Deploy a Cloud-Delivered FMC (cdFMC) in Cisco Defense Orchestrator (CDO)

Contents

Introduction

This document describes the deployment and onboard process of Cloud-Delivered FMC on the CDO platform.

Prerequisites

Requirements

Cisco recommends knowledge of these topics:

- Cloud-Delivered Firepower Management Center (cdFMC)
- Cisco Defense Orchestrator (CDO)
- Firepower Threat Defense Virtual (FTDv)

Minimum FTD version 7.0.3

Components Used

The information in this document is based on these software and hardware versions:

- cdFMC
- FTDv 7.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco Defense Orchestrator (CDO) is the platform for the cloud-delivered Firewall Management Center (cdFMC). 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 Secure Firewall Threat Defense. It has the same appearance and behavior as an on-premises Secure Firewall Management Center and uses the same FMC Application Programming Interface (API).

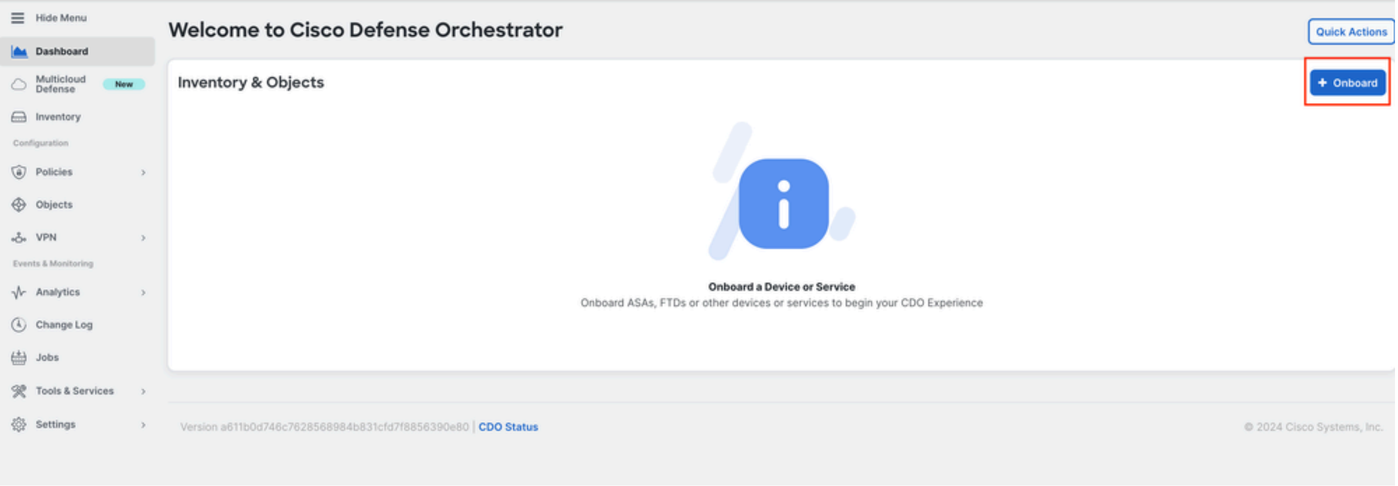
This product is designed for migration from the on-premises Secure Firewall Management Centers to the Secure Firewall Management Center SaaS version.

Configure

Deploy a Cloud-Delivered Firepower Management Center on CDO.

These pictures show the initial setup process needed to deploy a cloud-delivered FMC on CDO.

From the CDO menu, navigate to **Tools & Services** > **Firewall Management Center** > **Onboard**.



Welcome to Cisco Defense Orchestrator

Inventory & Objects

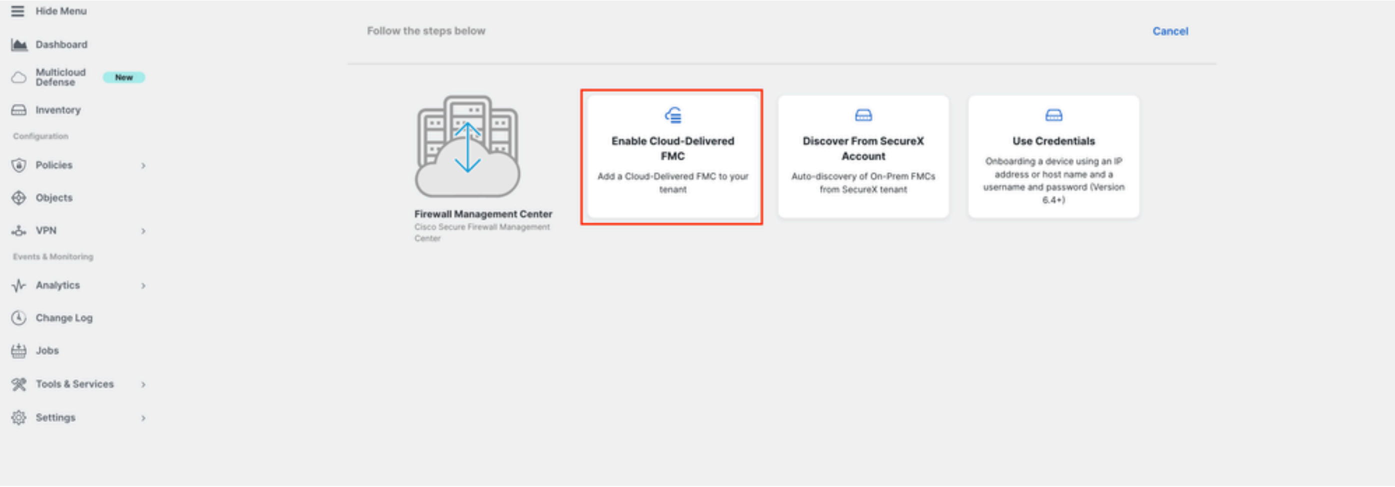
Onboard a Device or Service

Onboard ASAs, FTDs or other devices or services to begin your CDO Experience

Version a611b0d746c7628568984b831cfd7f8856390e80 | CDO Status

© 2024 Cisco Systems, Inc.

Select Enable Cloud-Delivered FMC.



