CDO(Cisco Defense Orchestrator)에서 클라우드 제공 FMC(cdFMC) 구축

목차

소개
사전 요구 사항
요구 사항
사용되는 구성 요소
배경 정보
구성
CDO에 클라우드 제공 Firepower Management Center를 구축합니다.
클라우드 제공 FMC에서 FTD 온보딩
관련 정보

소개

이 문서에서는 CDO 플랫폼에서 클라우드로 제공되는 FMC의 구축 및 온보드 프로세스에 대해 설명합니다.

사전 요구 사항

요구 사항

Cisco에서는 다음 항목에 대한 지식을 권장합니다.

- 클라우드 제공 Firepower Management Center(cdFMC)
- CDO(Cisco Defense Orchestrator)
- Firepower FTDv(Threat Defense Virtual)

사용되는 구성 요소

이 문서의 정보는 다음 소프트웨어 및 하드웨어 버전을 기반으로 합니다.

- cdFMC 7.2.0
- FTDv 7.2.0

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.

배경 정보

Cisco Defense Orchestrator(CDO)는 클라우드 기반 cdFMC(Firewall Management Center)를 위한 플랫폼입니다. 클라우드 기반 방화벽 관리 센터는 보안 방화벽 위협 방어 장치를 관리하는

SaaS(Software-as-a-Service) 제품입니다. 온프레미스 보안 방화벽 보안 방화벽 위협 방어 기능과 동일한 기능을 다수 제공합니다. 온프레미스 Secure Firewall Management Center와 모양과 동작이 동일하며 동일한 FMC API(Application Programming Interface)를 사용합니다.

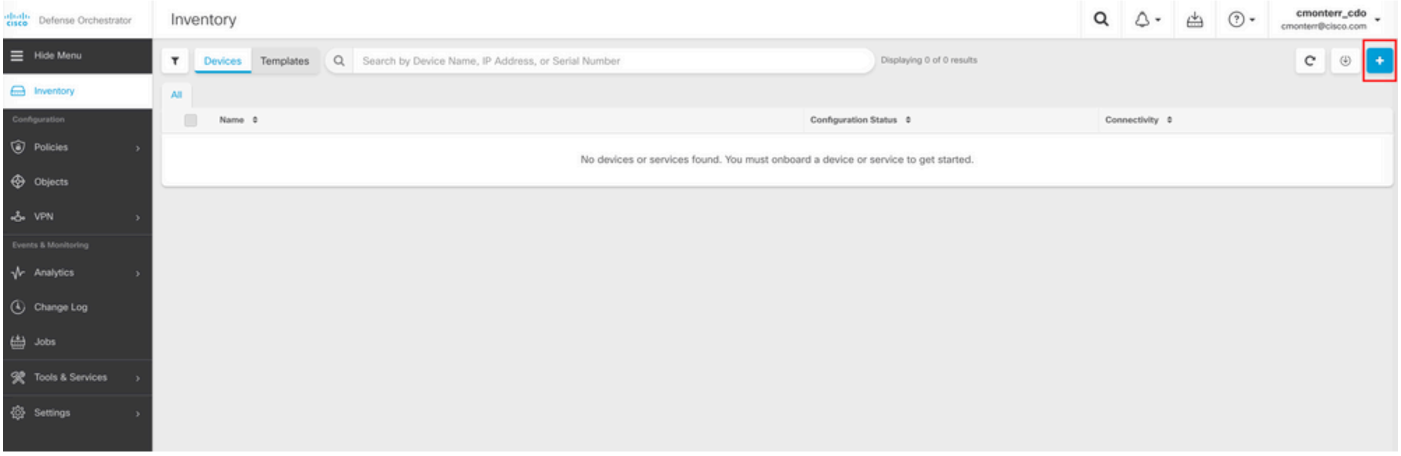
이 제품은 온프레미스 Secure Firewall Management Center에서 Secure Firewall Management Center SaaS 버전으로 마이그레이션하도록 설계되었습니다.

구성

CDO에 클라우드 제공 Firepower Management Center를 구축합니다.

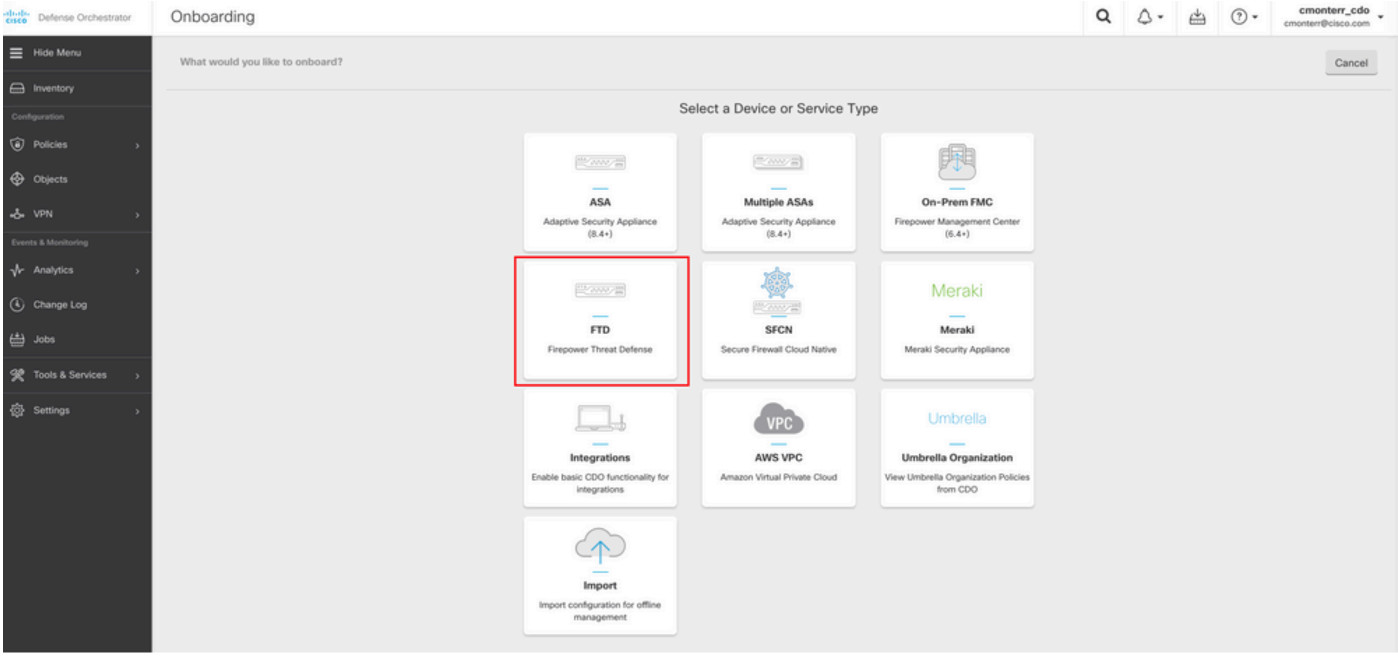
이 그림은 CDO에 클라우드 제공 FMC를 구축하는 데 필요한 초기 설정 프로세스를 보여줍니다.

