

SCC에서 온프레미스 매니지드 FMC로 유니버설 ZTNA에 대한 보안 액세스 구성

목차

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[네트워크 다이어그램](#)

[배경 정보](#)

[지원되는 디바이스](#)

[제한 사항](#)

[구성](#)

[FMC 버전 확인](#)

[FTD 버전 확인](#)

[FTD 라이선스 확인](#)

[플랫폼 설정 및 DNS가 올바르게 구성되었는지 확인](#)

[CDO에서 보안 클라우드 제어 테넌트 만들기](#)

[SCC 방화벽 일반 설정이 구성되었는지 확인](#)

[Secure Access Tenant 및 Security Control Firewall Management Base 통합 확인](#)

[FTD\(Firewall Threat Defense\) CA 서명 인증서 생성](#)

[온보드 온프레미스 방화벽 관리 센터에서 보안 클라우드 제어로](#)

[FTD에 uZTNA\(Universal Zero Trust Network Access\) 설정 등록](#)

[uZTNA에 클라이언트 등록](#)

[보안 액세스 컨피그레이션](#)

[클라이언트 컨피그레이션](#)

[다음을 확인합니다.](#)

[관련 정보](#)

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 라이선스와 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

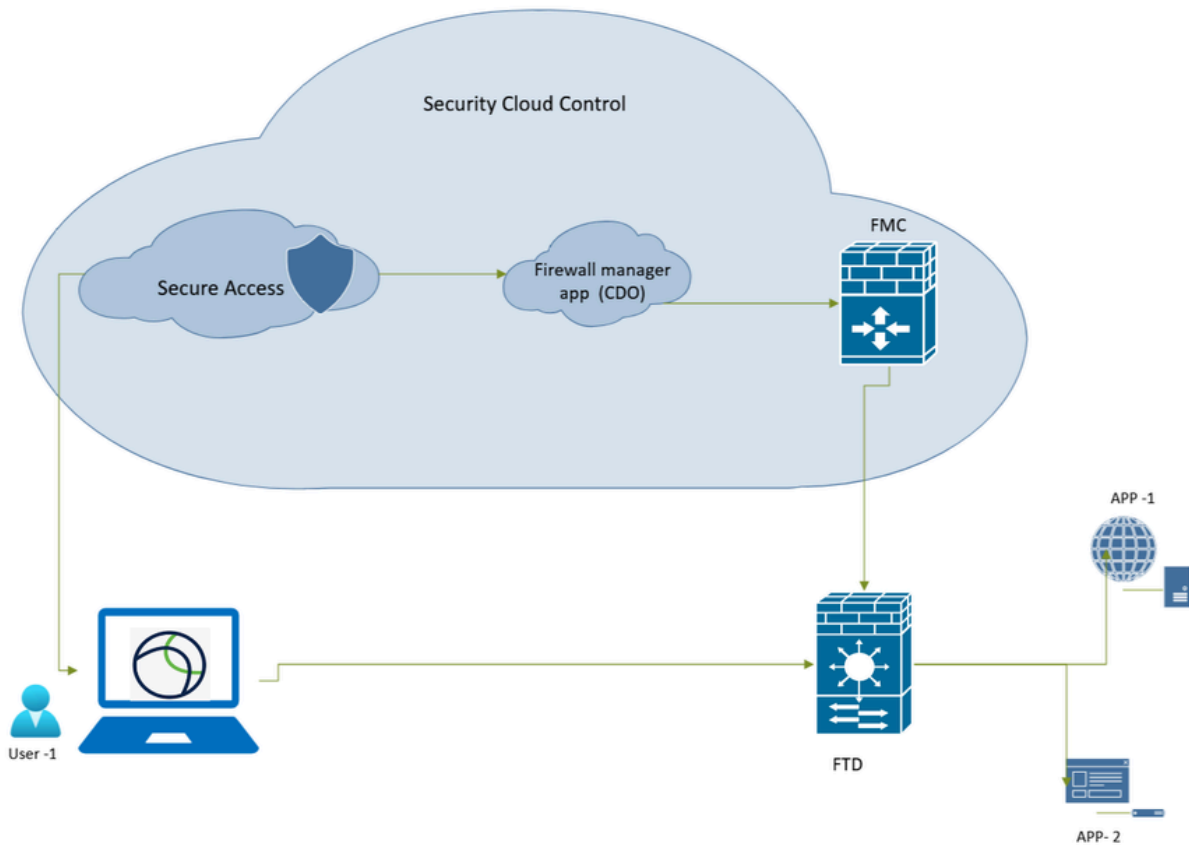
사용되는 구성 요소

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

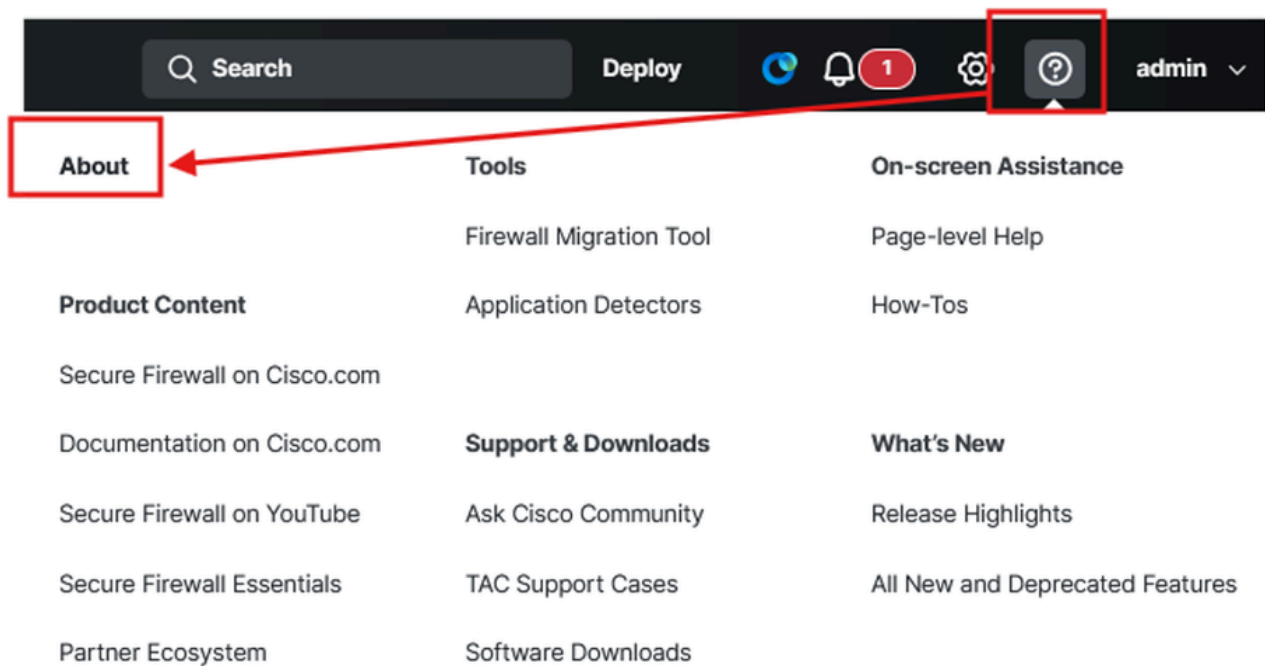
- 범용 ZTNA 세션은 점보 프레임을 지원하지 않습니다

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



Firewall Management Center

Version 7.7.10 (build 8)

Model	Cisco Secure Firewall Management Center for VMware
Serial Number	None
Snort Version	2.9.24 (Build 96)
Snort3 Version	3.3.5.1000 (Build 10)
Rule Pack Version	3115
Module Pack Version	3505
LSP Version	lsp-rel-20250430-1826
VDB Version	build 400 (2024-11-26 19:30:49)
Rule Update Version	2025-04-30-001-vrt
Geolocation Version	2025-04-19-097
OS	Cisco Firepower Extensible Operating System (FX-OS) 82.17.30 (build 3)
Hostname	firepower

For technical/system questions, email tac@cisco.com phone: 1-800-553-2447 or 1-408-526-7209. Copyright 2004-2025, Cisco and/or its affiliates. All rights reserved.

Copy

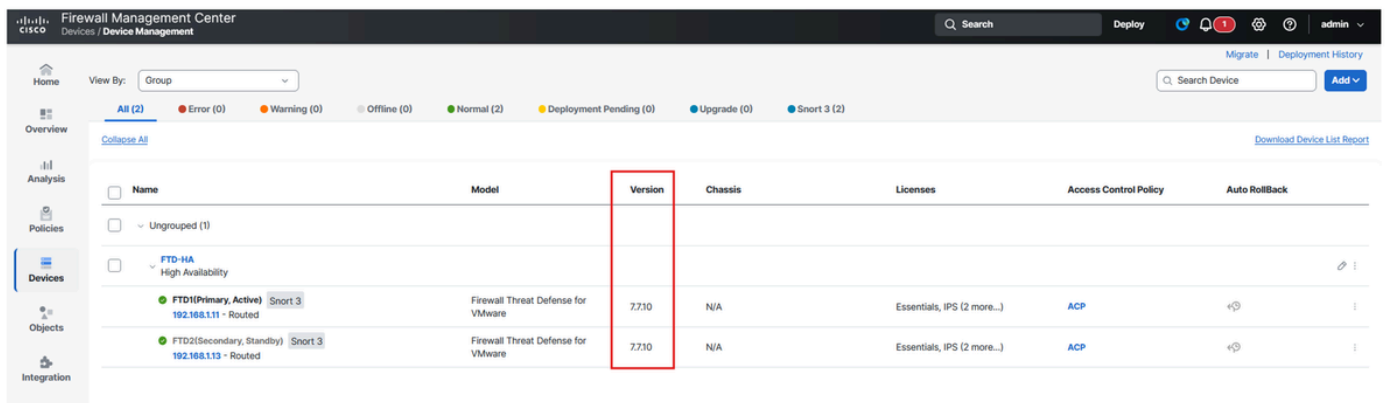
Close

Secure Firewall Management Center - 소프트웨어 버전

FTD 버전 확인

FMC UI로 이동합니다.

