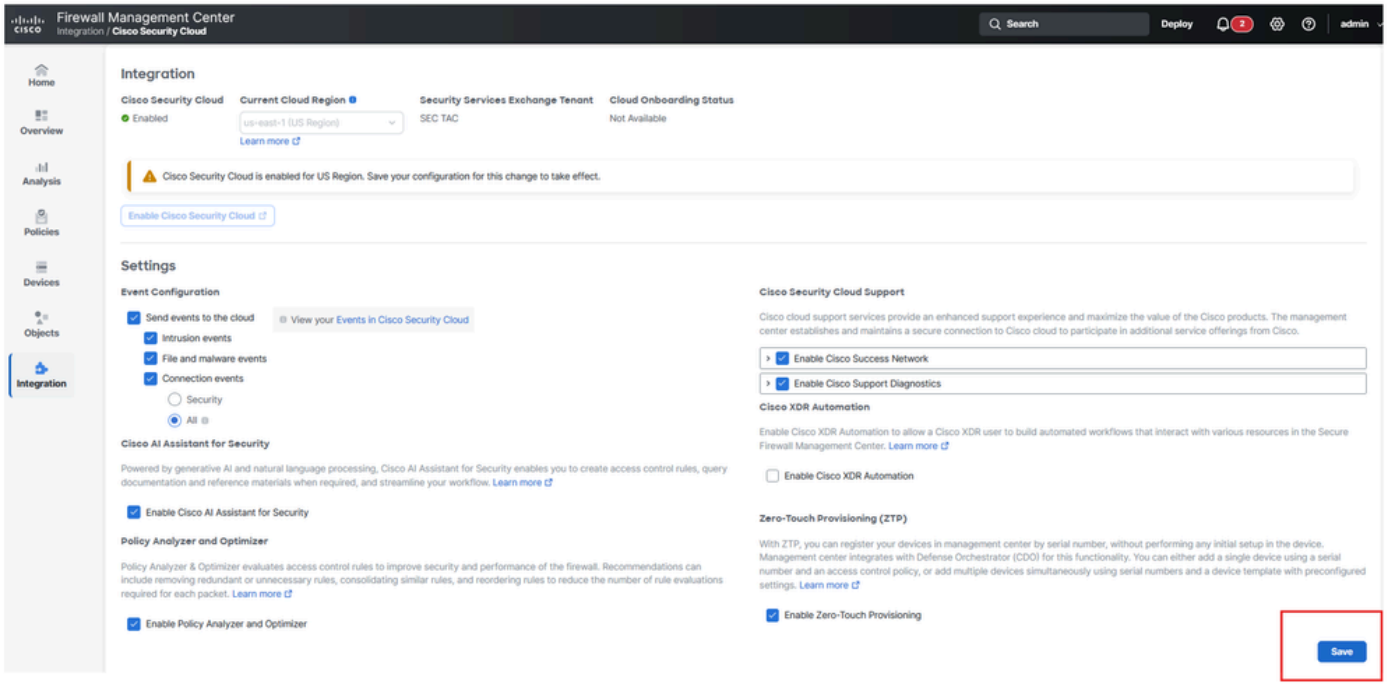
SCC에 대한 방화벽 관리 센터 온보딩

- SCC 테넌트를 선택하고 Authorize FMC



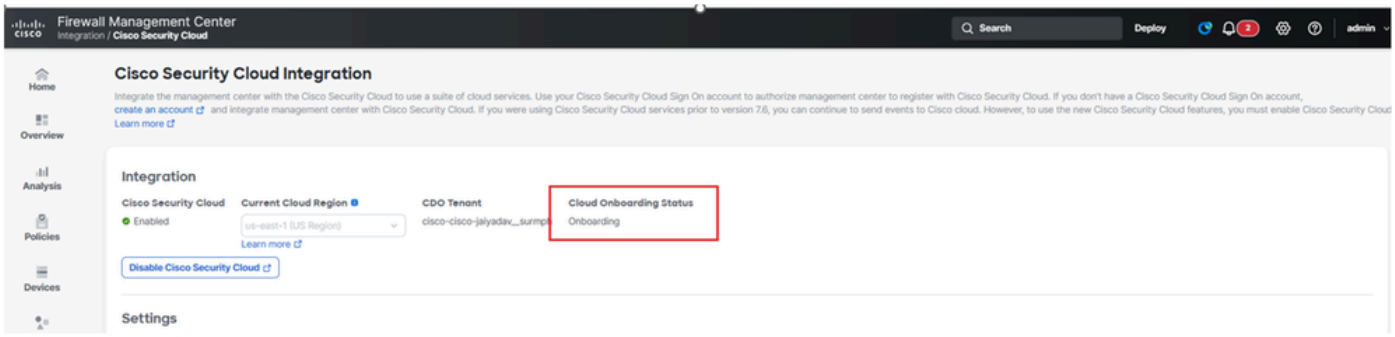
SCC에 대한 방화벽 관리 센터 온보딩