Follow the steps below

Firewall Management Center

Cisco Secure Firewall Management Center

Enable Cloud-Delivered FMC

Add a Cloud-Delivered FMC to your tenant

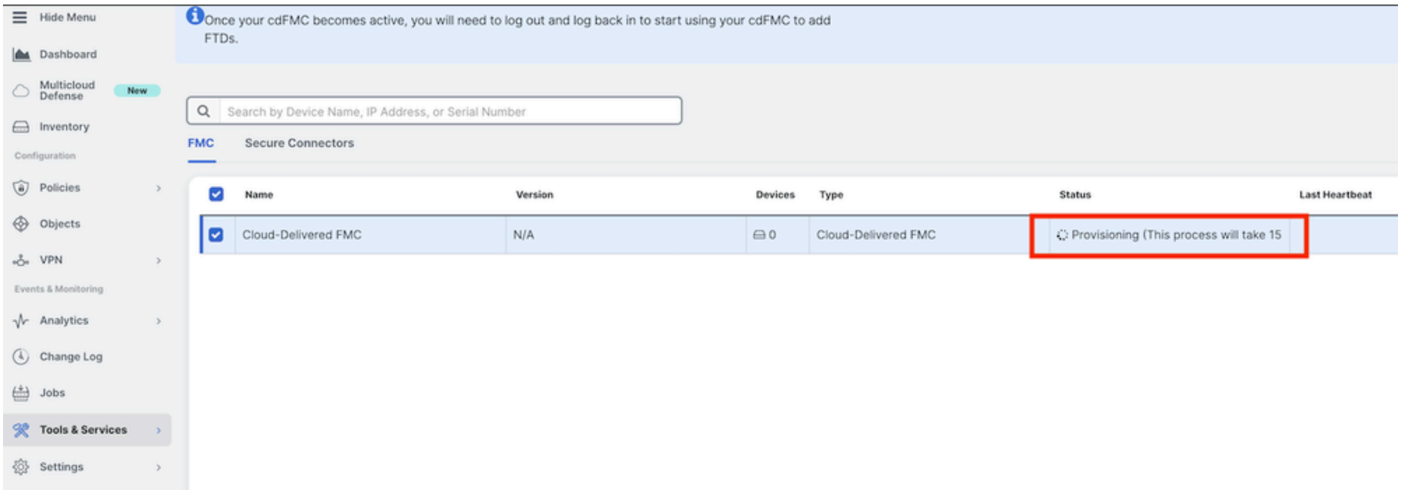
Discover From SecureX Account

Auto-discovery of On-Prem FMCs from SecureX tenant

Use Credentials

Onboarding a device using an IP address or host name and a username and password (Version 6.4+)

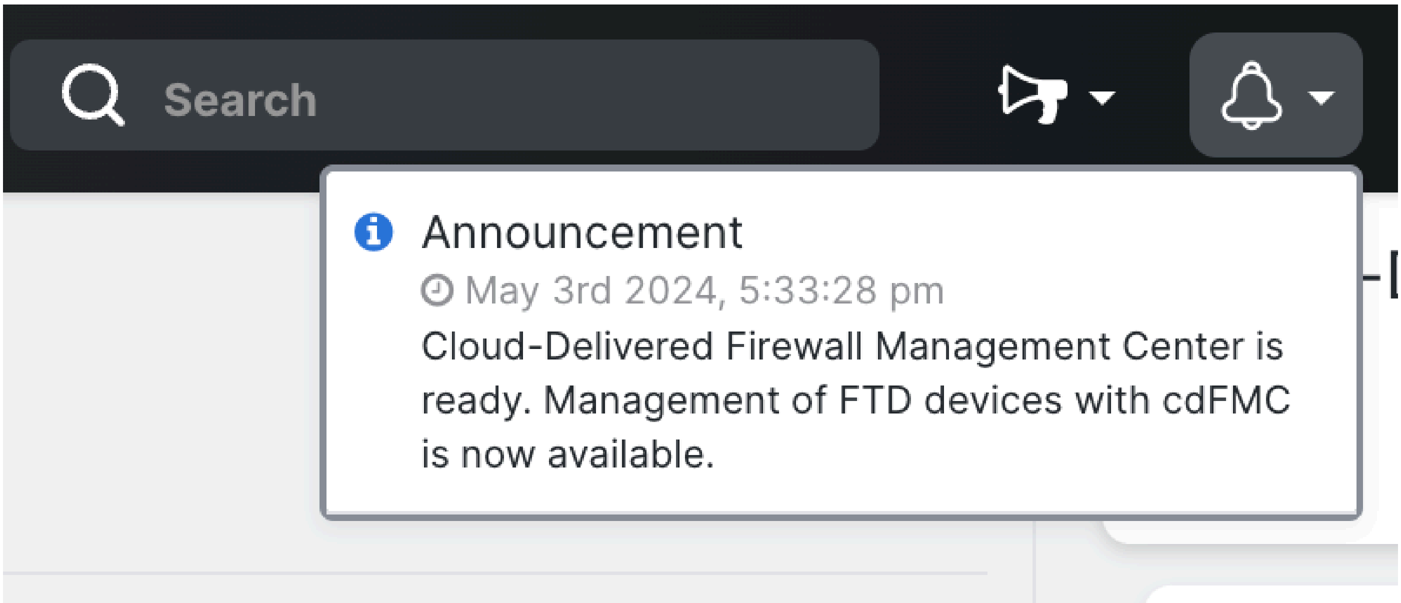
CDO privisions a cloud-delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the Status column of Cloud-Delivered FMC.



Once your cdFMC becomes active, you will need to log out and log back in to start using your cdFMC to add FTDs.

☑	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	N/A	0	Cloud-Delivered FMC	Provisioning (This process will take 15	