- 클릭Devices> Device Management



Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (1)						
FTD-HA High Availability						
FTD1(Primary, Active) 192.168.1.11 - Routed Snort 3	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	+
FTD2(Secondary, Standby) 192.168.1.13 - Routed Snort 3	Firewall Threat Defense for VMware	7.7.10	N/A	Essentials, IPS (2 more...)	ACP	+

보안 방화벽 위협 방어 - 소프트웨어 버전

FTD 라이선스 확인

- Setting Icon > Licenses를 클릭합니다. Smart Licenses



Configuration

Users

Domains

Product Upgrades

Content Updates

Licenses

Smart Licenses

Health

Monitor

Policy

Events

Exclude

Monitor Alerts

Monitoring

Audit

Syslog

Statistics

Tools

Backup/Restore

Scheduling

Import/Export

Data Purge

Smart Licenses					Filter Devices...	Edit Performance Tier
License Type/Device Name	License Status	Device Type	Domain	Group		
> Firewall Management Center Virtual (2)	In-Compliance					
Essentials (2)	In-Compliance					
> FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	In-Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A		
Malware Defense (2)	Out of Compliance					
> FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A		
IPS (2)	Out of Compliance					
> FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A		
URL (2)	Out of Compliance					
> FTD-HA (2) (Performance Tier: FTDv100) Cisco Secure Firewall Threat Defense for VMware Threat Defense High Availability	Out of Compliance	High Availability - Cisco Secure Firewall Threat Defense for VMv Global		N/A		
Carrier (0)						

보안 방화벽 위협 방어 - 스마트 라이선스

플랫폼 설정 및 DNS가 올바르게 구성되었는지 확인

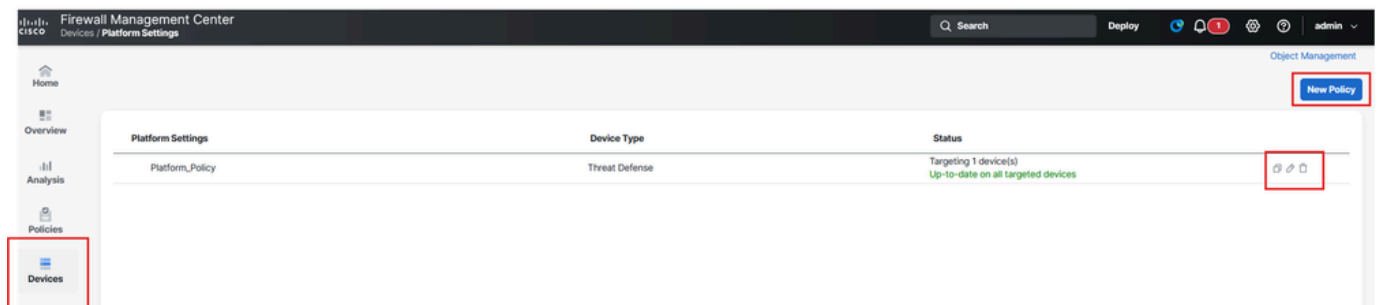
CLI를 통해 FTD에 로깅:

- 명령을 실행하여 DNS가 구성되었는지 확인합니다.