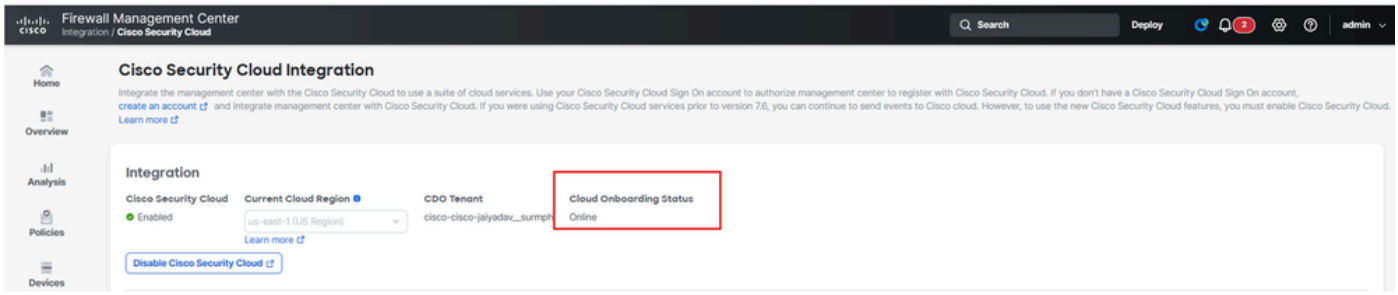
- 클릭 Save



SCC에 대한 방화벽 관리 센터 온보딩

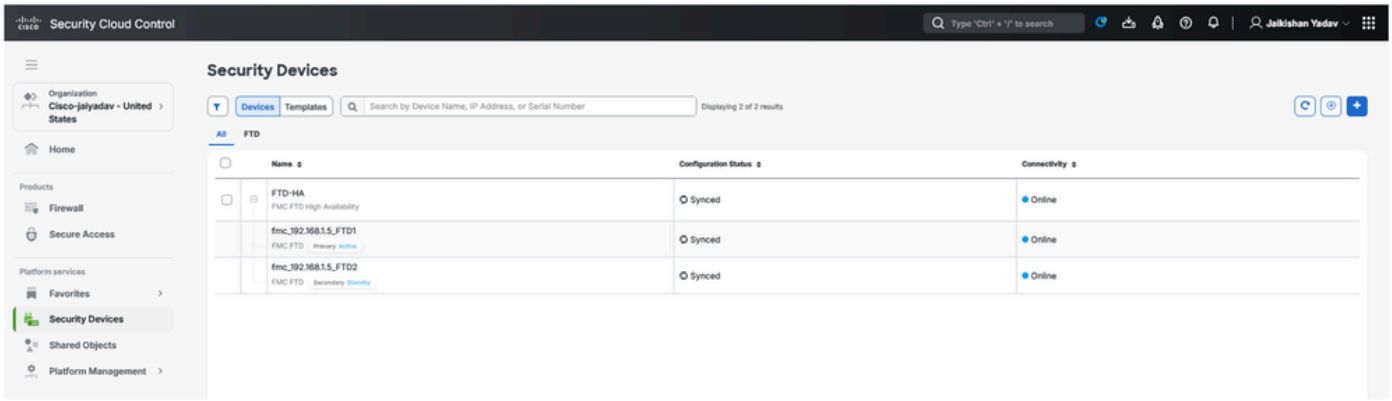
의Cloud Onboarding Status상태는 **Not Available** 에서Onboarding로Online변경되어야 합니다.