먼저, **Menu > Inventory** 새 디바이스를 추가합니다.

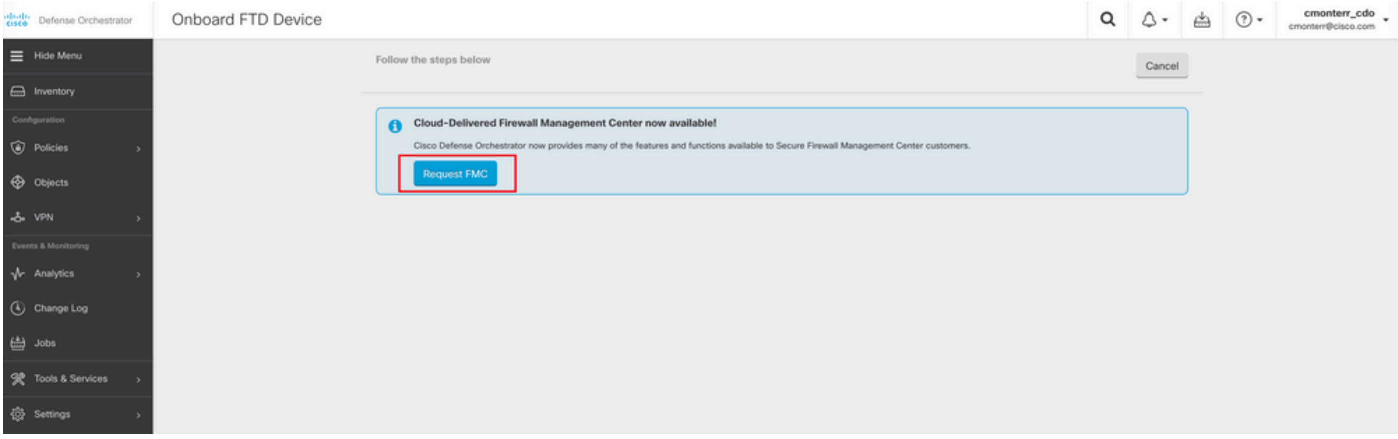


No devices or services found. You must onboard a device or service to get started.

선택 **Firepower Threat Defense (FTD).**


Defense Orchestrator
Onboarding
cmonterr_cdo
cmonterr@cisco.com
Hide Menu
Inventory
Configuration
Policies
Objects
VPN
Events & Monitoring
Analytics
Change Log
Jobs
Tools & Services
Settings
What would you like to onboard?
Cancel
Select a Device or Service Type
ASA
Adaptive Security Appliance (8.4+)
Multiple ASAs
Adaptive Security Appliance (8.4+)
On-Prem FMC
Firepower Management Center (6.4+)
FTD
Firepower Threat Defense
SFCN
Secure Firewall Cloud Native
Meraki
Meraki
Meraki Security Appliance
Integrations
Enable basic CDO functionality for integrations
VPC
AWS VPC
Amazon Virtual Private Cloud
Umbrella
Umbrella Organization
View Umbrella Organization Policies from CDO
Import
Import configuration for offline management

선택 **Request FMC** Firepower Management Center를 요청할 수 있습니다.

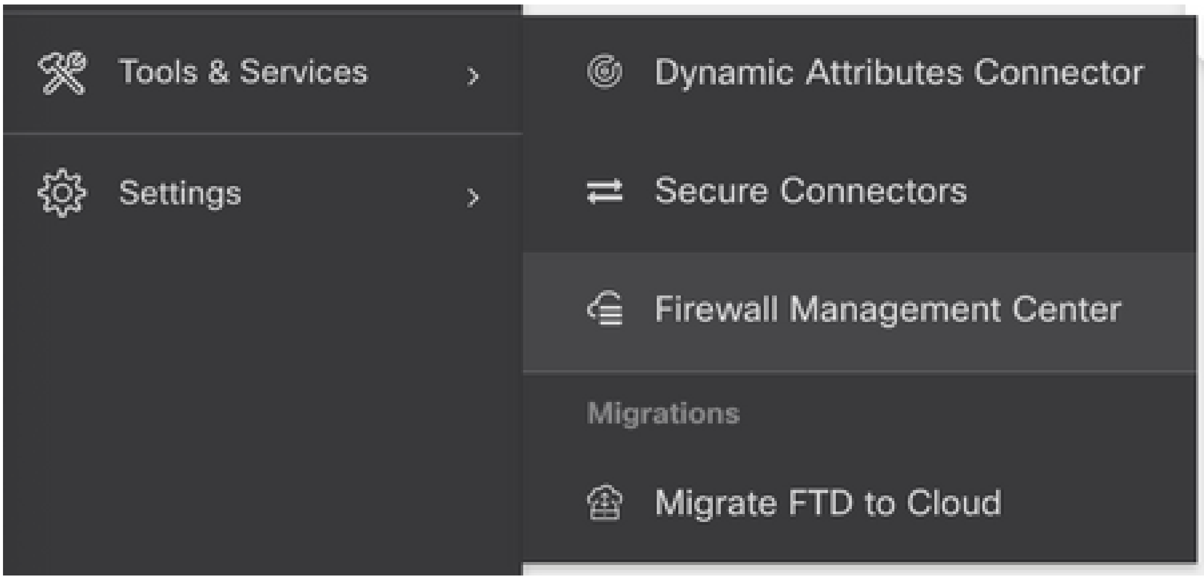


Cloud-Delivered Firewall Management Center now available!

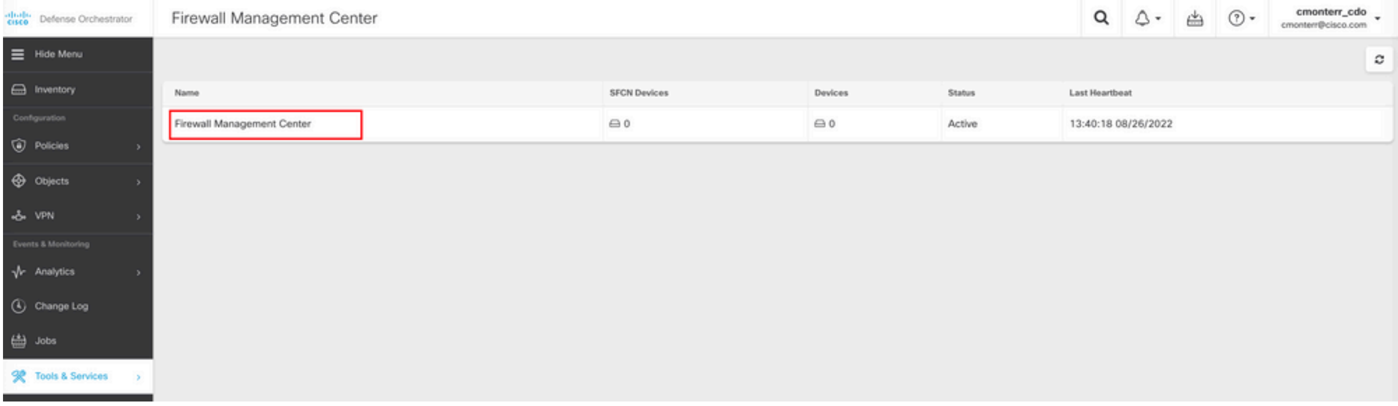
Cisco Defense Orchestrator now provides many of the features and functions available to Secure Firewall Management Center customers.