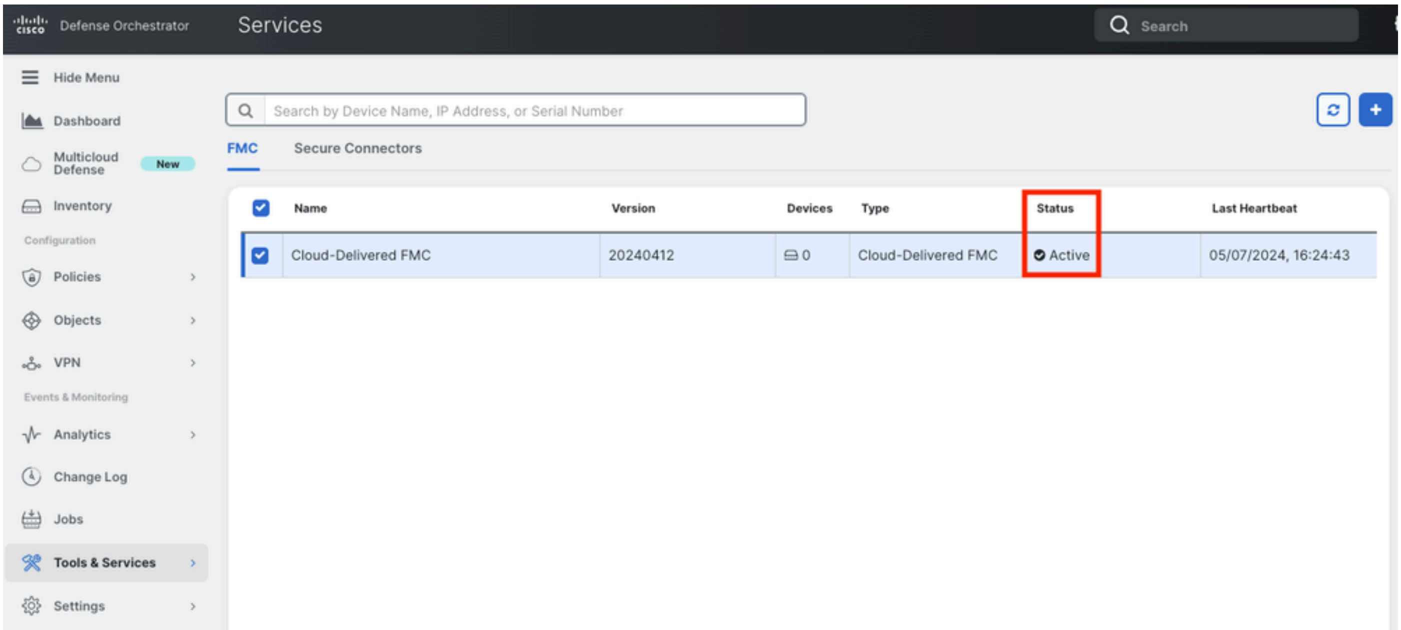
After the provisioning is complete, the status changes to Active. In addition, you get a Cloud-delivered Firewall Management Center is Ready notification on the CDO notifications panel.



Announcement

May 3rd 2024, 5:33:28 pm

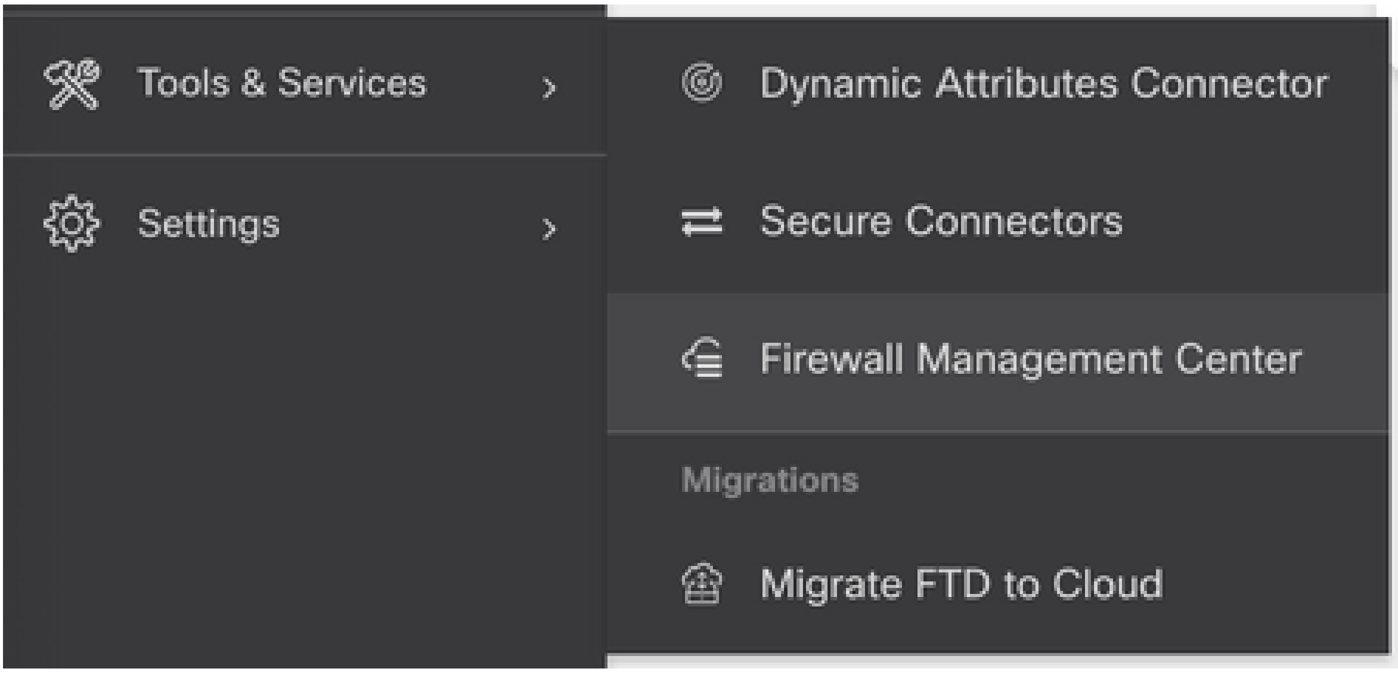
Cloud-Delivered Firewall Management Center is ready. Management of FTD devices with cdFMC is now available.