방화벽 관리 센터 온보딩 상태

- SCC로 이동하여Platform Services> Security Devices

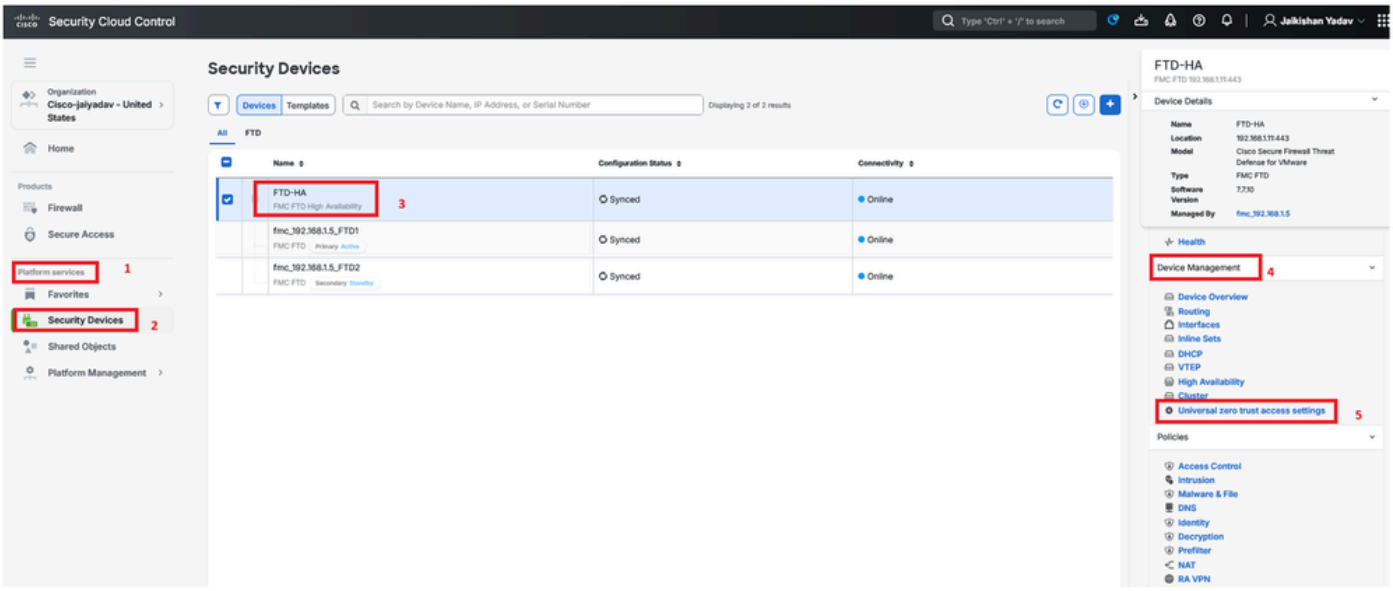


SCC의 보안 방화벽 위협 방어 상태

FTD에 uZTNA(Universal Zero Trust Network Access) 설정 등록

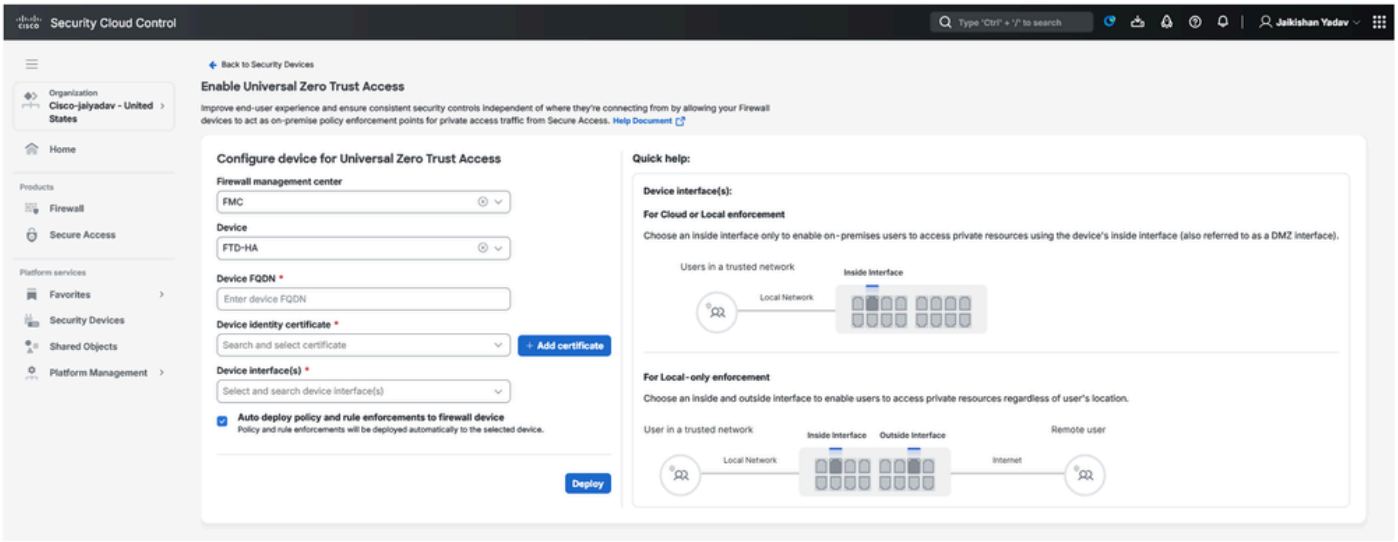
SCC로 이동합니다.

- 클릭Platform Services> **Security Devices** > **FTD** > **Device Management** > Universal Zero Trust Network Access