참고: 테넌트에 cdFMC가 없는 경우에만 "FMC 요청" 옵션이 표시됩니다.

탐색 **Menu > Tools & Services > Firewall Management Center** cdFMC를 사용할 준비가 된 경우

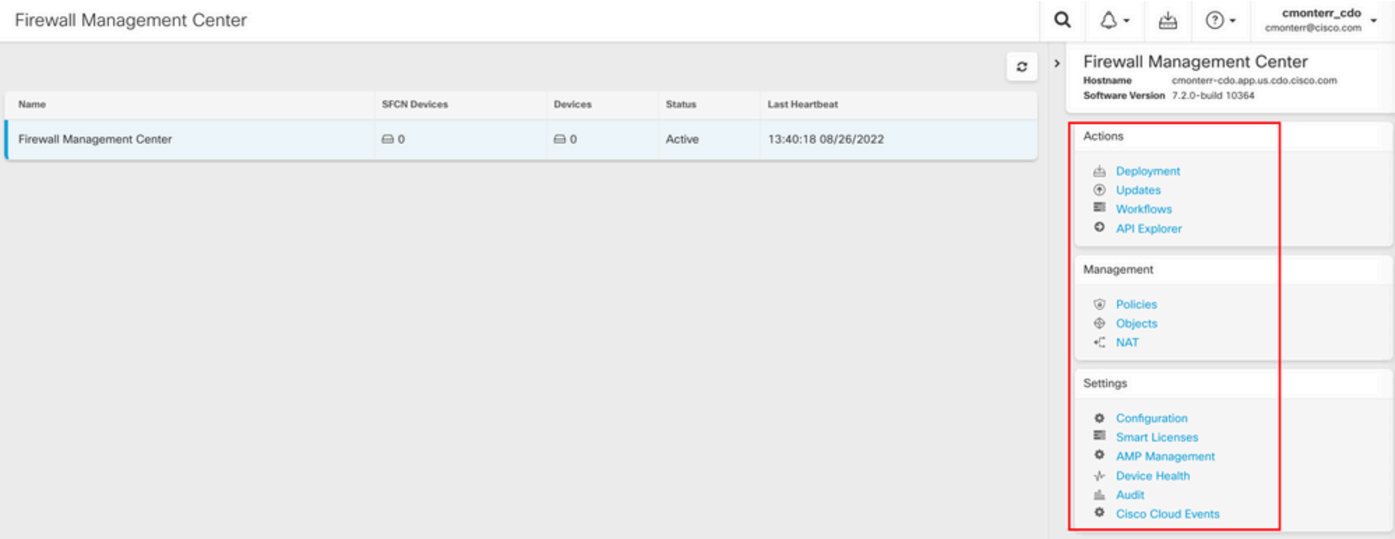


원하는 cdFMC를 선택하여 cdFMC 정보를 표시합니다.



Name	SFCN Devices	Devices	Status	Last Heartbeat
Firewall Management Center	0	0	Active	13:40:18 08/26/2022

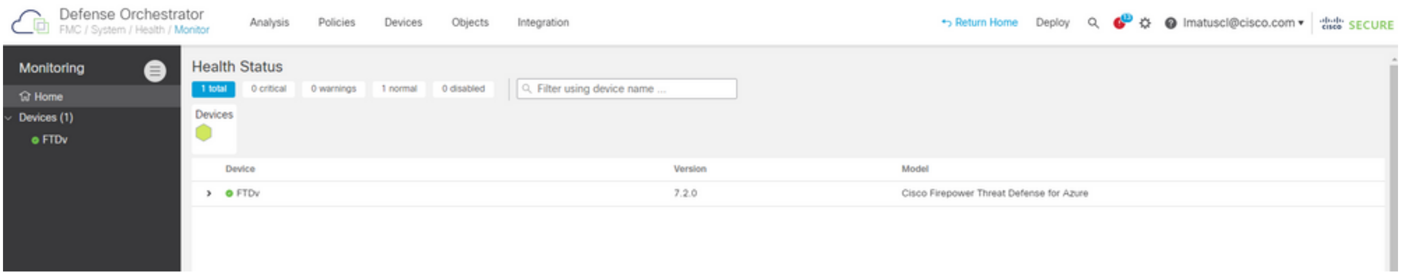
cdFMC의 GUI(Graphical User Interface)에 액세스하려면 오른쪽에서 사용 가능한 옵션을 선택합니다.



Name	SFCN Devices	Devices	Status	Last Heartbeat
Firewall Management Center	0	0	Active	13:40:18 08/26/2022

Firewall Management Center
Hostname cmonterr-cdo.app.us.cdo.cisco.com
Software Version 7.2.0-build 10364

이제 cdFMC GUI를 볼 수 있습니다.