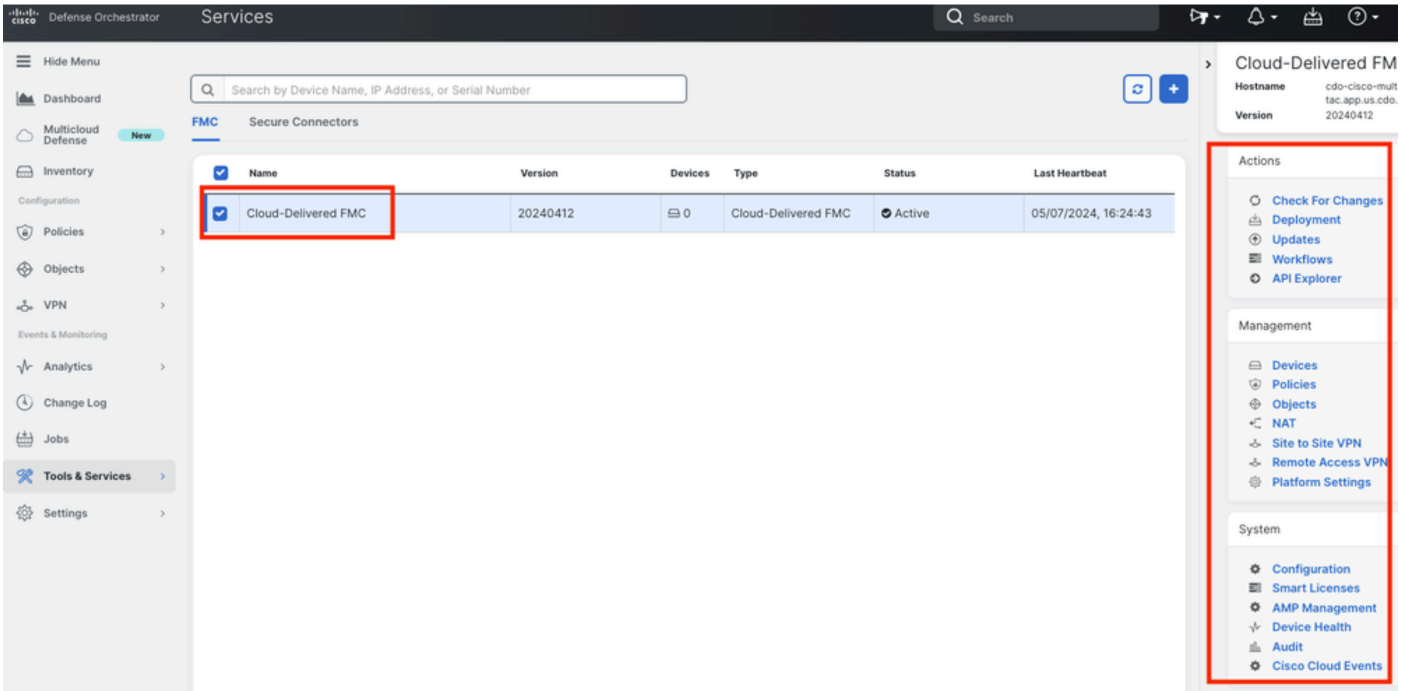
☑	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	Active	05/07/2024, 16:24:43

You can then onboard your threat defense devices to the cloud-delivered Firewall Management Center and manage them.

Navigate to **Menu** > **Tools & Services** > **Firewall Management Center**.



Select your cdFMC to display the cdFMC information and, in order to access the Graphical User Interface (GUI) of the cdFMC, select any of the options available on the right side.



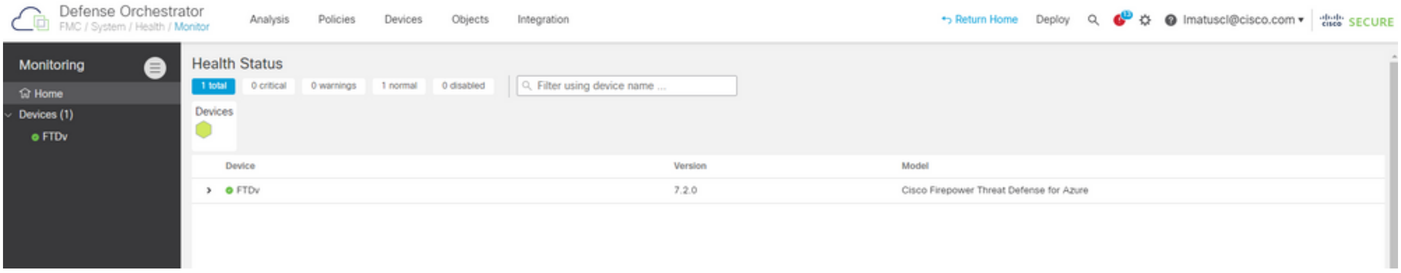
☑	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	Active	05/07/2024, 16:24:43

Cloud-Delivered FM

Hostname cdo-cisco-mult tac.app.us.cdo.

Version 20240412

Now you can see the cdFMC GUI.