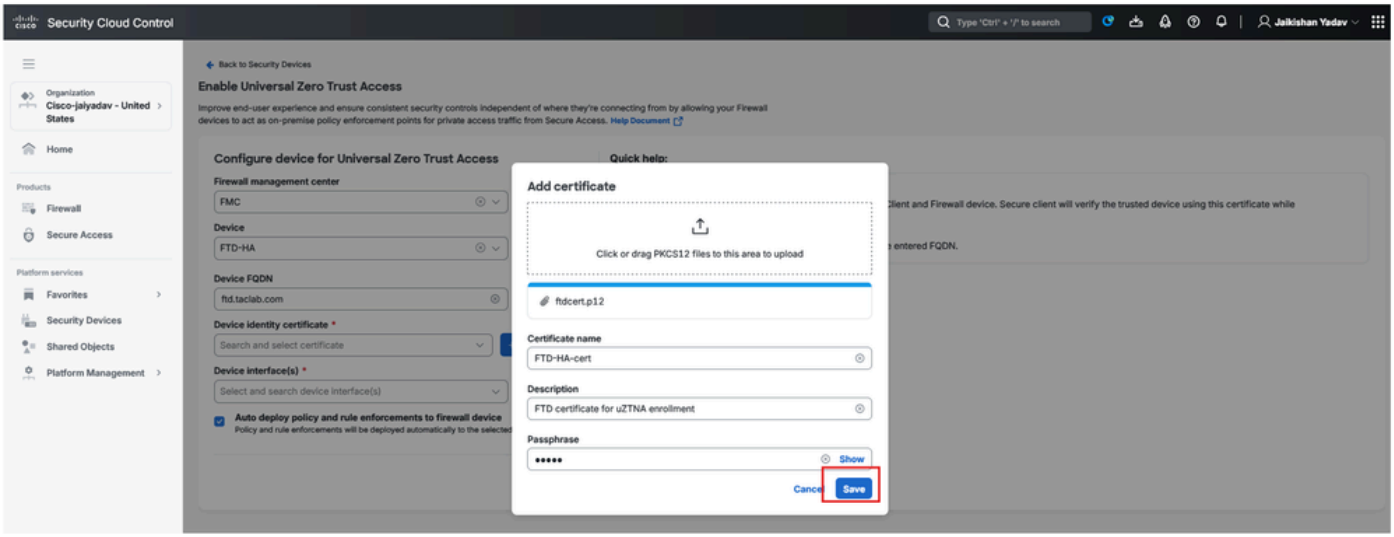


보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션

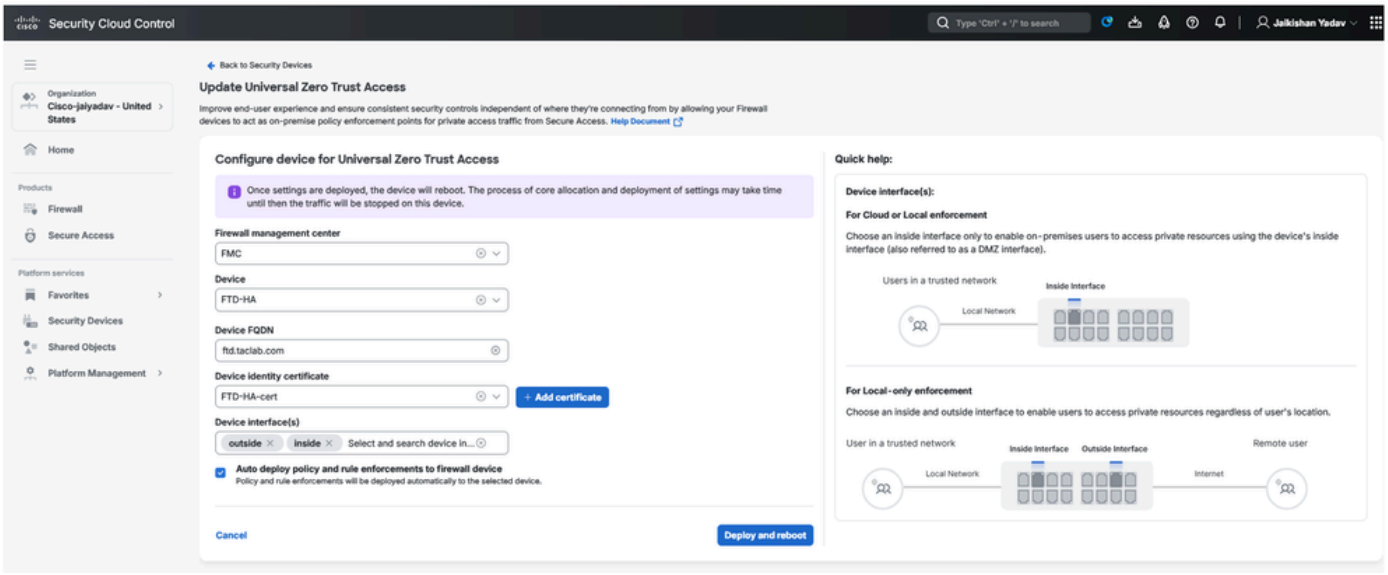
- 정보를 입력하고 FTD(Firewall Threat Defense) CA 서명 인증서 생성 단계에서 생성된 FTD 인증서를 업로드합니다



보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션



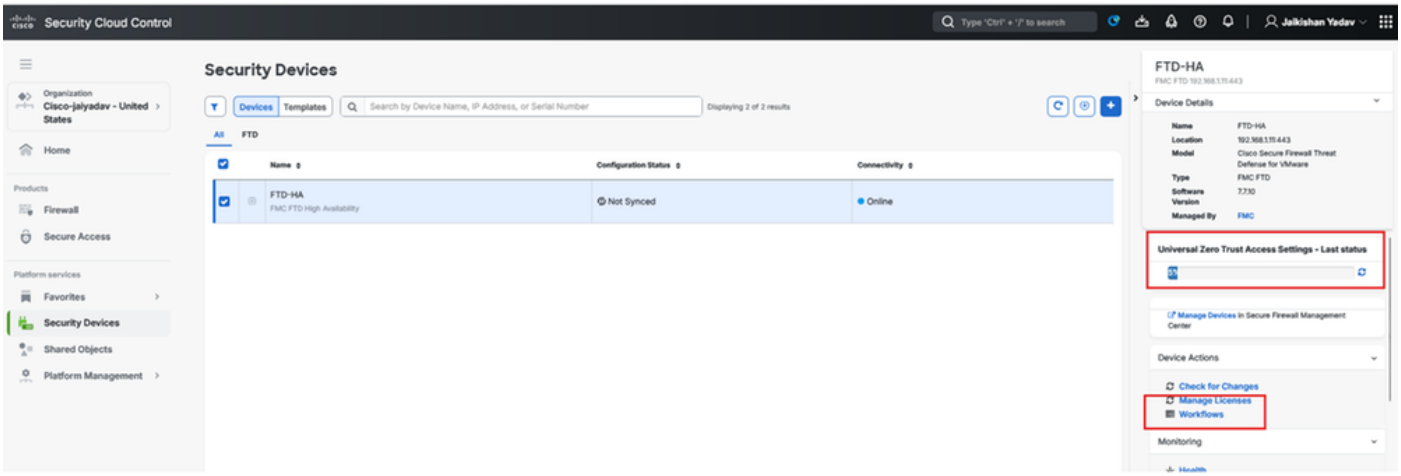
보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션