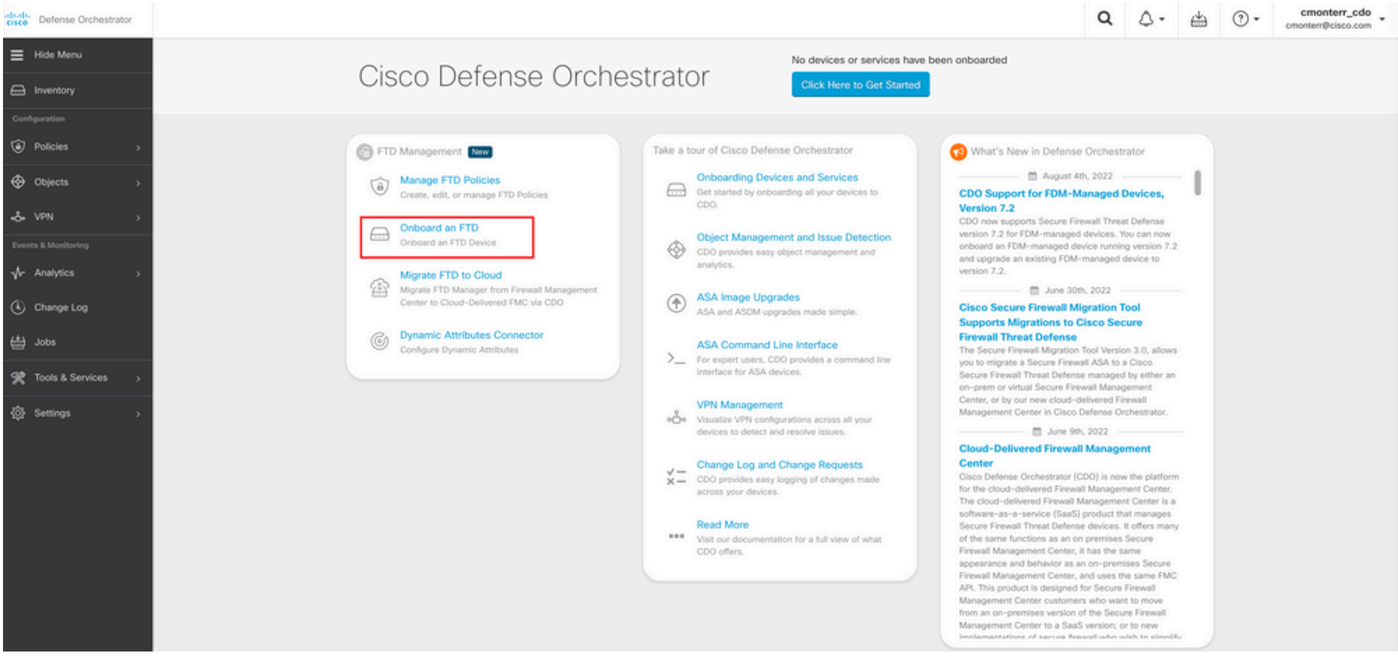


Device	Version	Model
FTDv	7.2.0	Cisco Firepower Threat Defense for Azure

클라우드 제공 FMC에서 FTD 온보딩

이 그림에서는 CLI(Command Line Interface) 등록 키를 사용하여 cdFMC에 등록하기 위해 FTD를 온보딩하는 방법을 보여 줍니다.

먼저 **Onboard an FTD** CDO 홈 페이지.



No devices or services have been onboarded

Manage FTD Policies
Create, edit, or manage FTD Policies

Onboard an FTD
Onboard an FTD Device

Migrate FTD to Cloud
Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO

Dynamic Attributes Connector
Configure Dynamic Attributes

Onboarding Devices and Services
Get started by onboarding all your devices to CDO.

Object Management and Issue Detection
CDO provides easy object management and analytics.

ASA Image Upgrades
ASA and ASDM upgrades made simple.

ASA Command Line Interface
For expert users, CDO provides a command line interface for ASA devices.

VPN Management
Visualize VPN configurations across all your devices to detect and resolve issues.

Change Log and Change Requests
CDO provides easy logging of changes made across your devices.

Read More
Visit our documentation for a full view of what CDO offers.

August 4th, 2022

CDO Support for FDM-Managed Devices, Version 7.2
CDO now supports Secure Firewall Threat Defense version 7.2 for FDM-managed devices. You can now onboard an FDM-managed device running version 7.2 and upgrade an existing FDM-managed device to version 7.2.

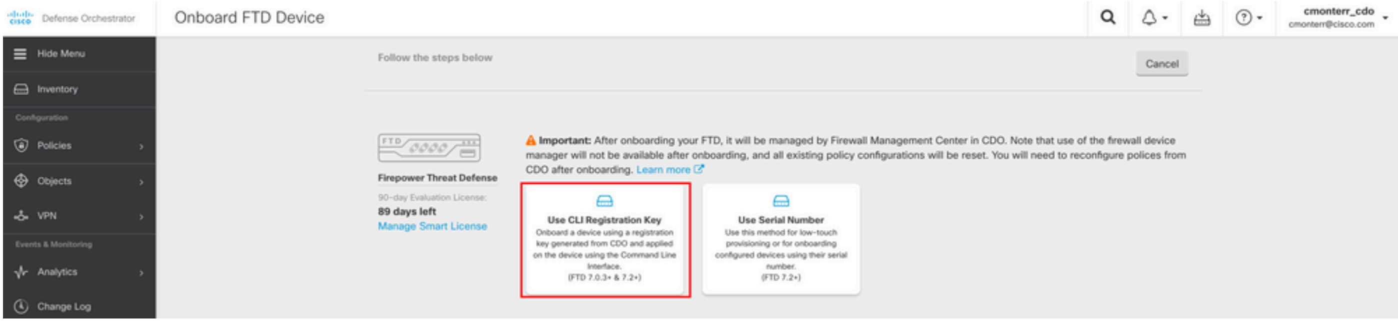
June 30th, 2022

Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense
The Secure Firewall Migration Tool Version 3.0, allows you to migrate a Secure Firewall ASA to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.

June 9th, 2022

Cloud-Delivered Firewall Management Center
Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center. The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API. This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version; or to new implementations of secure firewall who wish to simplify

그런 다음 **Use CLI Registration Key** 옵션을 선택합니다.



Follow the steps below

Firepower Threat Defense

90-day Evaluation License:

89 days left

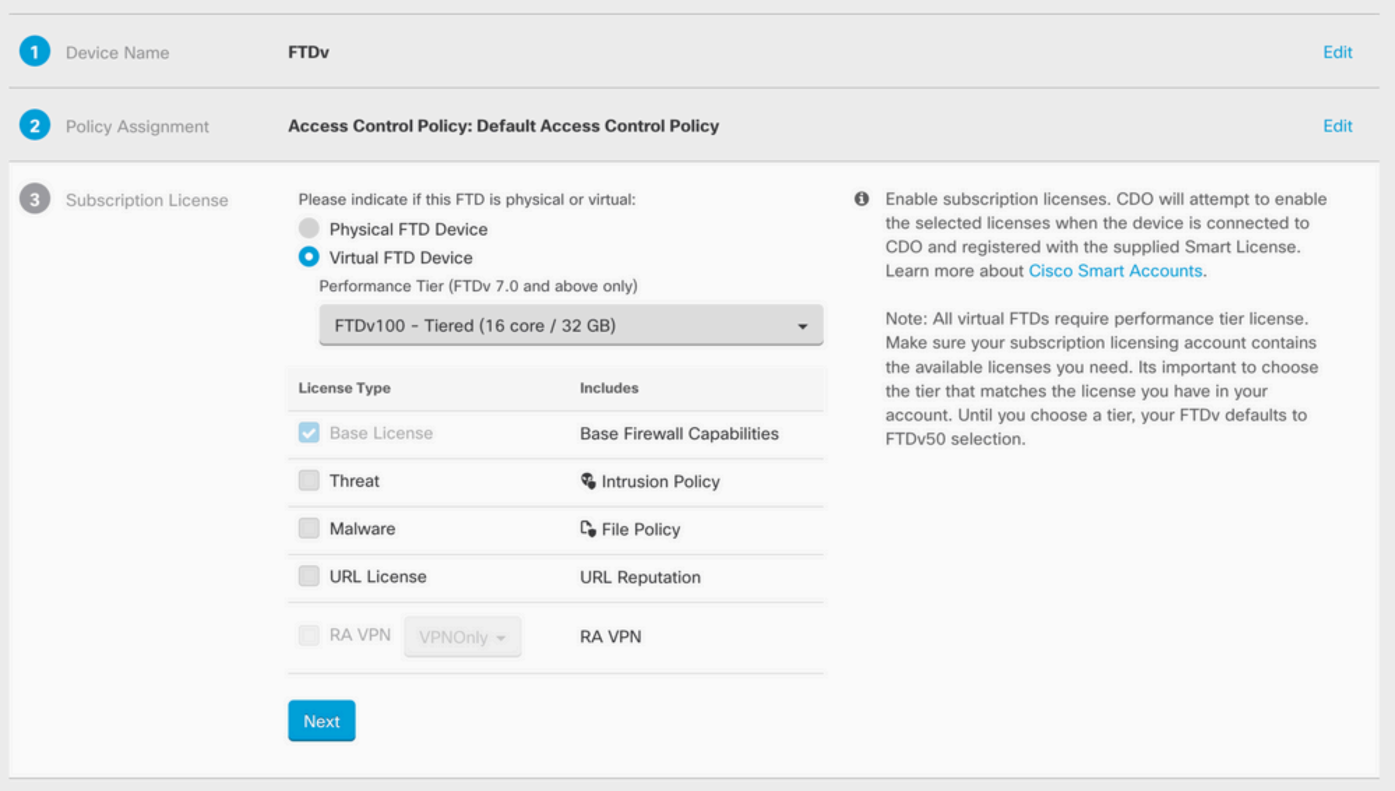
Manage Smart License

Important: After onboarding your FTD, it will be managed by Firewall Management Center in CDO. Note that use of the firewall device manager will not be available after onboarding, and all existing policy configurations will be reset. You will need to reconfigure polices from CDO after onboarding. Learn more

Use CLI Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using the Command Line Interface.
(FTD 7.0.3+ & 7.2+)

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 7.2+)

요청된 FTDv 정보와 원하는 FTDv 정보를 계속 입력합니다.



1 Device Name — **FTDv** — Edit

2 Policy Assignment — **Access Control Policy: Default Access Control Policy** — Edit

3 Subscription License

Please indicate if this FTD is physical or virtual:

○ Physical FTD Device

● Virtual FTD Device

Performance Tier (FTDv 7.0 and above only)

FTDv100 - Tiered (16 core / 32 GB)

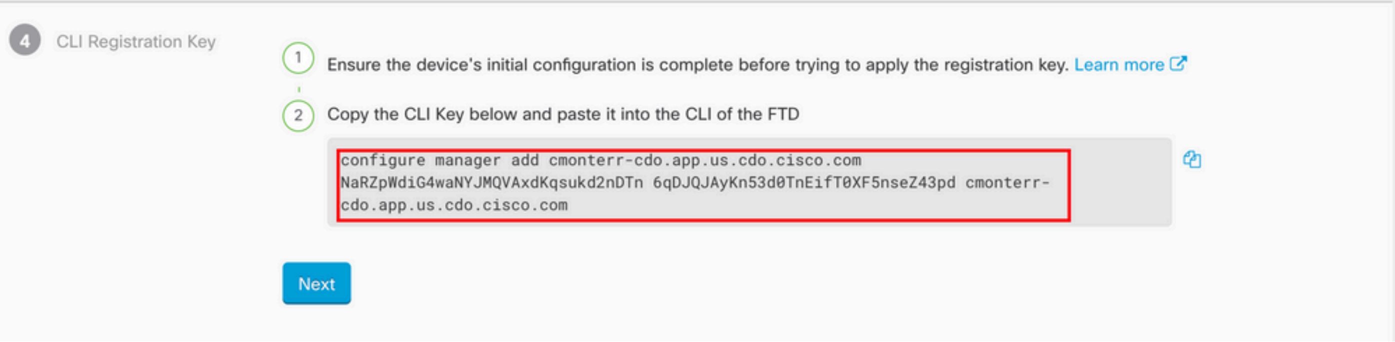
License Type	Includes
☑ Base License	Base Firewall Capabilities
□ Threat	Intrusion Policy
□ Malware	File Policy
□ URL License	URL Reputation
□ RA VPN VPNOnly	RA VPN

Next

Enable subscription licenses. CDO will attempt to enable the selected licenses when the device is connected to CDO and registered with the supplied Smart License. Learn more about Cisco Smart Accounts.

Note: All virtual FTDs require performance tier license. Make sure your subscription licensing account contains the available licenses you need. Its important to choose the tier that matches the license you have in your account. Until you choose a tier, your FTDv defaults to FTDv50 selection.

마지막으로, cdFMC는 **CLI Key**디바이스에 대한 CLI 키.



4 CLI Registration Key

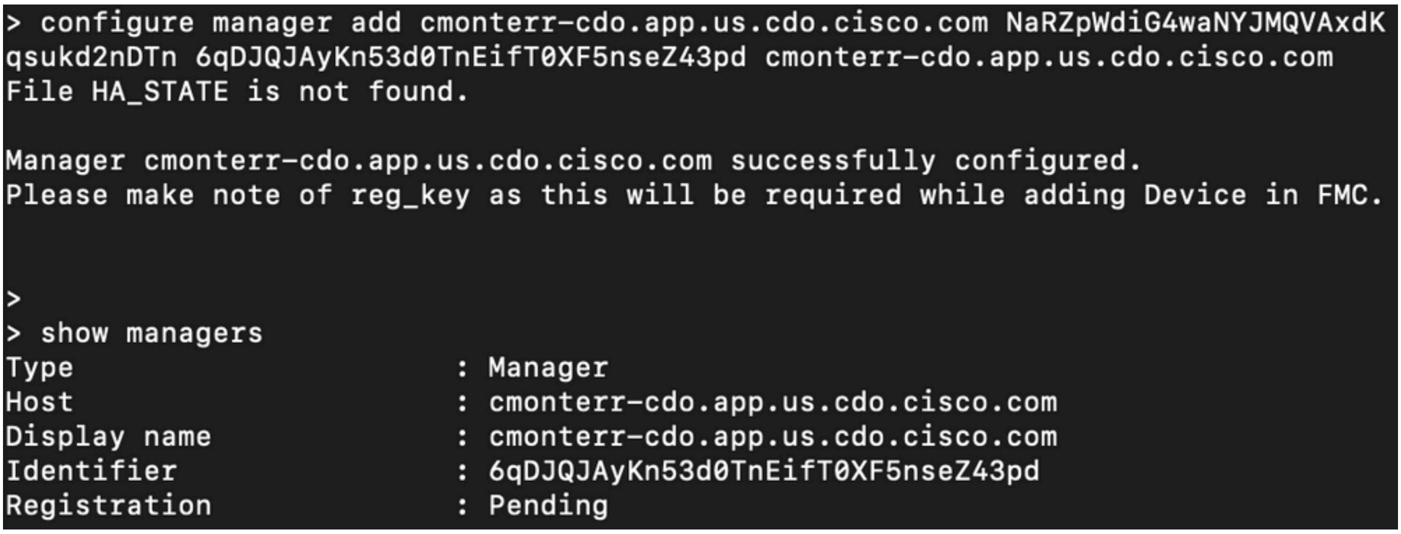
1 Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more