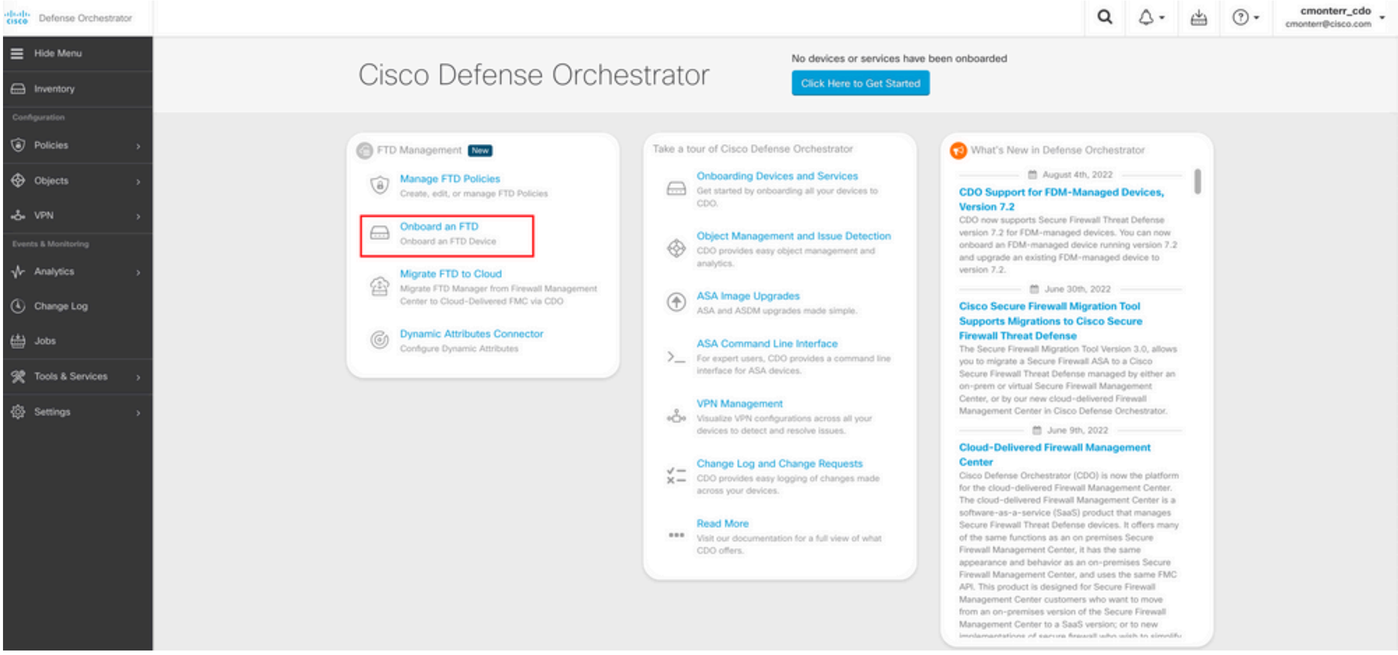
Health Status

Device	Version	Model
FTDv	7.2.0	Cisco Firepower Threat Defense for Azure

Onboard an FTD on a Cloud-Delivered FMC

These images show how to onboard an FTD in order to be registered on a cdFMC with Command Line Interface (CLI) registration key.

First, select **Onboard an FTD** on the CDO home page.



Cisco Defense Orchestrator

No devices or services have been onboarded

FTD Management New

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

Take a tour of Cisco Defense Orchestrator

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.

What's New in Defense Orchestrator

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.

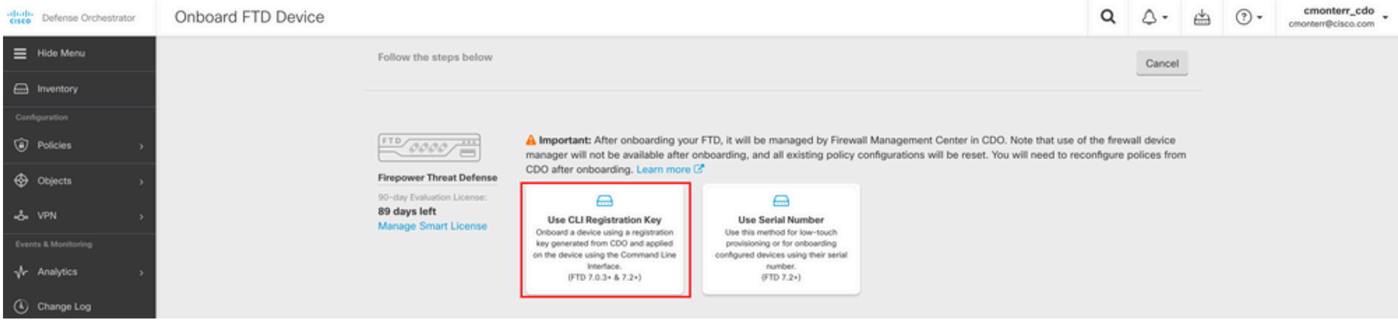
June 30th, 2022

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

Then, select the **Use CLI Registration Key** option.



Onboard FTD Device

Follow the steps below

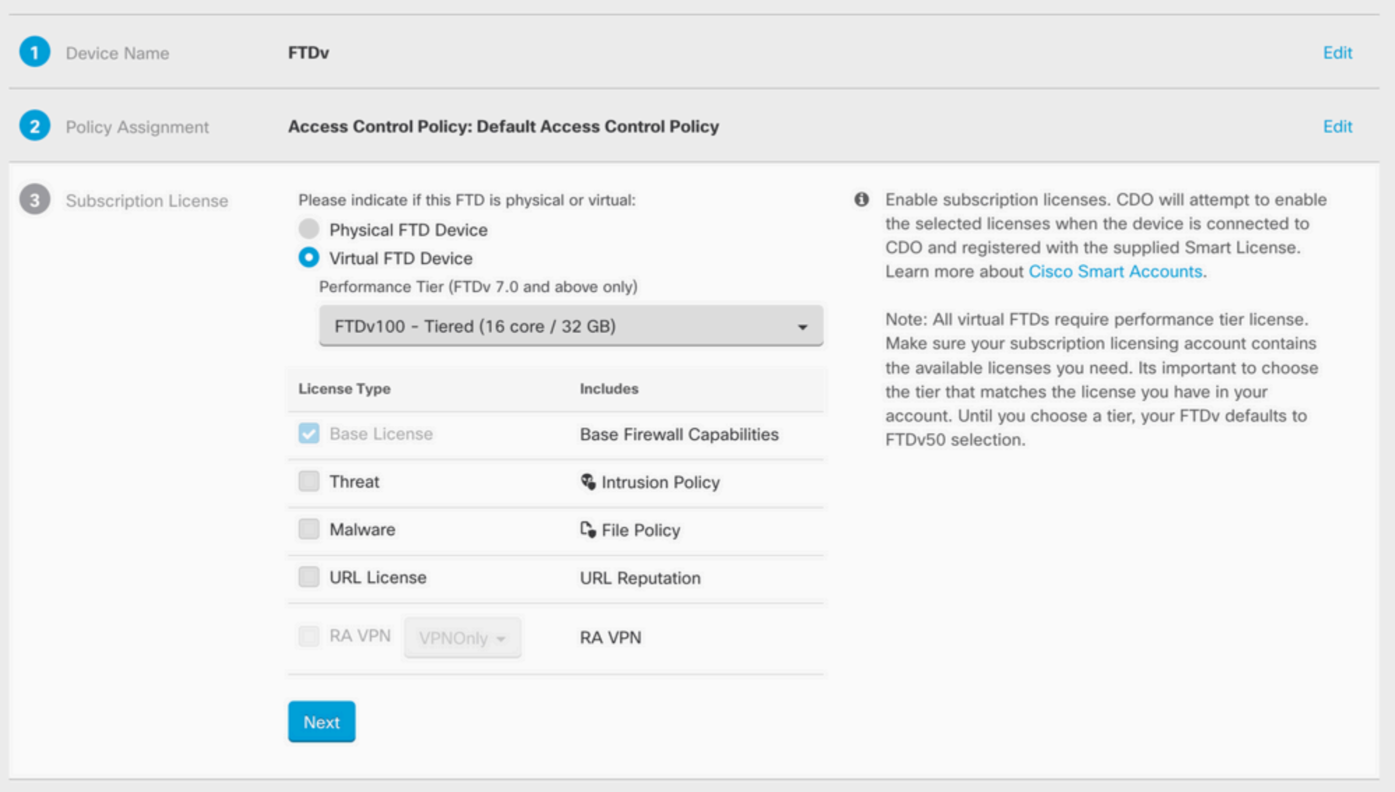
Firepower Threat Defense
90-day Evaluation License:
89 days left
Manage Smart License

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+)

Proceed to enter the requested and desired FTDv information.