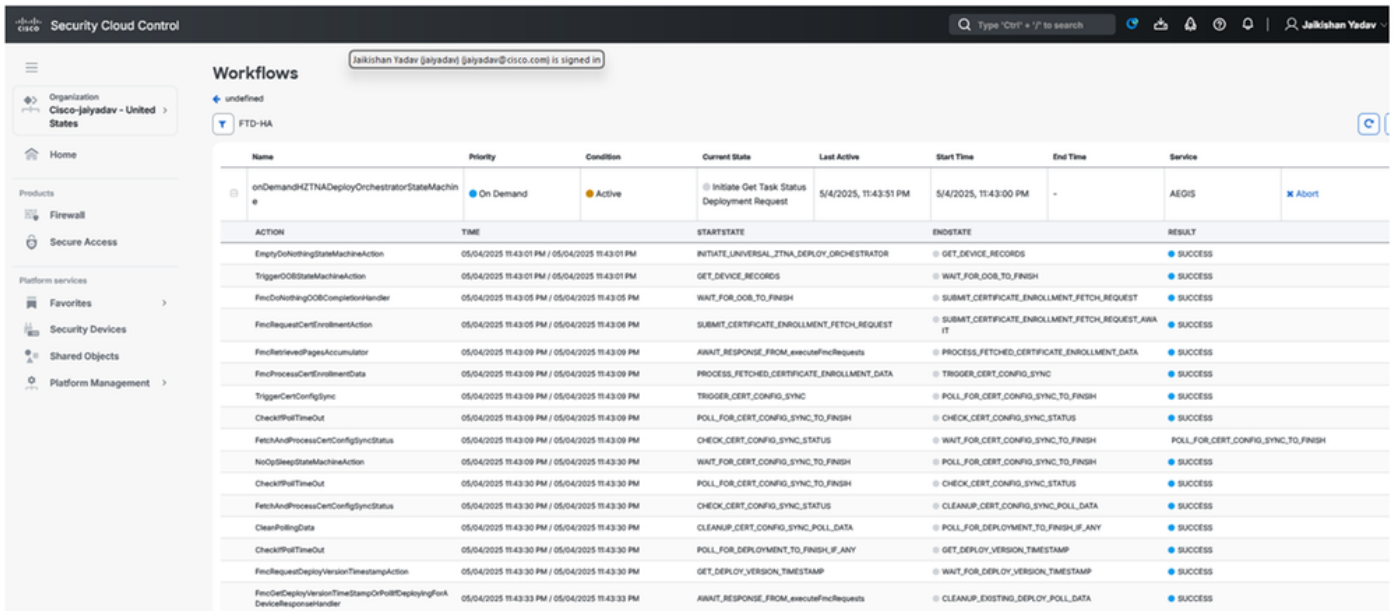
보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션

참고: FTD HA에서 uZTNA를 활성화하면 변경 사항이 구축되고 두 FTD(Firewall Threat Defense) 유닛이 동시에 재부팅됩니다. 적절한 유지 보수 기간을 예약해야 합니다.

- 로그를 확인하려면 클릭Workflow합니다.

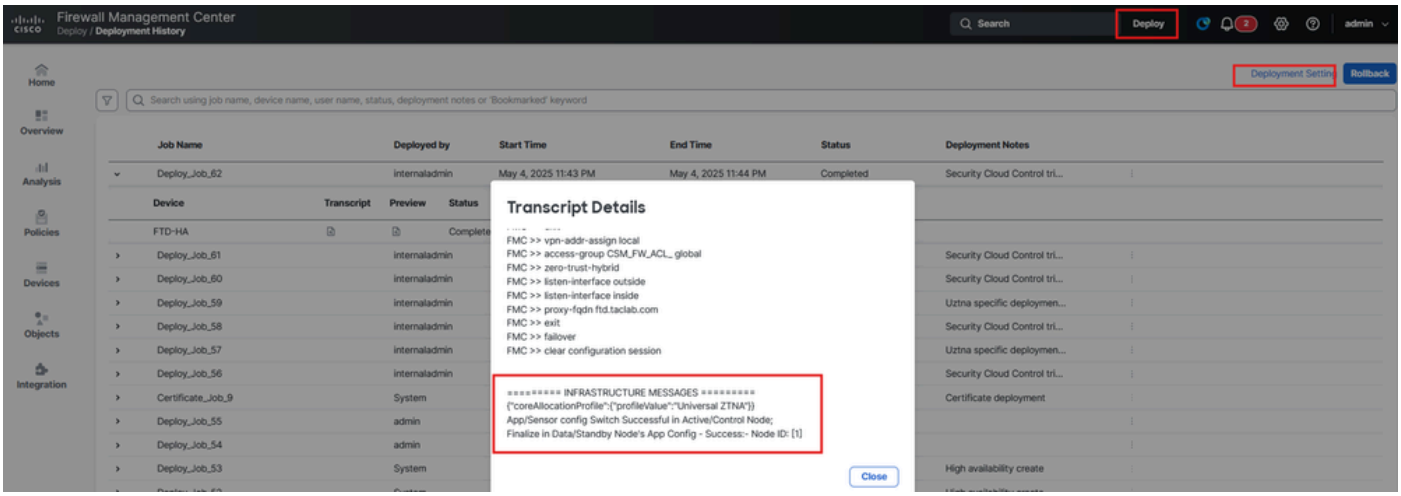


보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션 상태



보안 클라우드 제어 워크플로

Transcript Details(대본 세부사항)에서 및 변경 사항을 볼Policy Deployment Status수 있습니다. FMC.