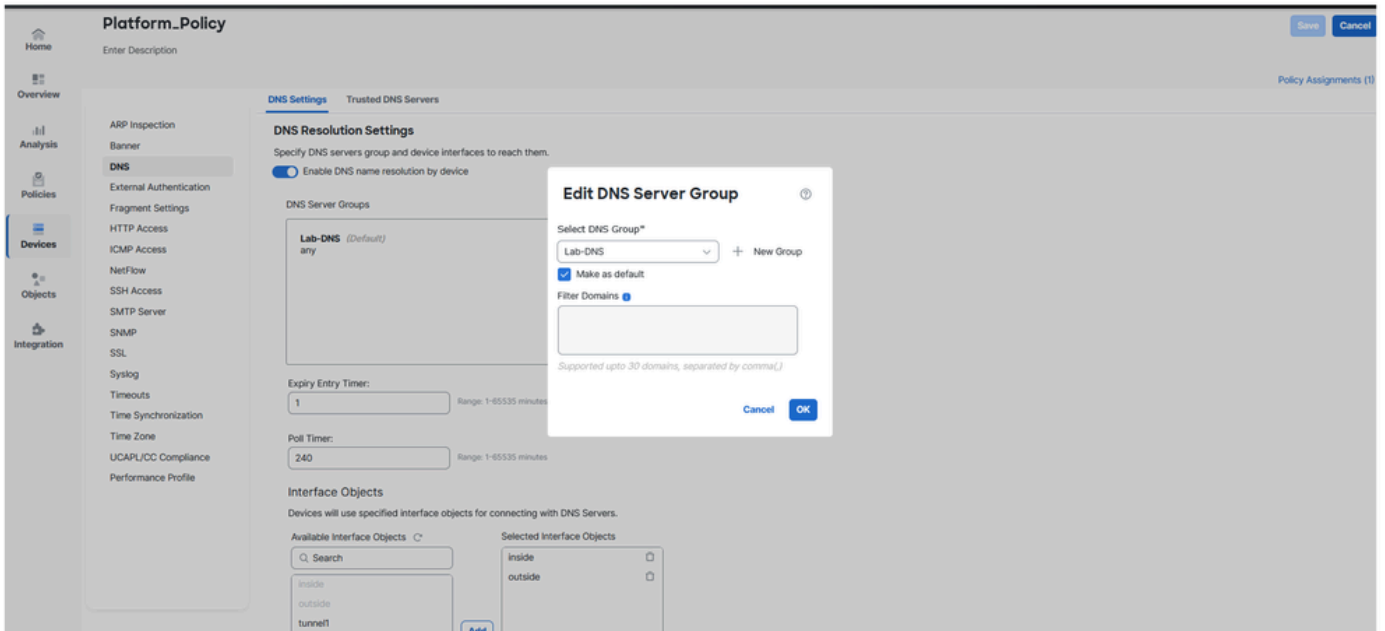
```
show run dns
```

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.tac1ab.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#
```

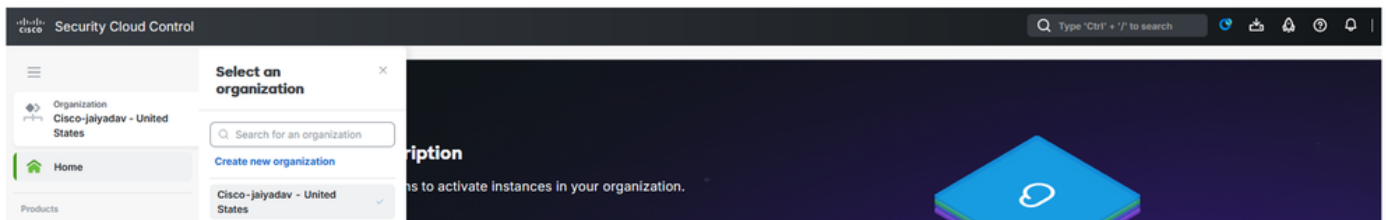
CDO에서 보안 클라우드 제어 테넌트 만들기



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

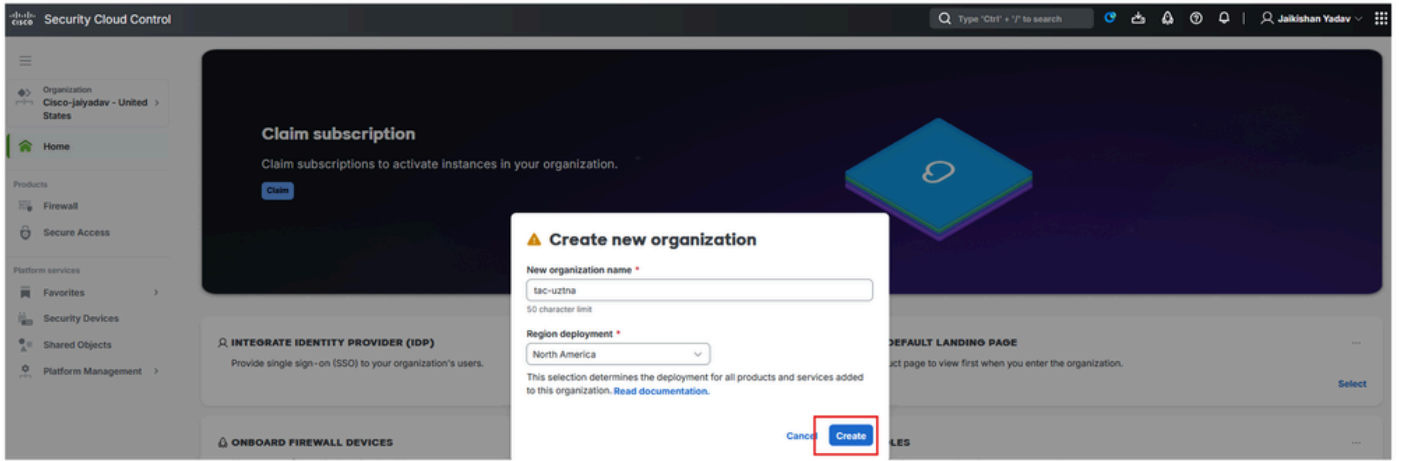
[Security Cloud Control\(보안 클라우드 제어\)로 이동합니다.](#)

- [클릭](#) Organization > 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.

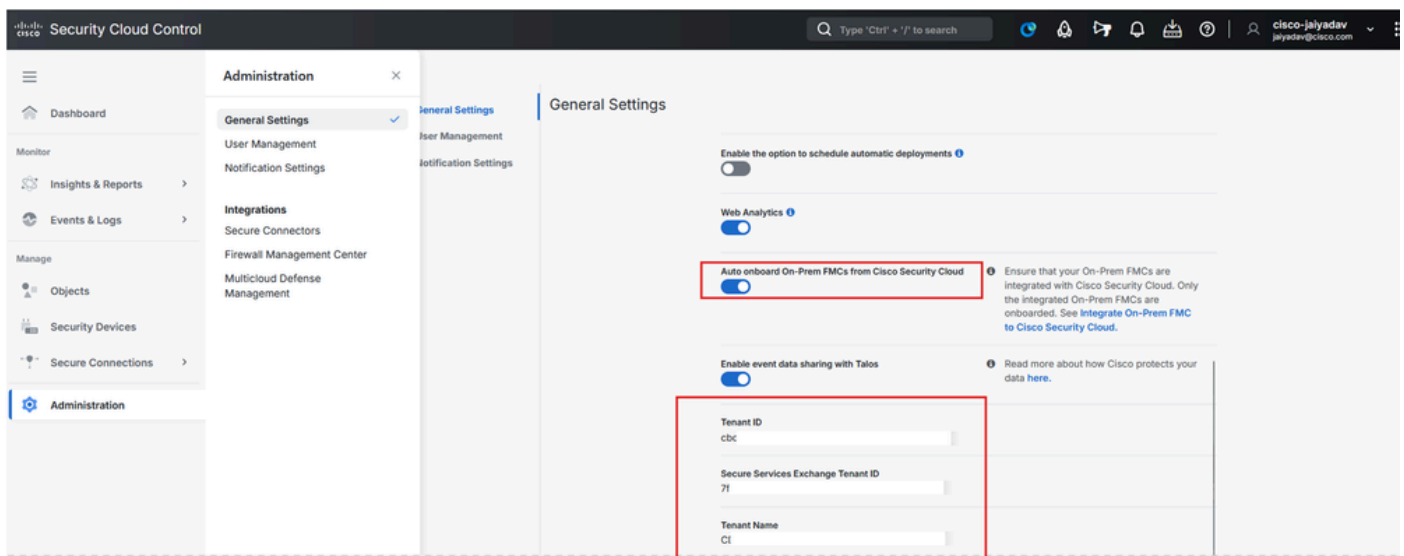
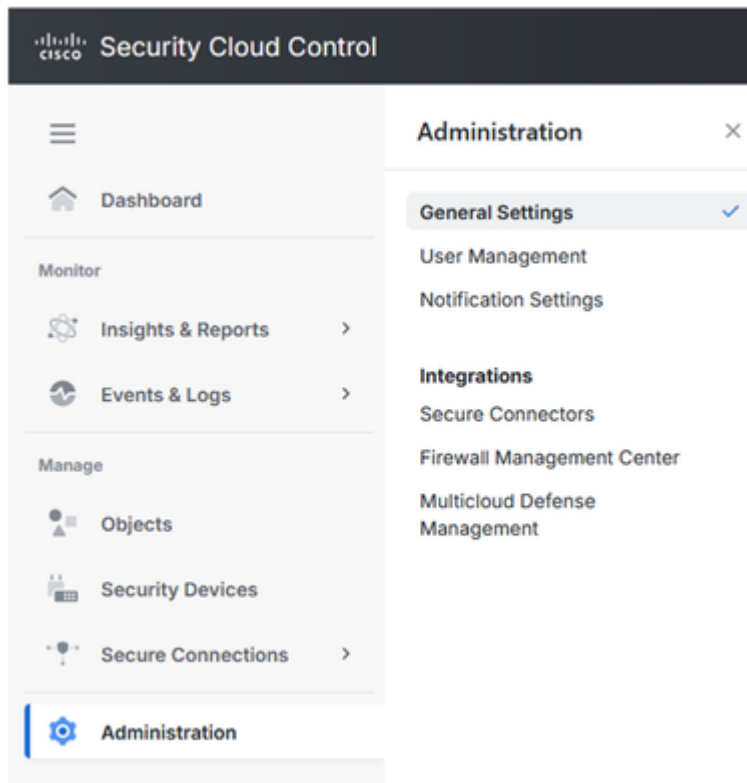
SCC 방화벽 일반 설정이 구성되었는지 확인

CDO/[SCC](#)로 [이동합니다](#).

- **클릭** Administration > General Settings
- **옵션** Auto onboard On-Prem FMCs from Cisco Security Cloud이 활성화되었는지 확인합니다.

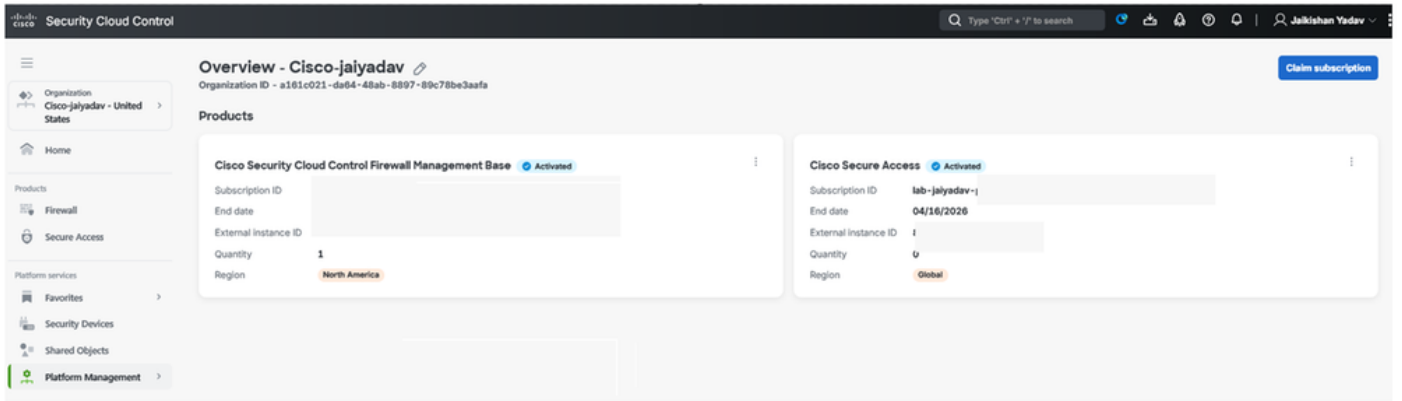


참고: Secure Access MicroApp에 액세스하려는 사용자에게는 Secure Access 및 관리자 역할 Security Cloud Control이 있어야 합니다.



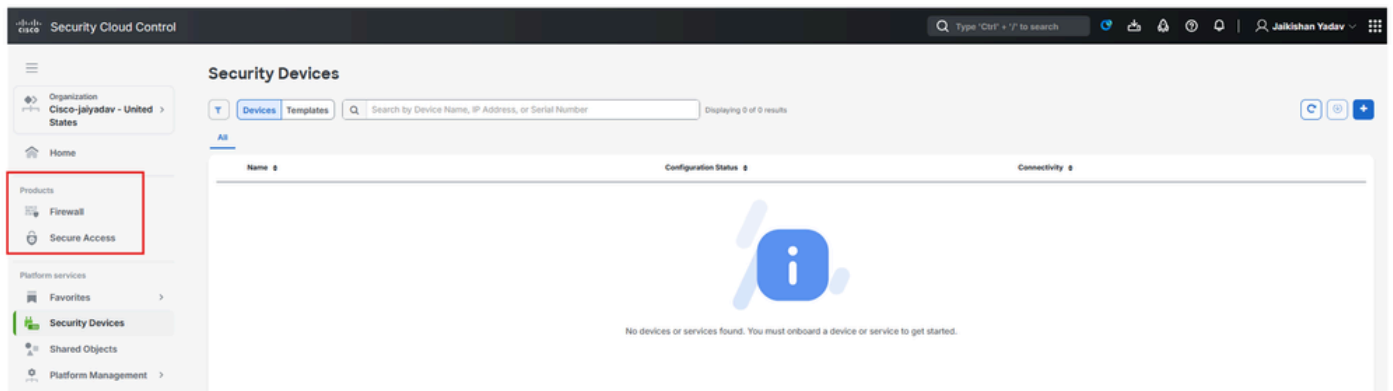
보안 클라우드 제어 - 조직 세부사항

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
- 명령expert 실행
- 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

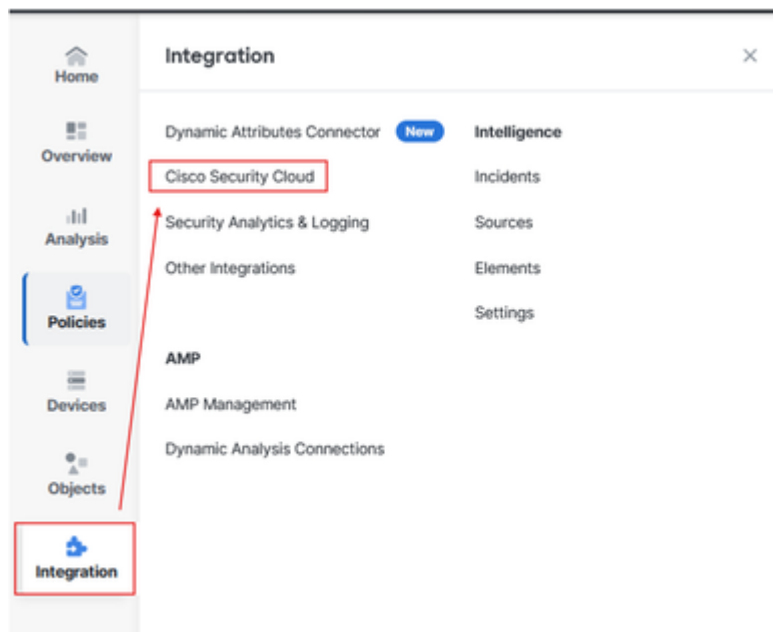
- CSR을 복사하고 CA 서명 인증서를 가져옵니다.
- FTD CA 서명 인증서와 키를 사용하고 인증서를 PKCS12 형식으로 변환합니다.
 - OpenSSL 명령:

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

- SCP 또는 기타 툴을 사용하여 인증서를 내보냅니다.

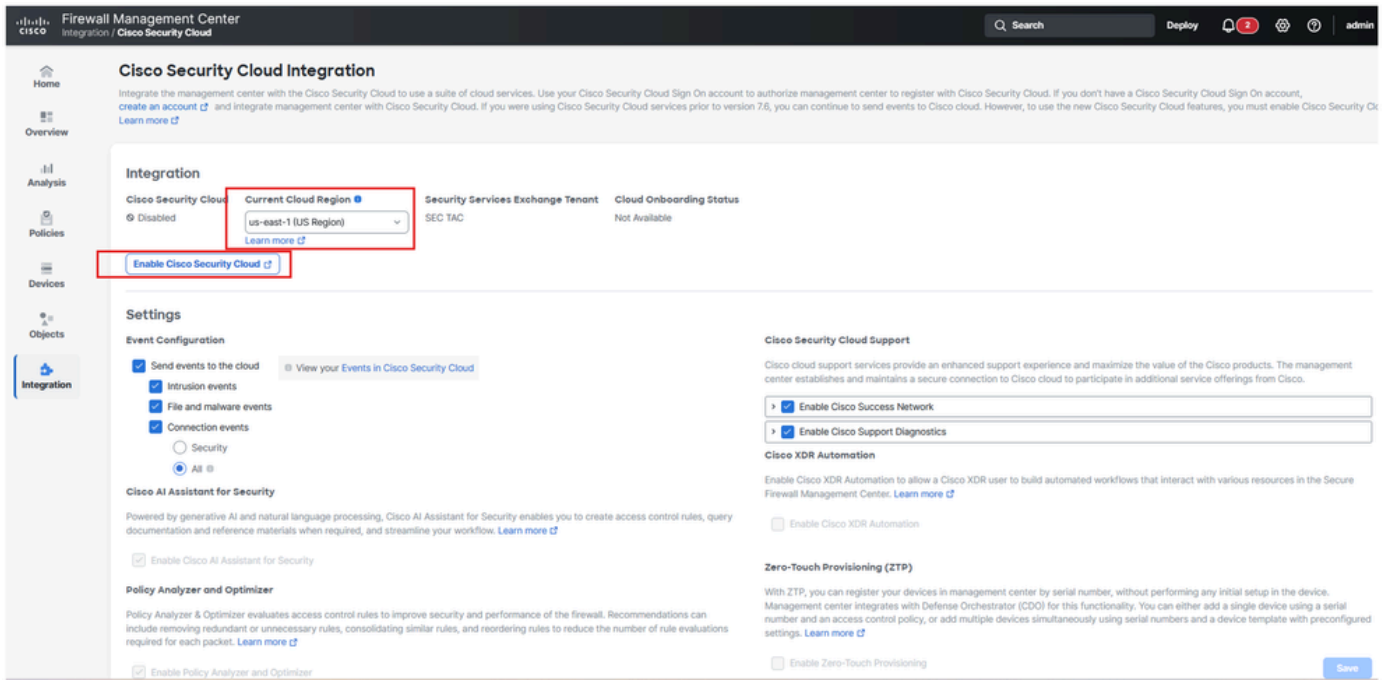
온보드 온프레미스 방화벽 관리 센터에서 보안 클라우드 제어로
FMC로 이동합니다.

- **클릭** Integration > Cisco Security Cloud



방화벽 관리 센터 및 SCC 통합

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