2 Copy the CLI Key below and paste it into the CLI of the FTD

```
configure manager add cmonterr-cdo.app.us.cdo.cisco.com
NaRZpWdiG4waNYJMQVAxdKqsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-
cdo.app.us.cdo.cisco.com
```

Next

복사 **CLI Key** 관리되는 디바이스의 CLI에 액세스합니다.

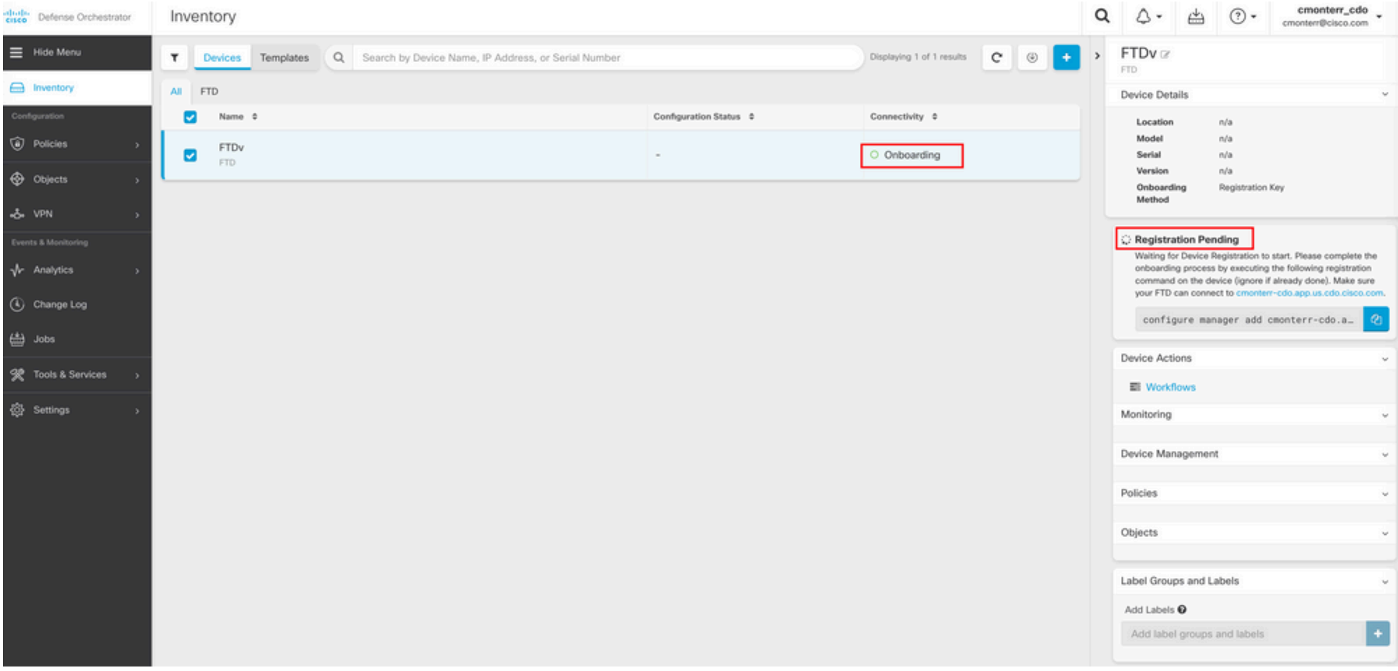


```
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK
qsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.

Manager cmonterr-cdo.app.us.cdo.cisco.com successfully configured.
Please make note of reg_key as this will be required while adding Device in FMC.


>
> show managers
Type                       : Manager
Host                       : cmonterr-cdo.app.us.cdo.cisco.com
Display name               : cmonterr-cdo.app.us.cdo.cisco.com
Identifier                 : 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd
Registration               : Pending
```

cdFMC가 등록 작업을 시작합니다.



Name	Configuration Status	Connectivity
☑ FTDv FTD	-	○ Onboarding

FTDv
FTD

Device Details

Location	n/a
Model	n/a
Serial	n/a
Version	n/a
Onboarding Method	Registration Key

Registration Pending

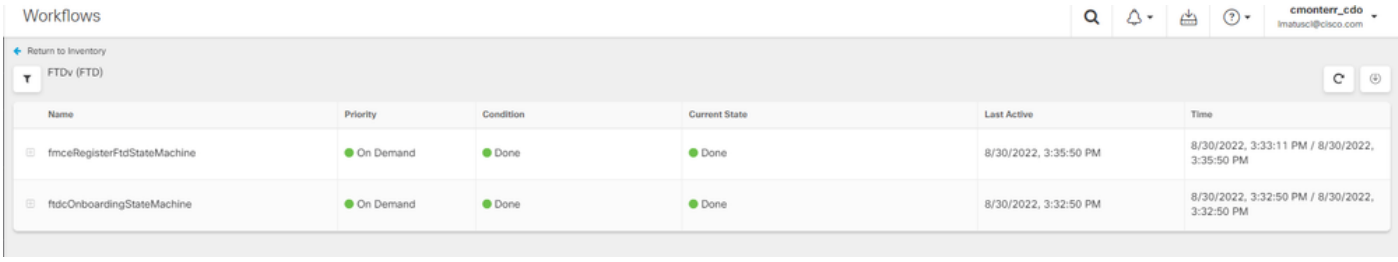
Waiting for Device Registration to start. Please complete the onboarding process by executing the following registration command on the device (ignore if already done). Make sure your FTD can connect to cmonterr-cdo.app.us.cdo.cisco.com.

```
configure manager add cmonterr-cdo.a…
```

참고: 등록 프로세스를 완료하려면 FTD 디바이스가 포트 8305(sftunnel) 및 443을 통해 CDO 테넌트에 연결되어 있는지 확인하십시오. 전체 네트워크 요구 사항을 참조하십시오.