Secure Firewall Management Center - 정책 구축 상태

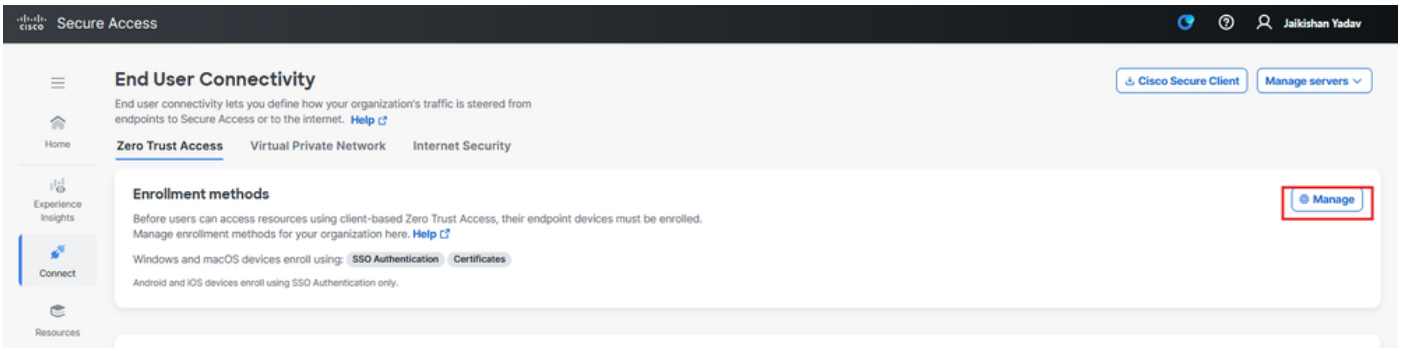
uZTNA에 클라이언트 등록

보안 액세스 컨피그레이션

참고: SSO 또는 인증서 기반 ZTA 등록을 사용할 수 있습니다. 다음은 인증서 기반 ZTA 등록 단계입니다

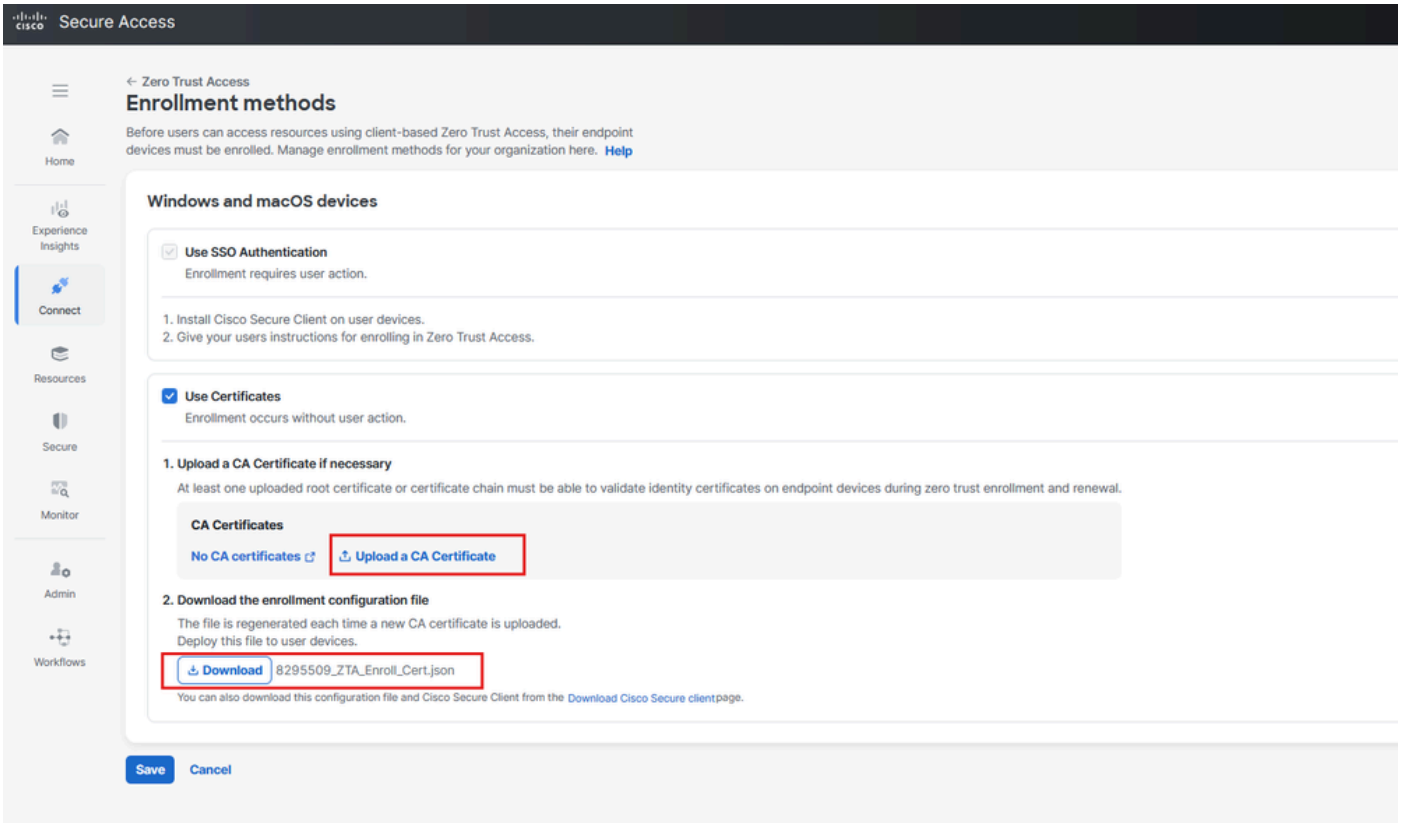
Secure Access Dashboard(보안 액세스 대시보드)로 이동합니다.

- **Connect** > > 를 **End User Connectivity** 클릭합니다. Zero Trust Access
- 클릭 Manage