The screenshot shows the Cisco Firewall Management Center (FMC) interface. The top navigation bar includes the Cisco logo, 'Firewall Management Center', and a search bar. The main content area is titled 'Cisco Security Cloud Integration'. It includes a sidebar with navigation options like Home, Overview, Analysis, Policies, Devices, and Objects. The main content area has a section for 'Integration' with a 'Current Cloud Region' dropdown menu set to 'us-east-1 (US Region)'. Below this, there is a button labeled 'Enable Cisco Security Cloud'. The 'Settings' section is also visible, containing 'Event Configuration' with checkboxes for 'Send events to the cloud', 'Intrusion events', 'File and malware events', and 'Connection events'. The 'Cisco AI Assistant for Security' section is also present.

SCC에 대한 방화벽 관리 센터 온보딩

새 탭에서 새 브라우저 탭이 열립니다.

- 클릭 Continue to Cisco SSO

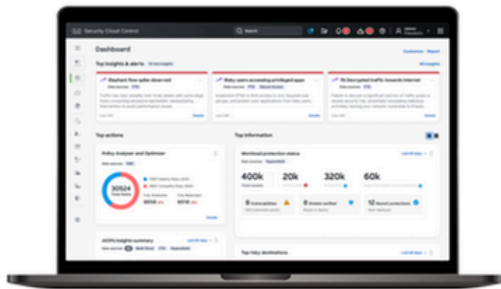


참고: SCC에서 로그아웃했으며 다른 탭이 열려 있지 않은지 확인하십시오.



Welcome to the Cisco Security Cloud Delivered through Security Cloud Control (SCC)

Staying on top of security is easier than ever. Security Cloud Control helps you consistently manage policies across your Cisco security products. It is a cloud-based application that cuts through complexity to save time and keep your organization protected against the latest threats.



SCC complements FMC by allowing you to:

- Drive consistent policy through shared object management with FMCs
- Enable Zero-Touch Provisioning of FTDs
- View events in the cloud
- Get a centralized view of inventory across FMCs
- Leverage cloud CSDAC and Cloud Delivered FMC
- and **more**

To continue with cloud registration of your FMC, you will need a Cisco Security Cloud Sign On (SSO) user account.