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)

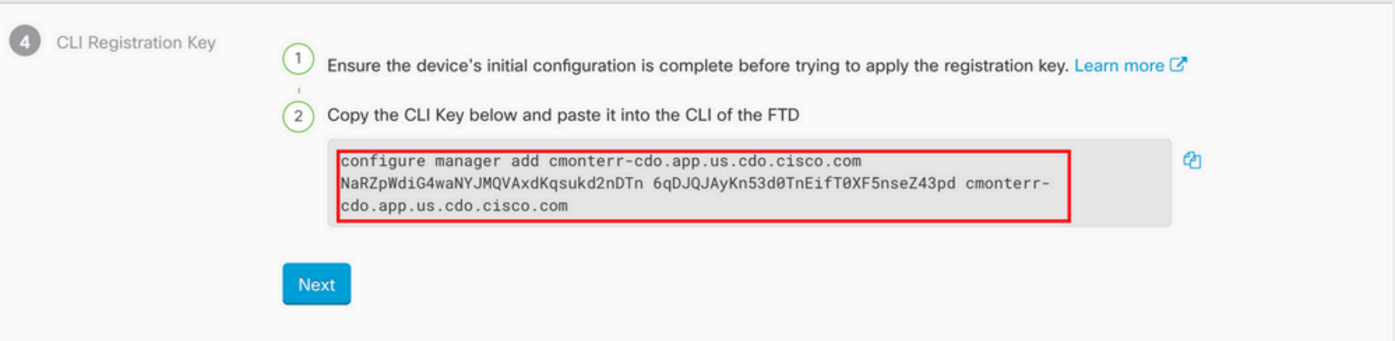
License Type	Includes
☑ Base License	Base Firewall Capabilities
□ Threat	Intrusion Policy
□ Malware	File Policy
□ URL License	URL Reputation
□ RA VPN VPNOnly	RA VPN

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.

Finally, the cdFMC creates a specific **CLI Key**for your device.



4 CLI Registration Key

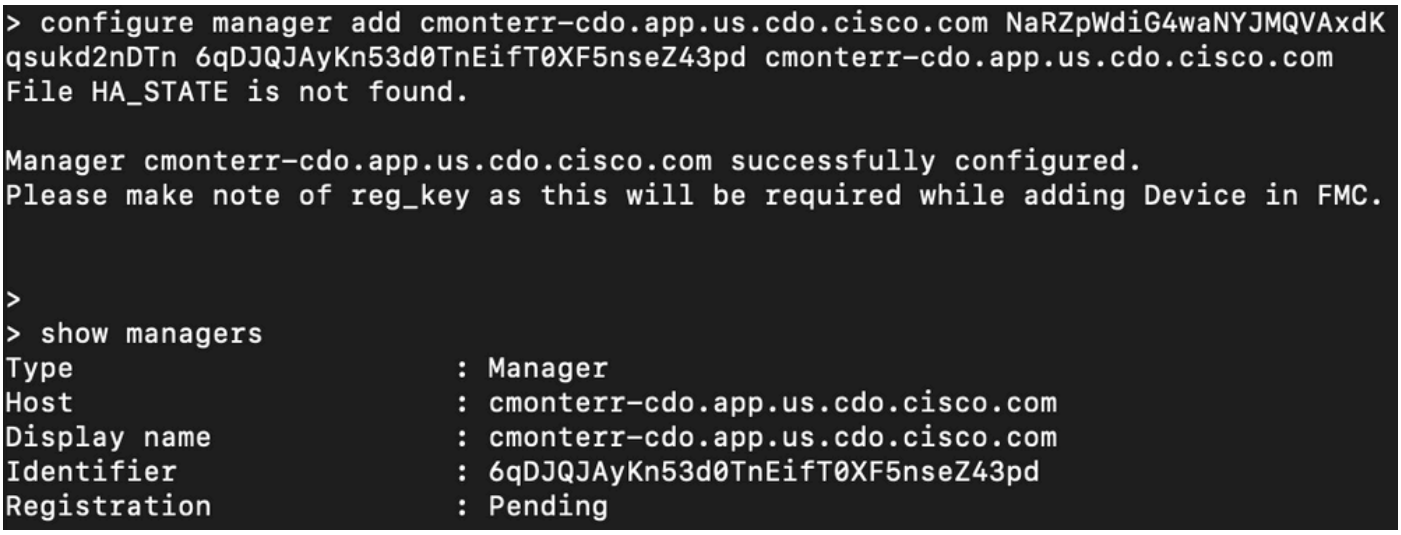
1 Ensure the device's initial configuration is complete before trying to apply the registration key. Learn more

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

Copy the **CLI Key** into the CLI of your managed device.