보안 액세스 - ZTA 인증서 등록

- 루트 CA 인증서 업로드 및 등록 컨피그레이션 파일 다운로드

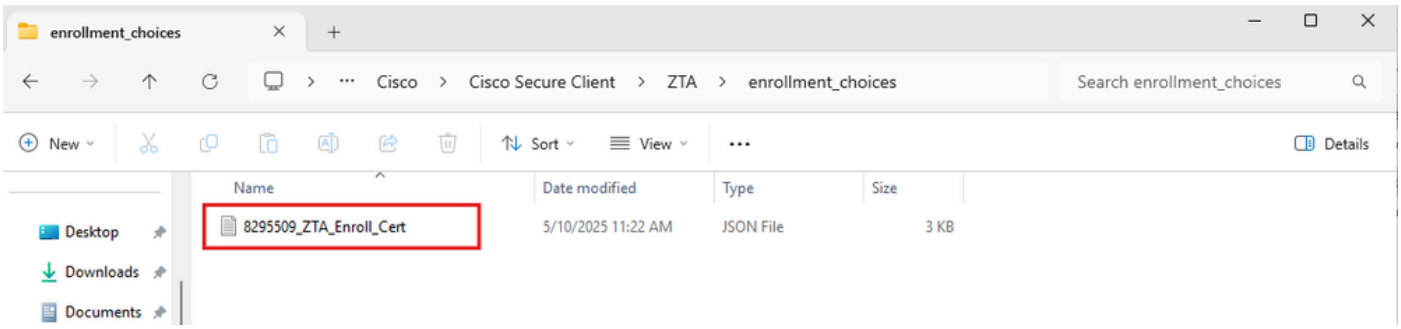


보안 액세스 - ZTA 인증서 등록

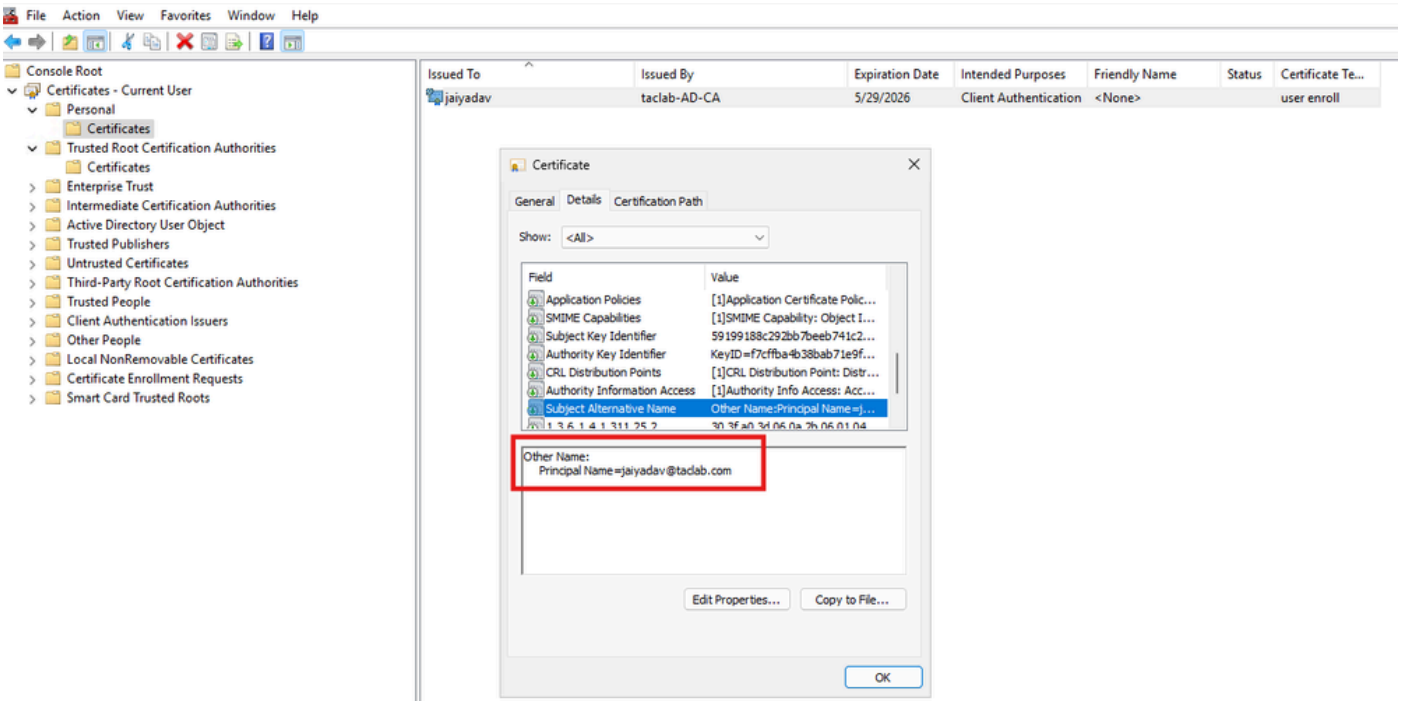
- 클릭 Save

클라이언트 컨피그레이션

등록 컨피그레이션 파일을 C:\ProgramData\Cisco\Cisco Secure Client\ZTA\enrollment_choices

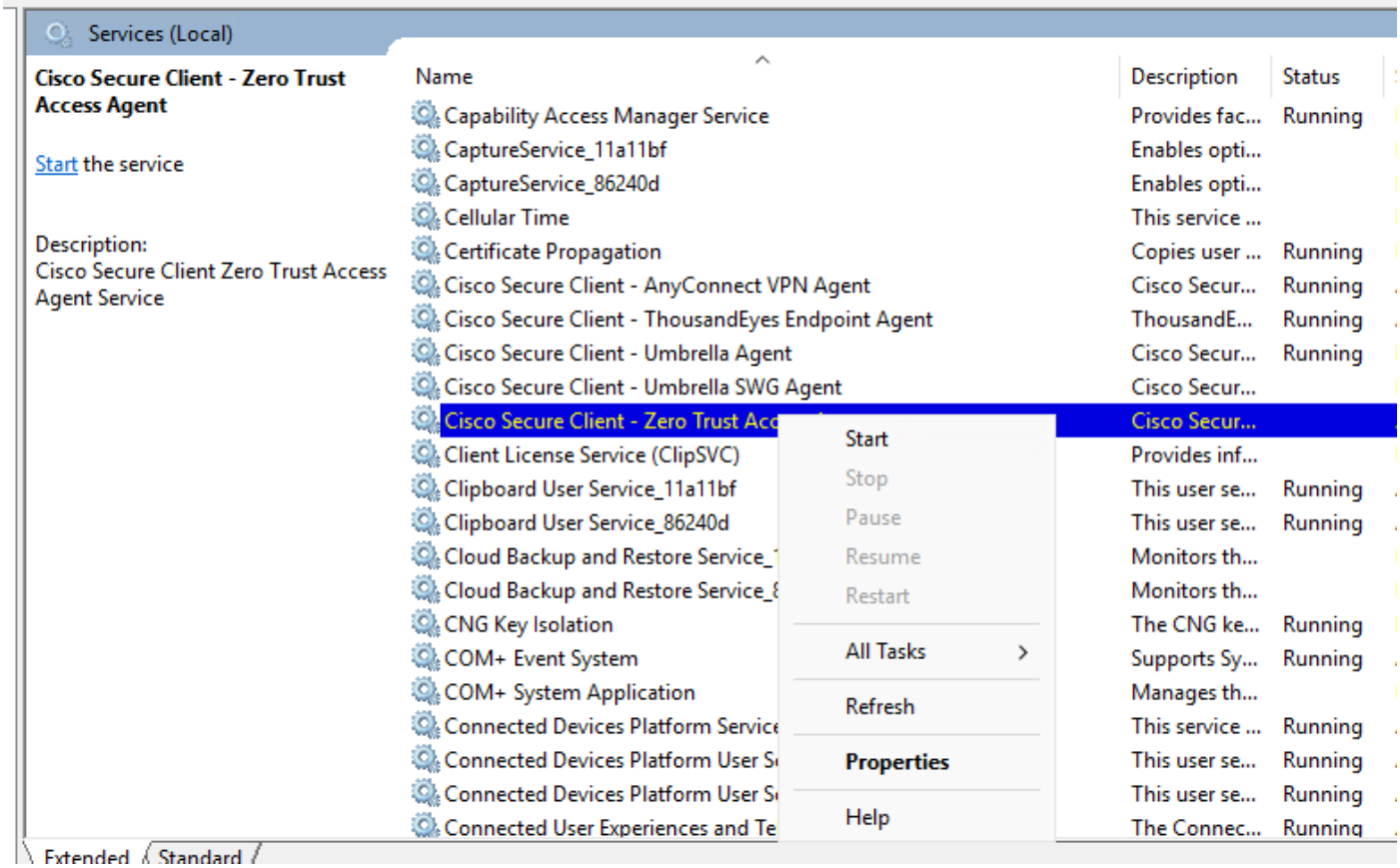


- SAN 필드에 UPN이 있어야 하는 클라이언트 인증서 생성



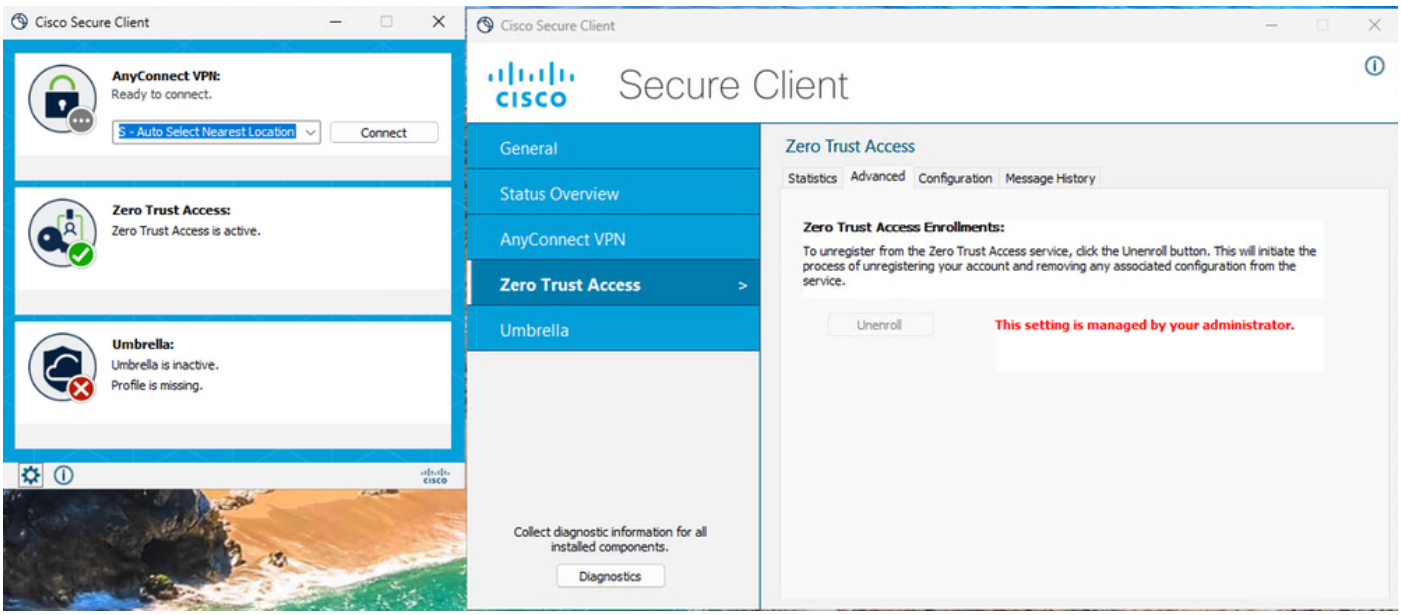
인증서 설치

- 시작/재시작 Cisco Secure Client - Zero Trust Access Agent



Windows 서비스

- ZTA 모듈 상태 확인



보안 액세스 - ZTA 인증서 등록 상태

다음을 확인합니다.

다음 명령을 사용하여 FTD(Firewall Threat Defense)에서 uZTNA 컨피그레이션을 확인합니다.

```
show allocate-core profile
show running-config universal-zero-trust
```

관련 정보

- Cisco 기술 지원 및 다운로드
- Cisco Secure Access Help Center
- Cisco ISE 설계 가이드

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.