If you don't already have a Cisco SSO account, please proceed below and Sign Up for free. Note that you will need to restart the cloud registration from your FMC after your new SSO account is created.

If you already have a Cisco SSO account, please proceed below to choose or create a free SCC account to register your FMC.

Let's get started!


- 1 Sign Up/Sign In with Cisco SSO
- 2 Register FMC with a SCC Tenant

[Continue to Cisco SSO](#)


SCC에 대한 방화벽 관리 센터 온보딩

- SCC 테넌트를 선택하고 Authorize FMC





Welcome to Security Cloud Control

 To proceed with the registration of your FMC, please select a SCC tenant or enterprise to register with the FMC and verify the code displayed below matches the user code from your FMC.

☒ Select Tenant

☐ Create Tenant

Search Tenants

cisco-jaiyadav

cisco-ngfw-us-sspt

cisco-vibobrov

default_enterprise

Grant Application Access

Compare the code below to the authorization code shown in the FMC tab. If the codes match, authorize the FMC to complete the registration. If the codes do not match, [cancel registration](#).

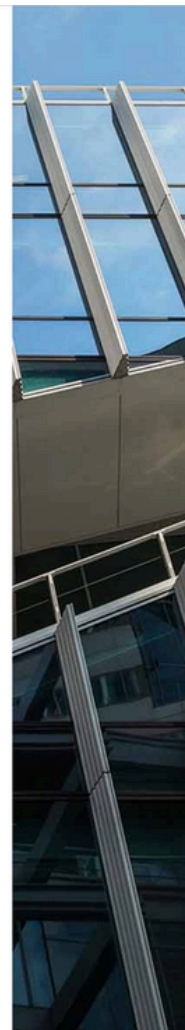
8ABA15B5

FMC would like access to your SCC tenant **cisco-jaiyadav**.

- **Users:** All internal users in FMC will have read-only access to this SCC tenant.
- **Data:** FMC will be able to collect data using SCC APIs.

The FMC will be registered with tenant **cisco-jaiyadav**

Authorize FMC



SCC에 대한 방화벽 관리 센터 온보딩

- 클릭 Save

Firewall Management Center

Integration / Cisco Security Cloud

Q Search

Deploy

2

admin

Home

Overview

Analysis

Policies

Devices

Objects

Integration

Integration

Cisco Security Cloud

Current Cloud Region

us-east-1 (US Region)

Learn more