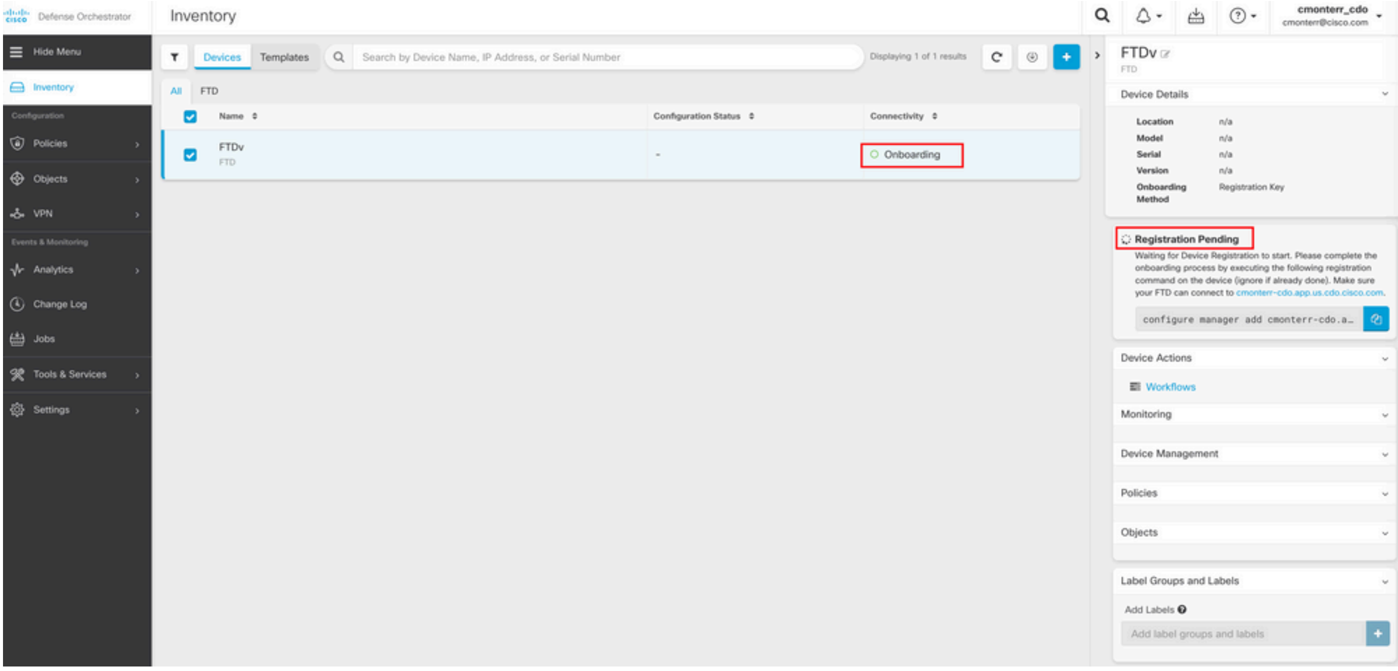


```
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK
qsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.

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
```

The cdFMC initiates a registration task.



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

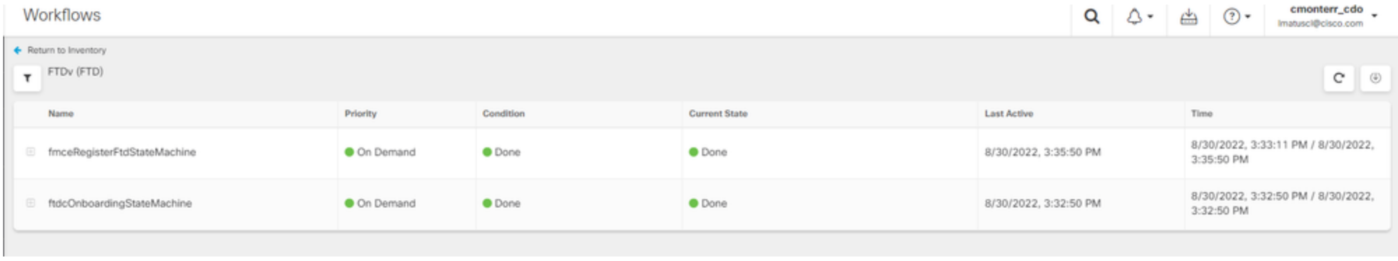
Waiting for Device Registration to start. Please complete the onboarding process by executing the following registration command on the device (ignore if already done). Make sure your FTD can connect to cmonterr-cdo.app.us.cdo.cisco.com.

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

Note: Make sure your FTD device has communication over ports 8305 (sftunnel) and 443 to the CDO tenant in order to complete the registration process. Consult the full Network Requirements.

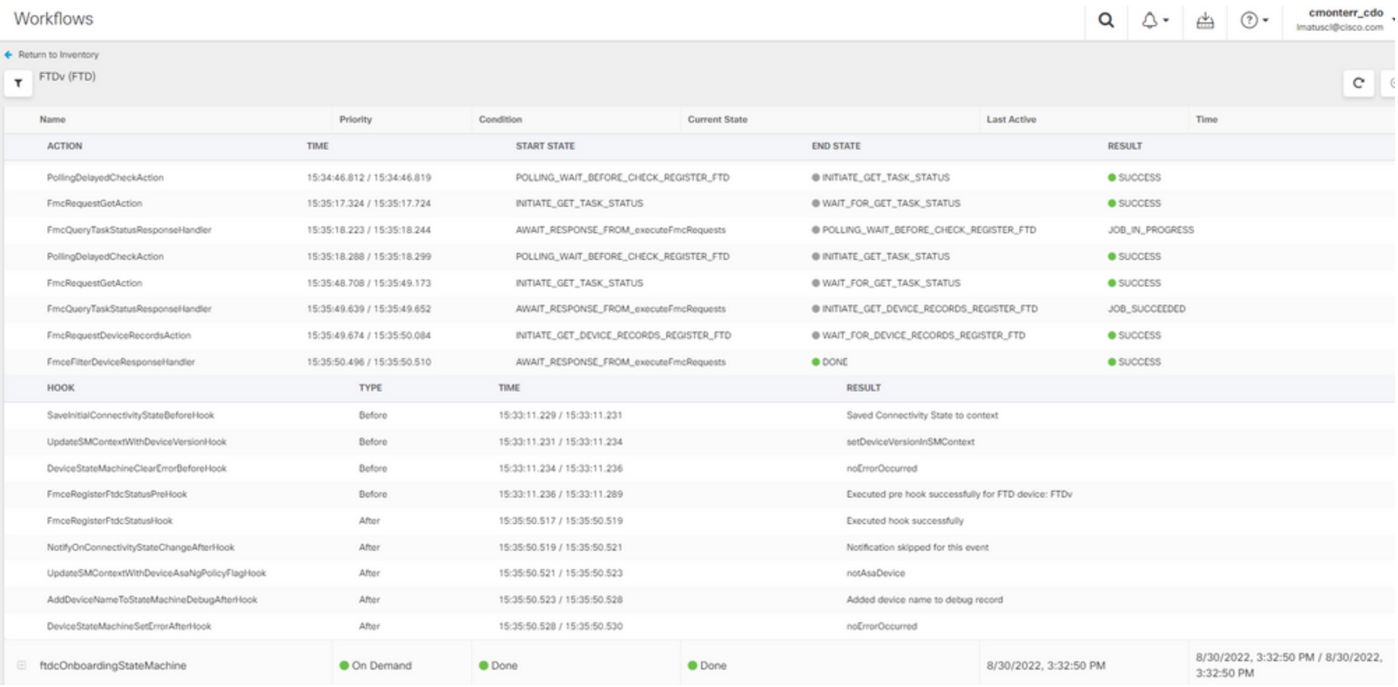
Note: If you can not connect to the host, you can rectify the DNS configuration in the FTD-CLI with this command: **configure network dns <address>**.