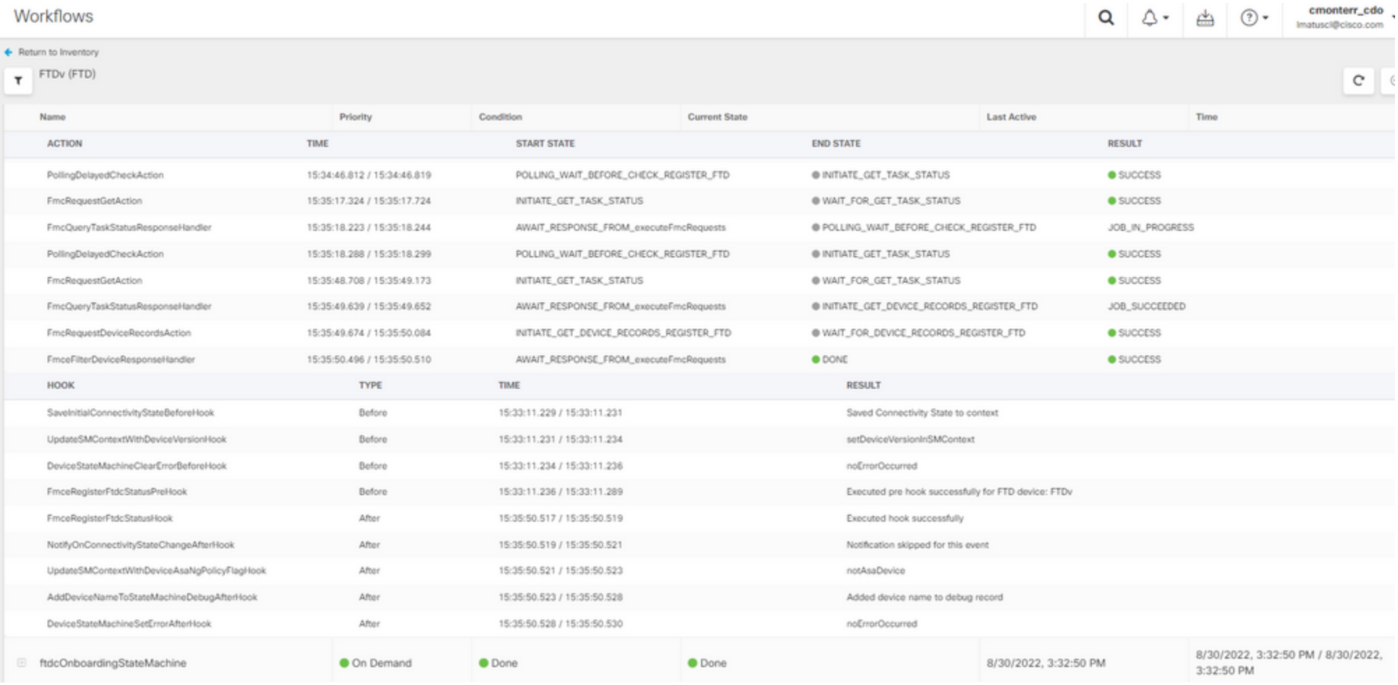
참고: 호스트에 연결할 수 없는 경우 다음 명령을 사용하여 FTD-CLI에서 DNS 컨피그레이션을 수정할 수 있습니다. configure **network dns <address>**.

등록 프로세스를 모니터링하려면 **Device Actions > Workflows..**



Name	Priority	Condition	Current State	Last Active	Time
fmceRegisterFtdStateMachine	● On Demand	● Done	● Done	8/30/2022, 3:35:50 PM	8/30/2022, 3:33:11 PM / 8/30/2022, 3:35:50 PM
ftdcOnboardingStateMachine	● On Demand	● Done	● Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM

를 펼칩니다. **Active** 참고: 이 그림은 FTDv가 성공적으로 등록된 방식을 보여줍니다.