Security Services Exchange Tenant

SEC TAC

Cloud Onboarding Status

Not Available

⚠ Cisco Security Cloud is enabled for US Region. Save your configuration for this change to take effect.

Enable Cisco Security Cloud

Settings

Event Configuration

☒ Send events to the cloud

View your Events in Cisco Security Cloud

☒ Intrusion events

☒ File and malware events

☒ Connection events

☐ Security

☒ All

Cisco AI Assistant for Security

Powered by generative AI and natural language processing, Cisco AI Assistant for Security enables you to create access control rules, query documentation and reference materials when required, and streamline your workflow. [Learn more](#)

☒ Enable Cisco AI Assistant for Security

Policy Analyzer and Optimizer

Policy Analyzer & Optimizer evaluates access control rules to improve security and performance of the firewall. Recommendations can include removing redundant or unnecessary rules, consolidating similar rules, and reordering rules to reduce the number of rule evaluations required for each packet. [Learn more](#)

☒ Enable Policy Analyzer and Optimizer

Cisco Security Cloud Support

Cisco cloud support services provide an enhanced support experience and maximize the value of the Cisco products. The management center establishes and maintains a secure connection to Cisco cloud to participate in additional service offerings from Cisco.

☒ Enable Cisco Success Network

☒ Enable Cisco Support Diagnostics

Cisco XDR Automation

Enable Cisco XDR Automation to allow a Cisco XDR user to build automated workflows that interact with various resources in the Secure Firewall Management Center. [Learn more](#)