To monitor the registration process, navigate to **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

Expand the **Active** state to have additional information, these pictures show how the FTDv was successfully registered.



Workflows

cmonterr_cdo
lmatuscl@cisco.com

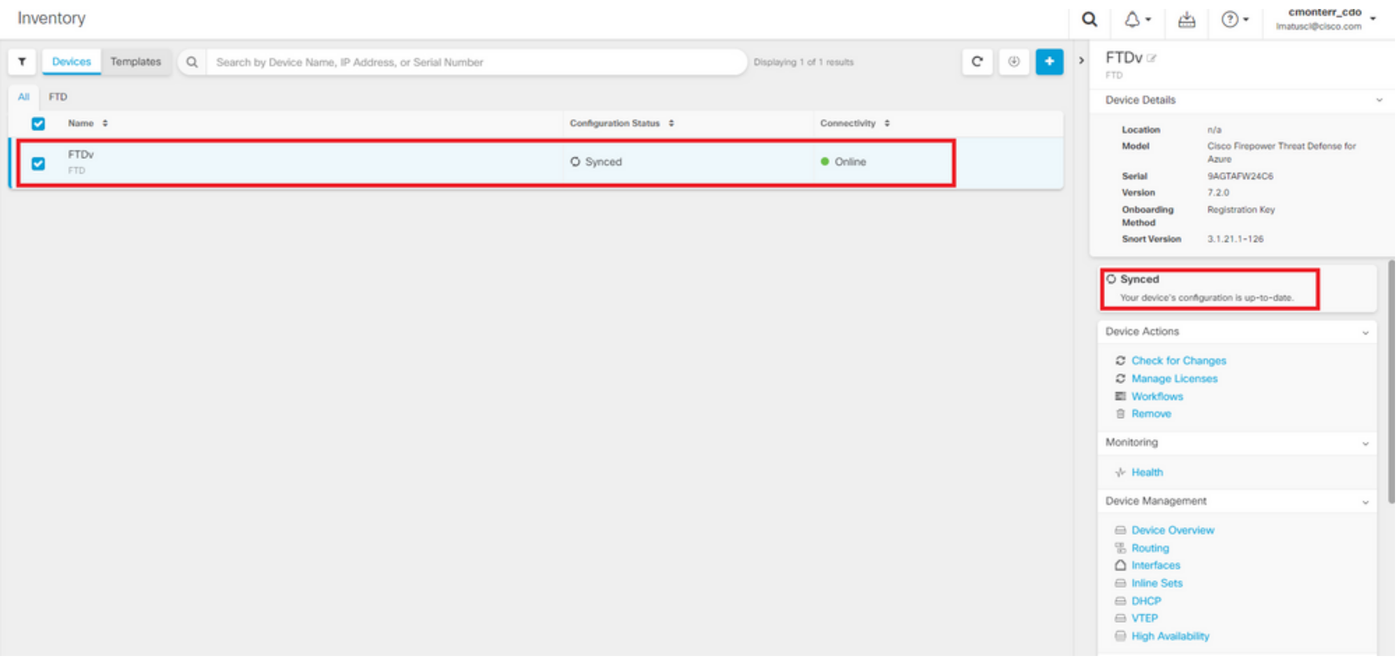
Return to Inventory

FTDv (FTD)

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

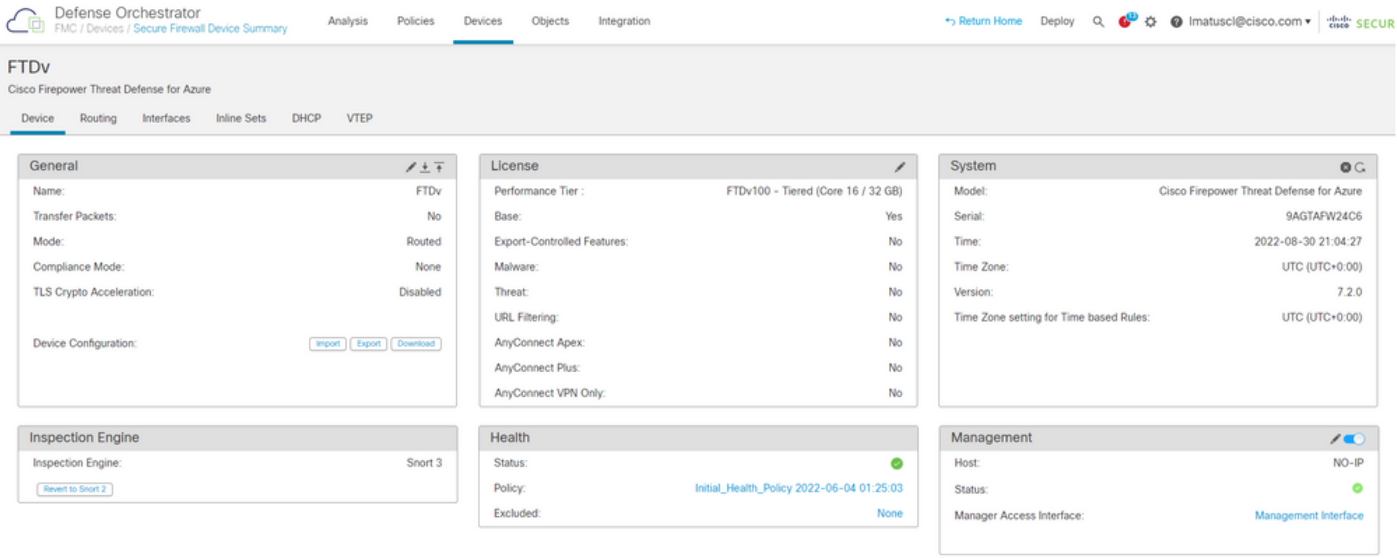
FTDv
FTD

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.

Finally, Navigate to **Device Management** > **Device Overview** in order to access the cdFMC and review the FTDv overview status.



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

Health

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

Management

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

Related Information

- [Technical Support & Documentation - Cisco Systems]
- [Manage Cisco Secure Firewall Threat Defense Devices with Cloud-Delivered Firewall Management Center]