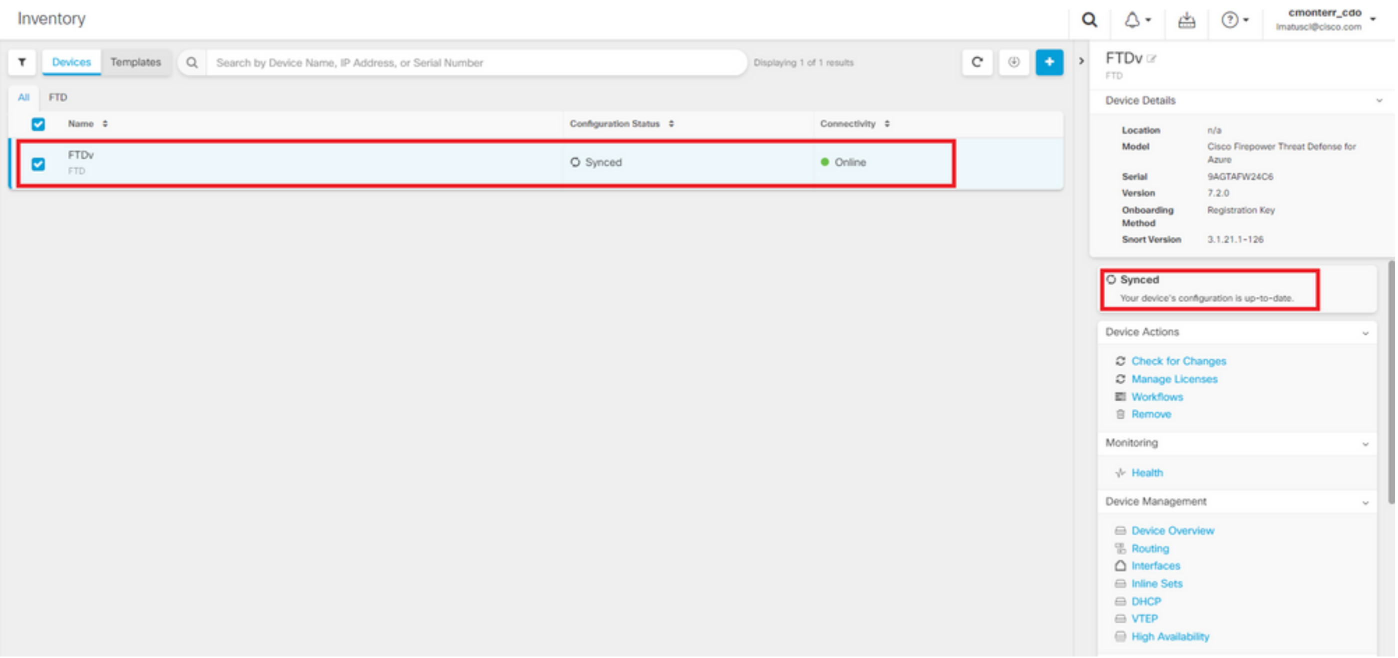


Name	Priority	Condition	Current State	Last Active	Time

ACTION	TIME	START STATE	END STATE	RESULT
PollingDelayedCheckAction	15:34:46.812 / 15:34:46.819	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS
FmcRequestGetAction	15:35:17.324 / 15:35:17.724	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS
FmcQueryTaskStatusResponseHandler	15:35:18.223 / 15:35:18.244	AWAIT_RESPONSE_FROM_executeFmcRequests	● POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	JOB_IN_PROGRESS
PollingDelayedCheckAction	15:35:18.288 / 15:35:18.299	POLLING_WAIT_BEFORE_CHECK_REGISTER_FTD	● INITIATE_GET_TASK_STATUS	● SUCCESS
FmcRequestGetAction	15:35:48.708 / 15:35:49.173	INITIATE_GET_TASK_STATUS	● WAIT_FOR_GET_TASK_STATUS	● SUCCESS
FmcQueryTaskStatusResponseHandler	15:35:49.639 / 15:35:49.652	AWAIT_RESPONSE_FROM_executeFmcRequests	● INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	JOB_SUCCEEDED
FmcRequestDeviceRecordsAction	15:35:49.674 / 15:35:50.084	INITIATE_GET_DEVICE_RECORDS_REGISTER_FTD	● WAIT_FOR_DEVICE_RECORDS_REGISTER_FTD	● SUCCESS
FmceFilterDeviceResponseHandler	15:35:50.496 / 15:35:50.510	AWAIT_RESPONSE_FROM_executeFmcRequests	● DONE	● SUCCESS

HOOK	TYPE	TIME	RESULT
SaveInitialConnectivityStateBeforeHook	Before	15:33:11.229 / 15:33:11.231	Saved Connectivity State to context
UpdateSMContextWithDeviceVersionHook	Before	15:33:11.231 / 15:33:11.234	setDeviceVersionInSMContext
DeviceStateMachineClearErrorBeforeHook	Before	15:33:11.234 / 15:33:11.236	noErrorOccurred
FmceRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FTD device: FTDv
FmceRegisterFtdcStatusHook	After	15:35:50.517 / 15:35:50.519	Executed hook successfully
NotifyOnConnectivityStateChangeAfterHook	After	15:35:50.519 / 15:35:50.521	Notification skipped for this event
UpdateSMContextWithDeviceAsaNgPolicyFlagHook	After	15:35:50.521 / 15:35:50.523	notAsaDevice
AddDeviceNameToStateMachineDebugAfterHook	After	15:35:50.523 / 15:35:50.528	Added device name to debug record
DeviceStateMachineSetErrorAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred

Name	Priority	Condition	Current State	Last Active	Time
ftdcOnboardingStateMachine	● On Demand	● Done	● Done	8/30/2022, 3:32:50 PM	8/30/2022, 3:32:50 PM / 8/30/2022, 3:32:50 PM



Inventory
cmonterr_cdo
lmatuscl@cisco.com
Devices
Templates
Search by Device Name, IP Address, or Serial Number
Displaying 1 of 1 results
All
FTD

Name	Configuration Status	Connectivity
FTDv FTD	○ Synced	● Online

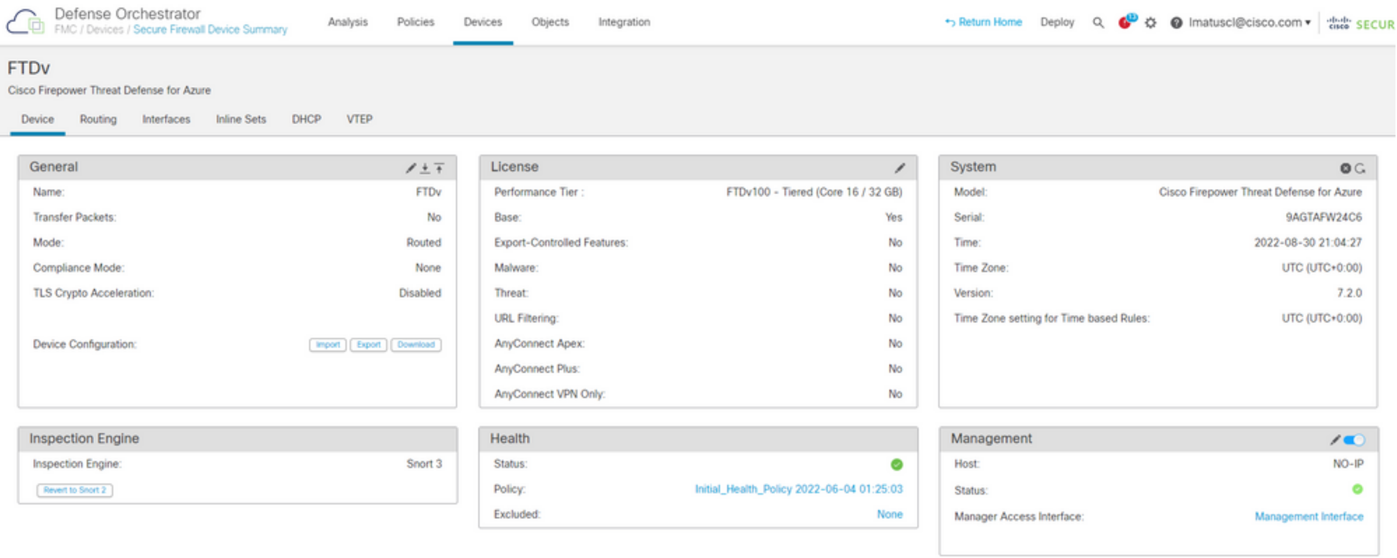
FTDv
FTD

Device Details

Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	9AGTAFW24C6
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	3.1.21.1-126

○ Synced
Your device's configuration is up-to-date.

마지막으로 **Device Management > Device Overview** cdFMC에 액세스하여 FTDv 개요 상태를 검토합니다.



FTDv
Cisco Firepower Threat Defense for Azure

General

Name:	FTDv
Transfer Packets:	No
Mode:	Routed
Compliance Mode:	None
TLS Crypto Acceleration:	Disabled
Device Configuration:	Import Export Download

License

Performance Tier :	FTDv100 - Tiered (Core 16 / 32 GB)
Base:	Yes
Export-Controlled Features:	No
Malware:	No
Threat:	No
URL Filtering:	No
AnyConnect Apex:	No
AnyConnect Plus:	No
AnyConnect VPN Only:	No

System

Model:	Cisco Firepower Threat Defense for Azure
Serial:	9AGTAFW24C6
Time:	2022-08-30 21:04:27
Time Zone:	UTC (UTC+0:00)
Version:	7.2.0
Time Zone setting for Time based Rules:	UTC (UTC+0:00)

Inspection Engine

Inspection Engine:	Snort 3

Revert to Snort 2

Health

Status:	●
Policy:	Initial_Health_Policy 2022-06-04 01:25:03
Excluded:	None

Management

Host:	NO-IP
Status:	●
Manager Access Interface:	Management Interface

관련 정보

- 기술 지원 및 문서 – Cisco Systems
- 클라우드 기반 방화벽 관리 센터를 통해 Cisco Secure Firewall Threat Defense 디바이스 관리

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.