☐ Enable Cisco XDR Automation

Zero-Touch Provisioning (ZTP)

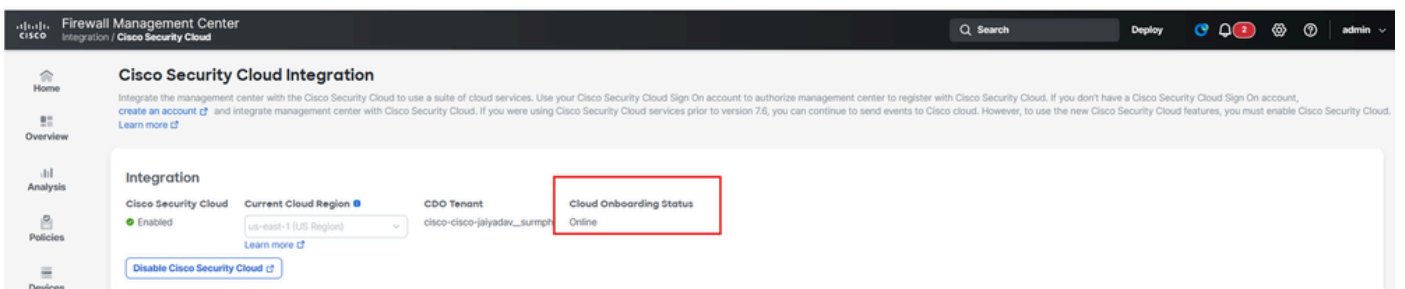
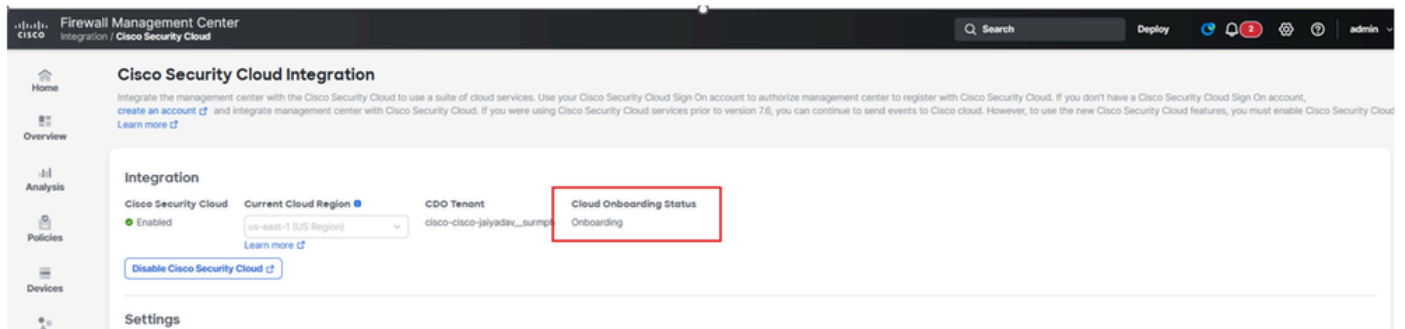
With ZTP, you can register your devices in management center by serial number, without performing any initial setup in the device. Management center integrates with Defense Orchestrator (CDO) for this functionality. You can either add a single device using a serial number and an access control policy, or add multiple devices simultaneously using serial numbers and a device template with preconfigured settings. [Learn more](#)

☒ Enable Zero-Touch Provisioning

Save

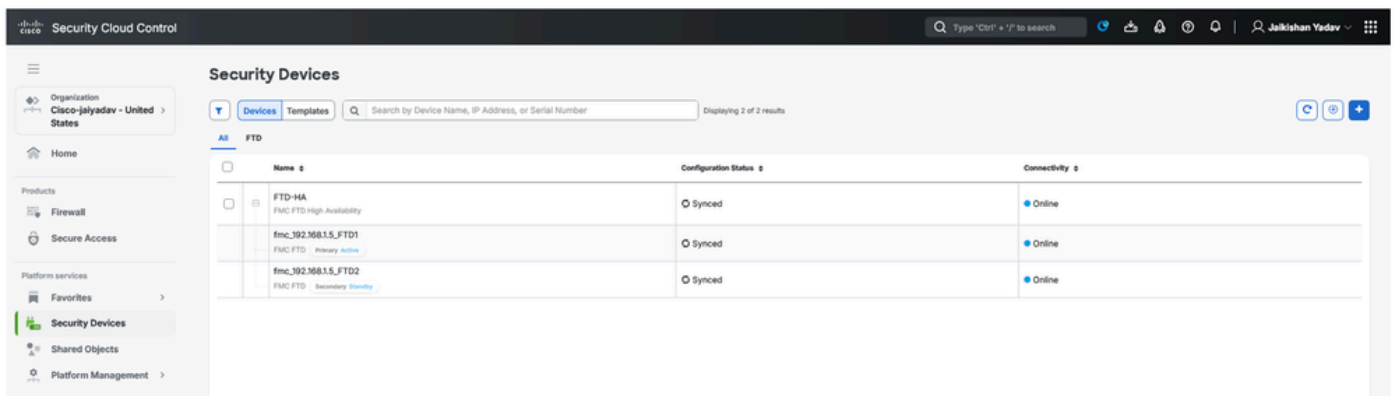
SCC에 대한 방화벽 관리 센터 온보딩

의 Cloud Onboarding Status 상태는 **Not Available** 에서 Onboarding 로 Online 변경되어야 합니다.



방화벽 관리 센터 온보딩 상태

- [SCC로 이동하여](#) Platform Services > Security Devices



SCC의 보안 방화벽 위협 방어 상태

FTD에 uZTNA(Universal Zero Trust Network Access) 설정 등록

SCC로 이동합니다.

- [클릭](#) Platform Services > Security Devices > FTD > Device Management > Universal Zero Trust Network Access

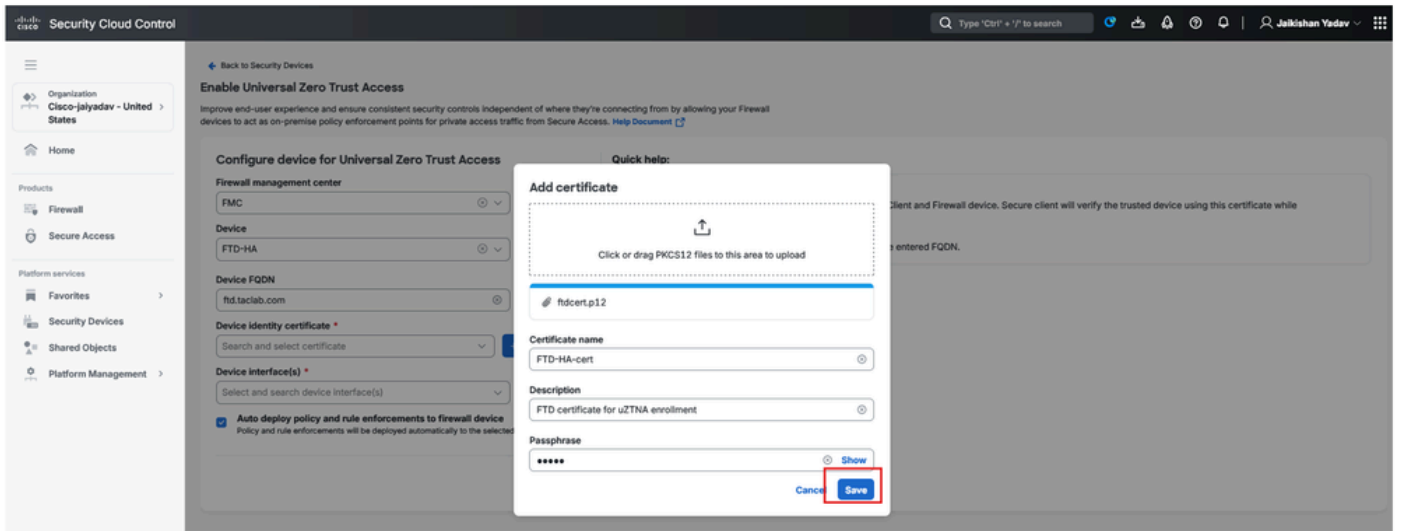
The screenshot shows the Cisco Security Cloud Control interface. On the left, the navigation menu includes 'Platform services' (1) and 'Security Devices' (2). The main area displays a table of security devices under the 'FTD' filter. The first device, 'FTD-HA' (3), is highlighted. On the right, the 'Device Details' panel shows 'Device Management' (4) and 'Universal zero trust access settings' (5) as options.

보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션

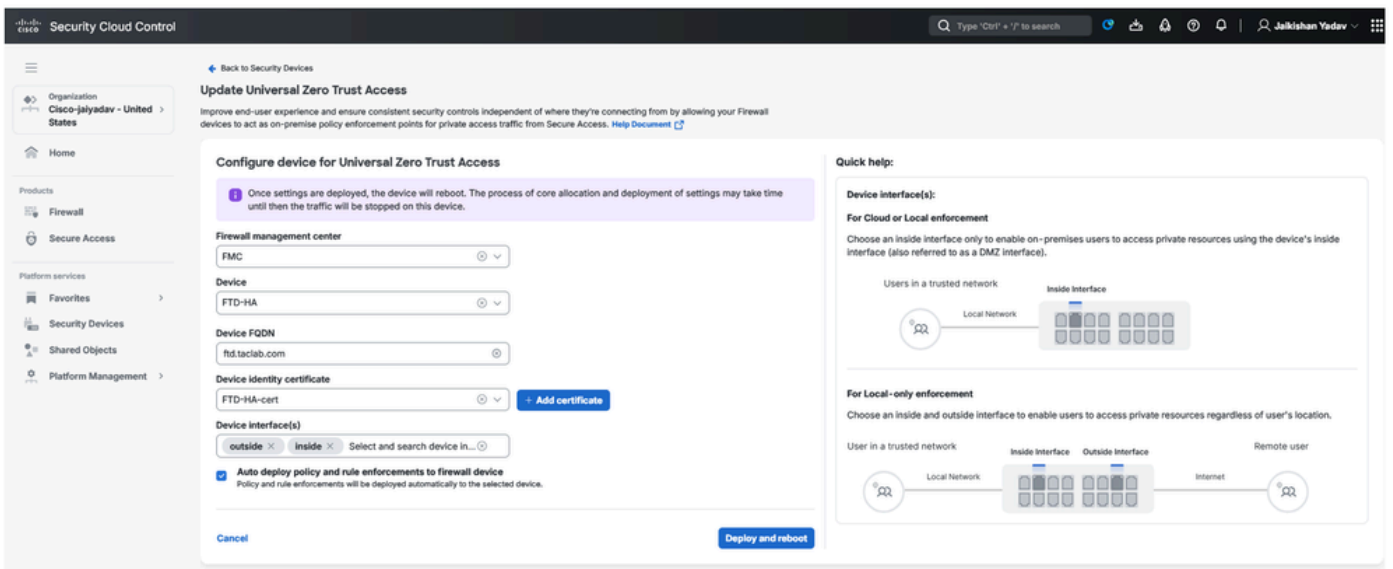
- 정보를 입력하고 FTD(Firewall Threat Defense) CA 서명 인증서 생성 단계에서 생성된 FTD 인증서를 업로드합니다

The screenshot shows the 'Enable Universal Zero Trust Access' configuration page. The 'Device Identity certificate' field is highlighted with a blue button 'Add certificate'. The page includes sections for 'Configure device for Universal Zero Trust Access' and 'Quick help' with diagrams for 'Device interface(s)' and 'For Local-only enforcement'.

보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션



보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션

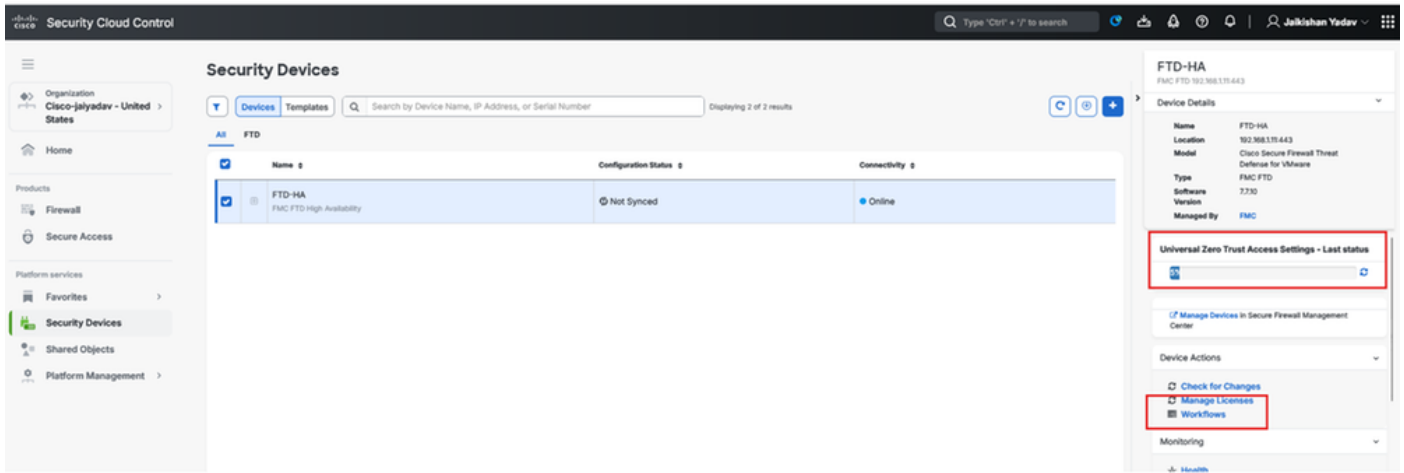


보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션

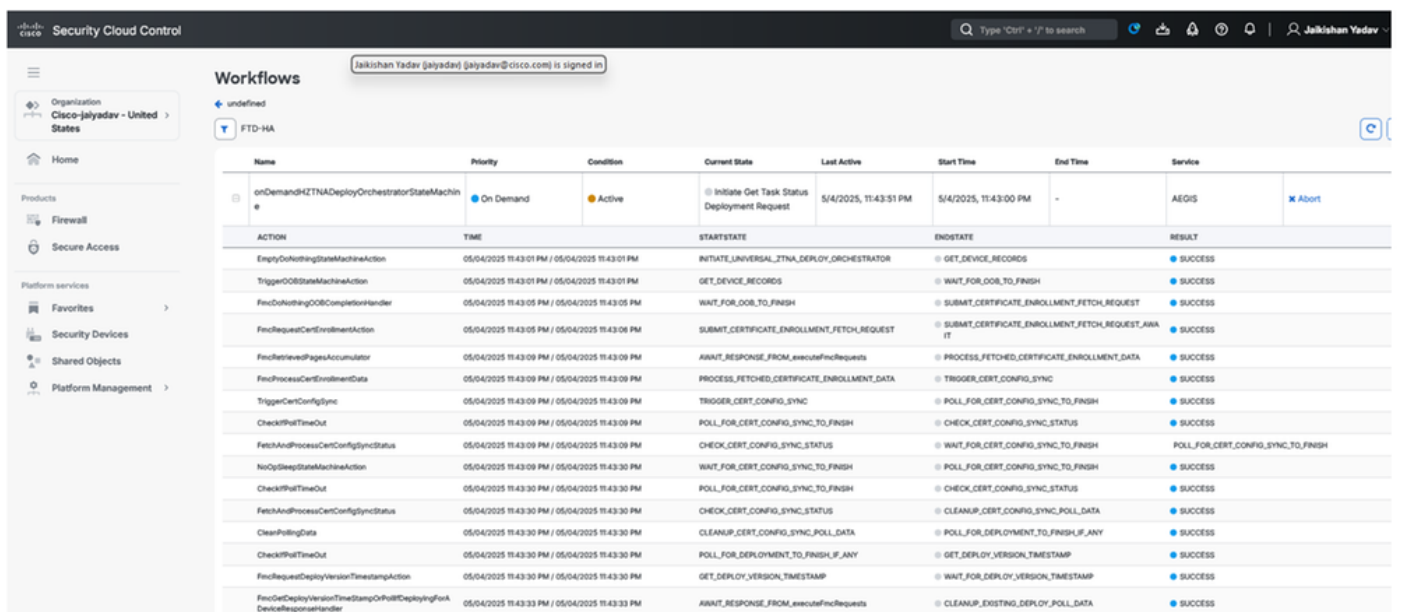


참고: FTD HA에서 uZTNA를 활성화하면 변경 사항이 구축되고 두 FTD(Firewall Threat Defense) 유닛이 동시에 재부팅됩니다. 적절한 유지 보수 기간을 예약해야 합니다.

- 로그를 확인하려면 클릭Workflow 합니다.

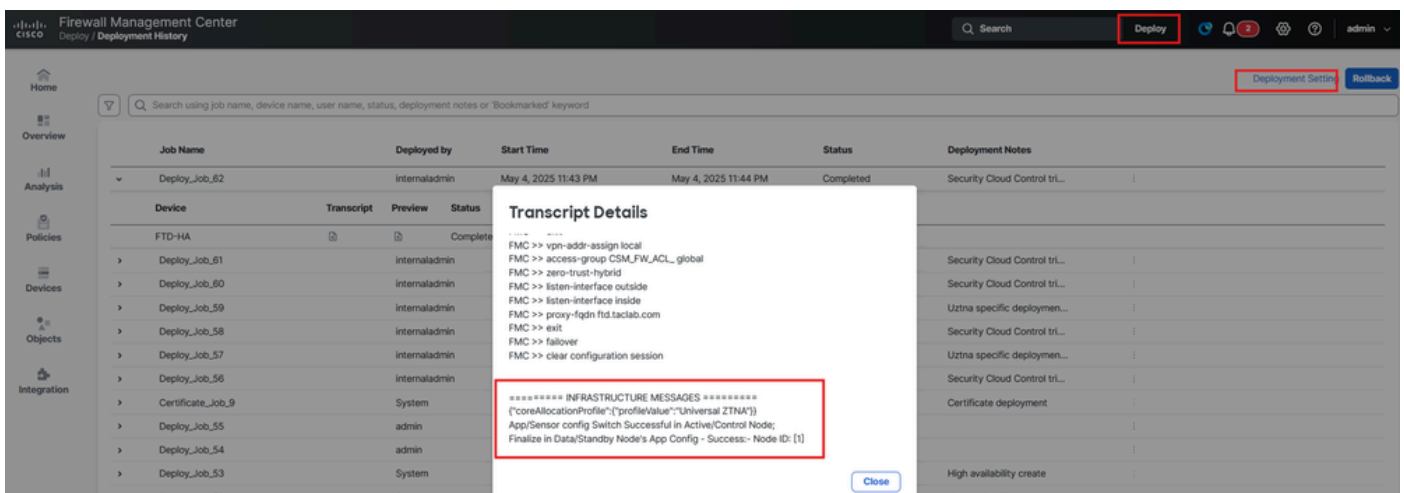


보안 방화벽 위협 방어 - 범용 ZTNA 컨피그레이션 상태



보안 클라우드 제어 워크플로

Transcript Details(대본 세부사항)에서 및 변경 사항을 볼 Policy Deployment Status 수 있습니다. FMC.



Secure Firewall Management Center - 정책 구축 상태

uZTNA에 클라이언트 등록

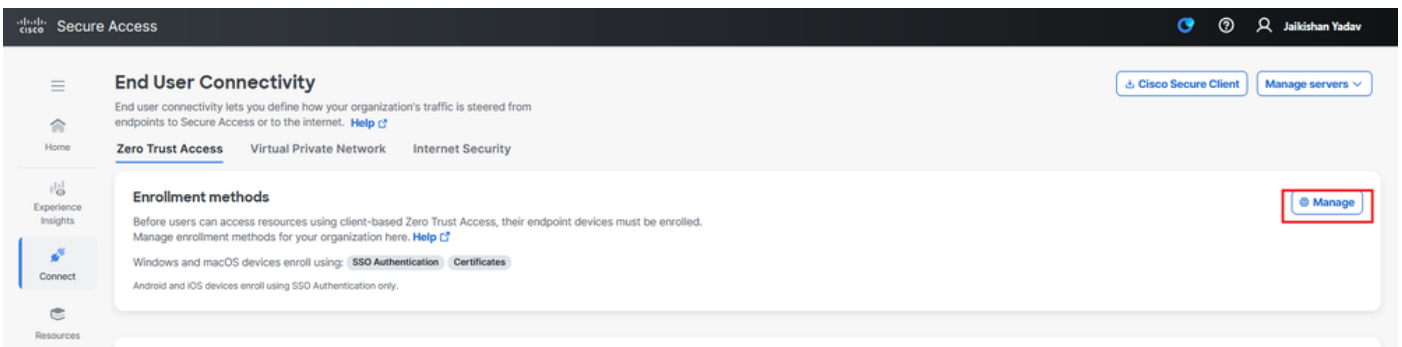
보안 액세스 컨피그레이션



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

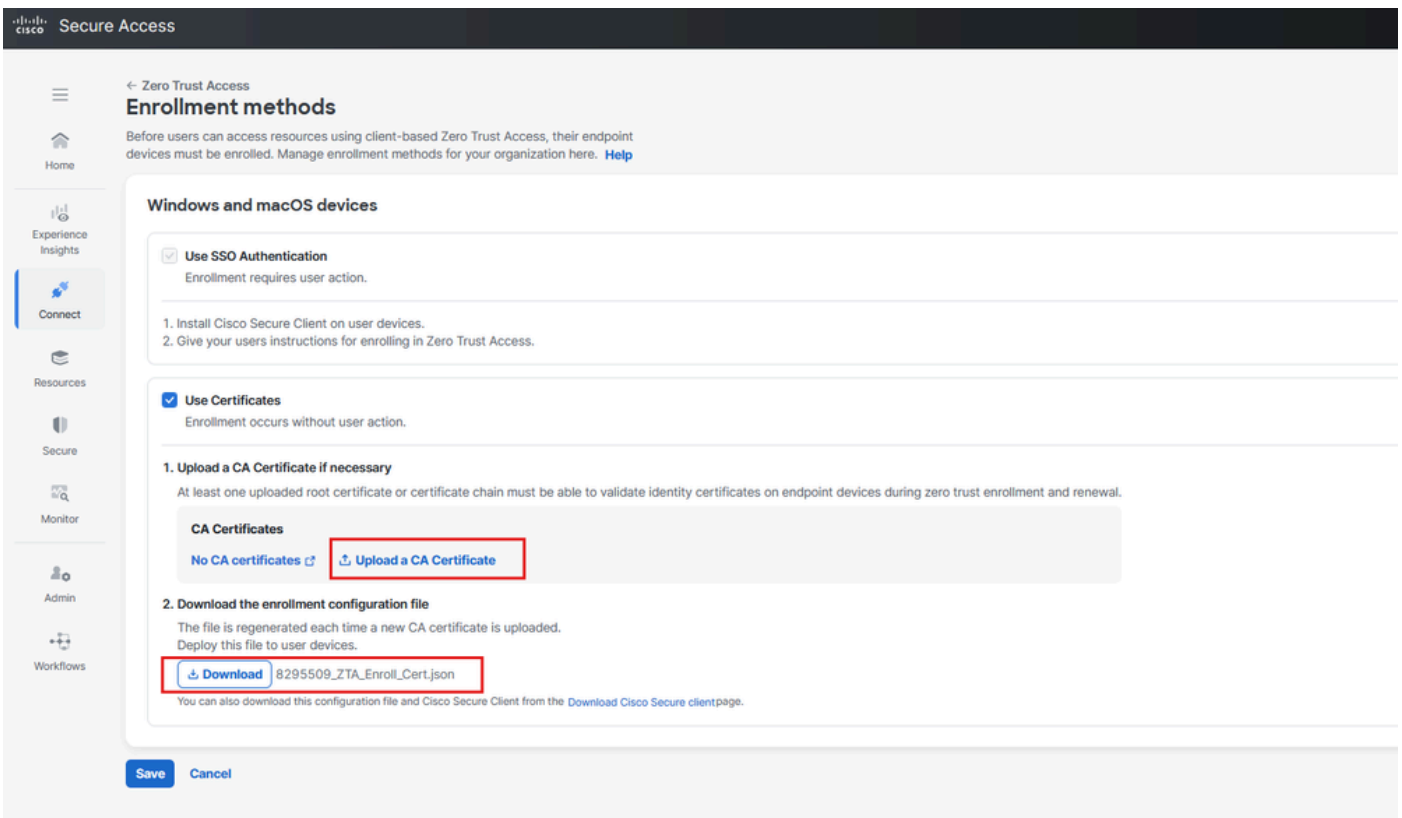
Secure [Access Dashboard\(보안 액세스 대시보드\)](#)로 이동합니다.

- > > **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

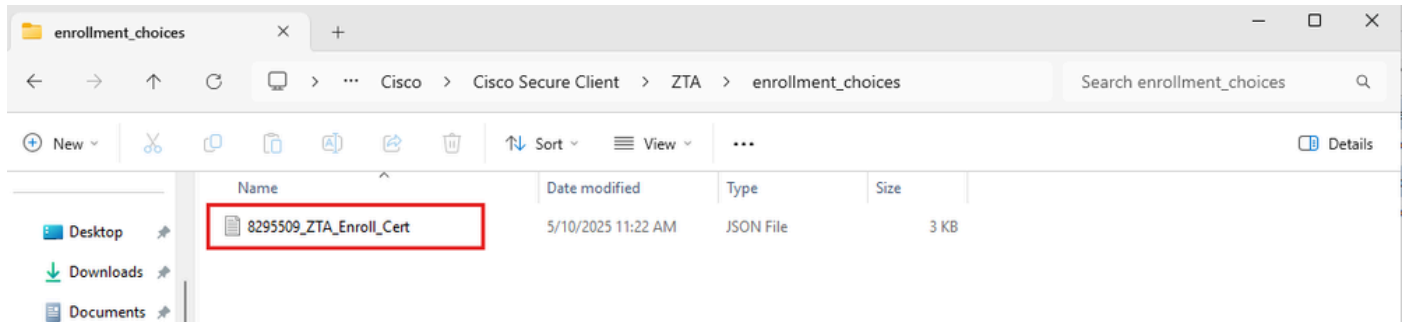


보안 액세스 - ZTA 인증서 등록

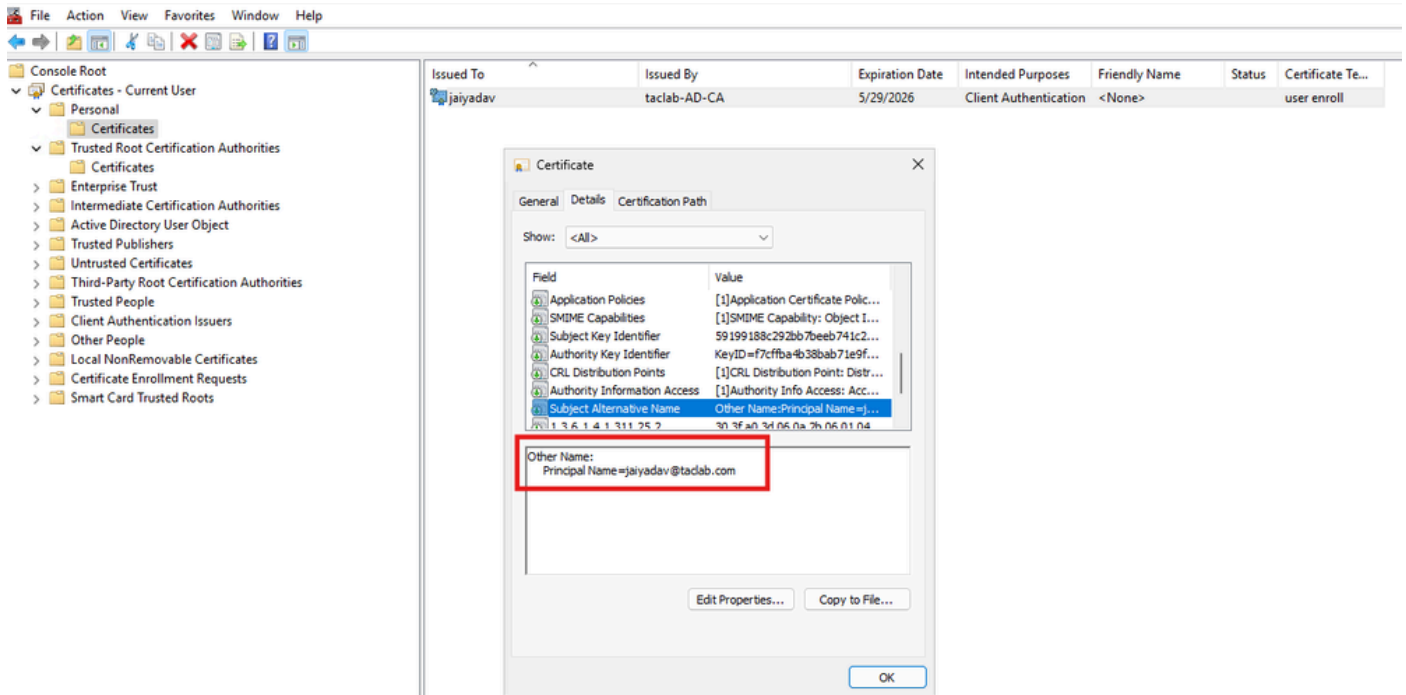
- 클릭 Save

클라이언트 컨피그레이션

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

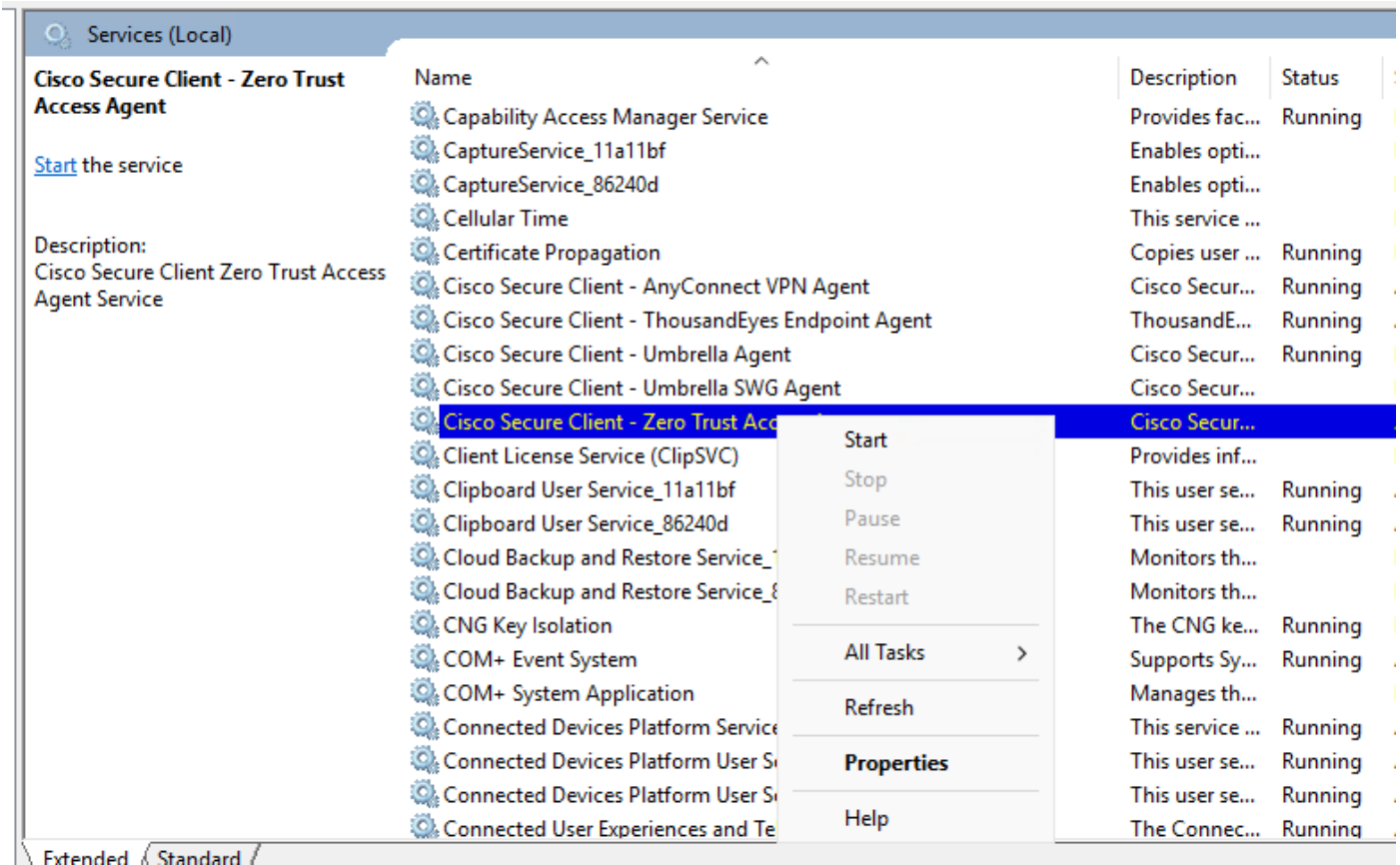


- SAN 필드에 UPN이 있어야 하는 클라이언트 인증서 생성



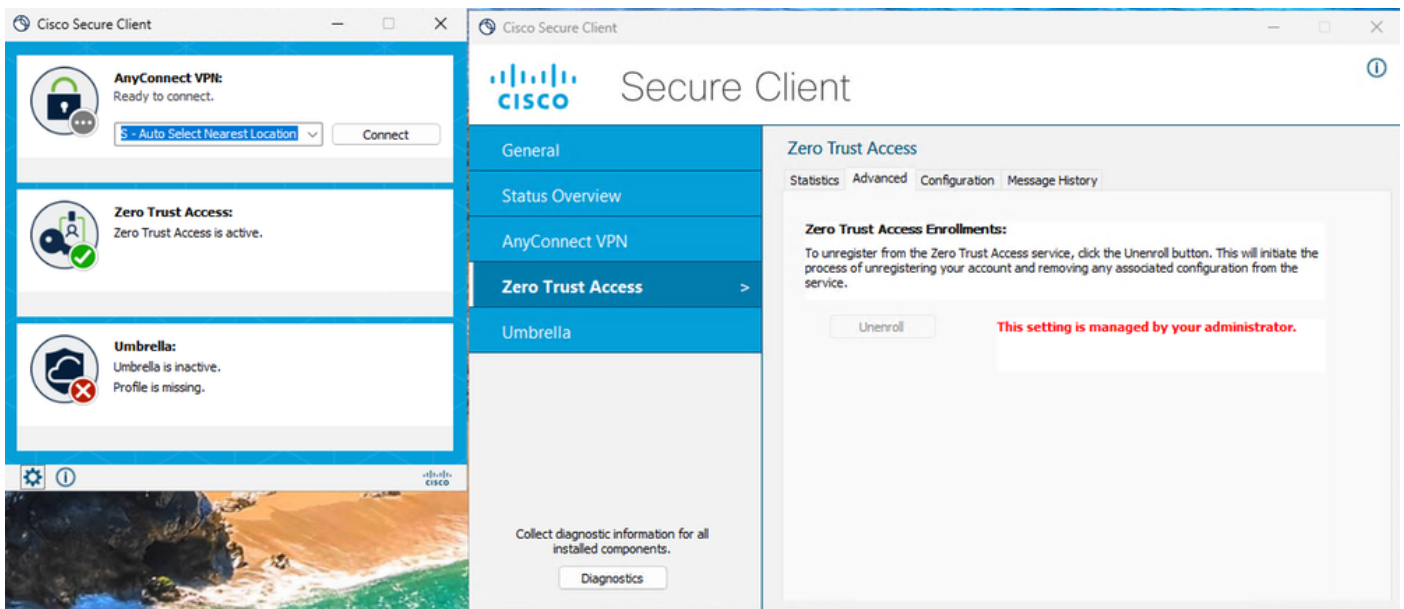
인증서 설치

- 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.