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

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

Configure

- Deploy a Cloud-Delivered Firepower Management Center on CDO.
- Onboard an FTD on a Cloud-Delivered FMC

Related Information

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).

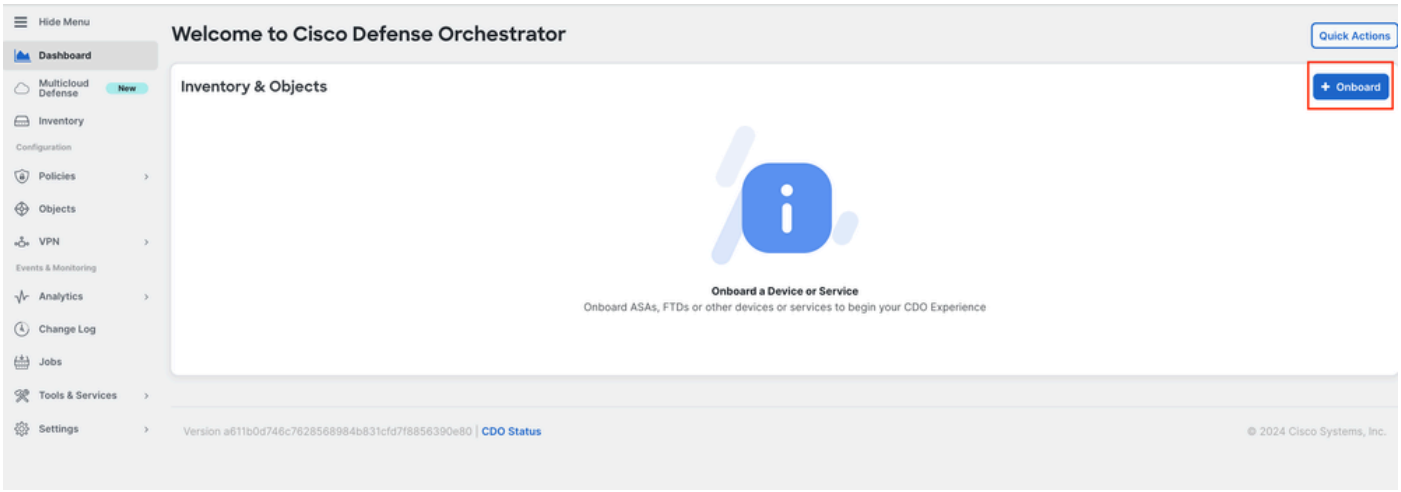
This product is designed for migration from the on-premises Secure Firewall Management Centers to the Secure Firewall Management Center SaaS version.

Configure

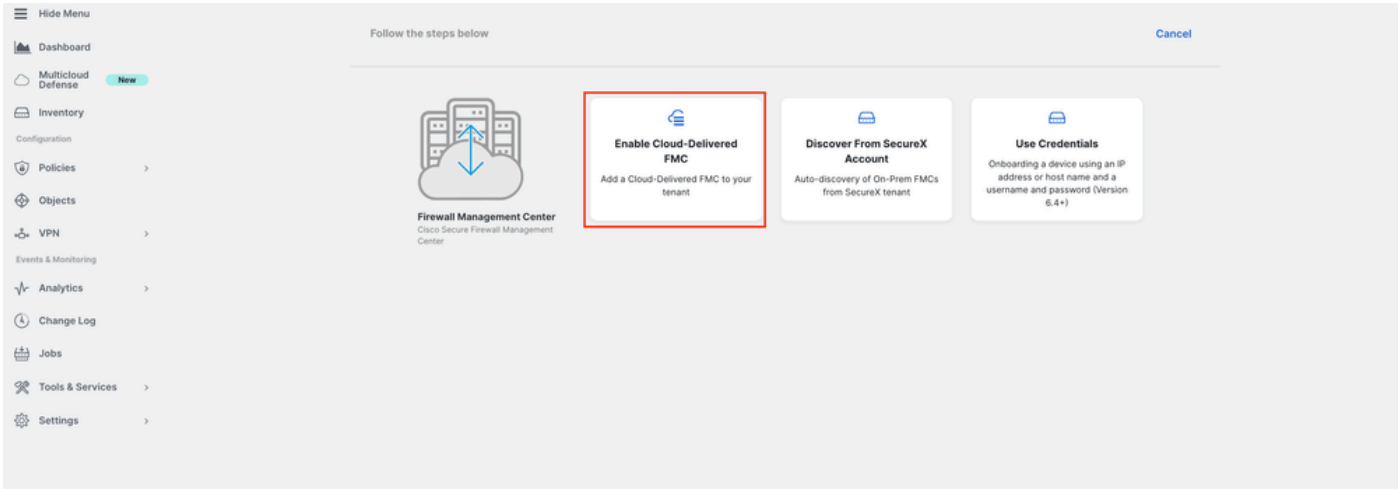
Deploy a Cloud-Delivered Firepower Management Center on CDO.

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

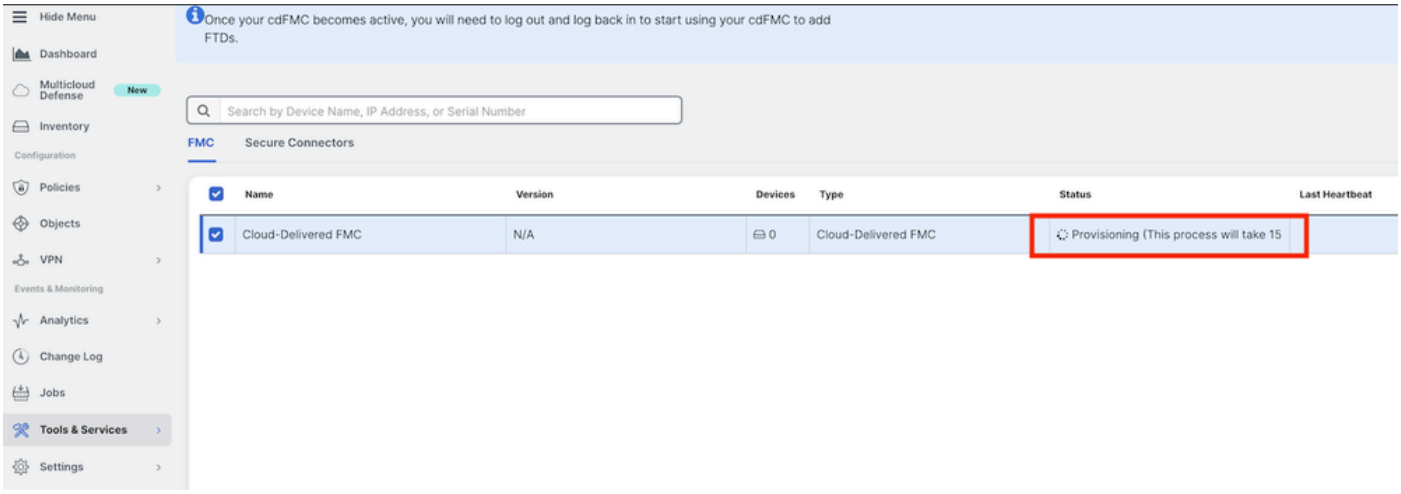
From the CDO menu, navigate to **Tools & Services > Firewall Management Center > Onboard**.



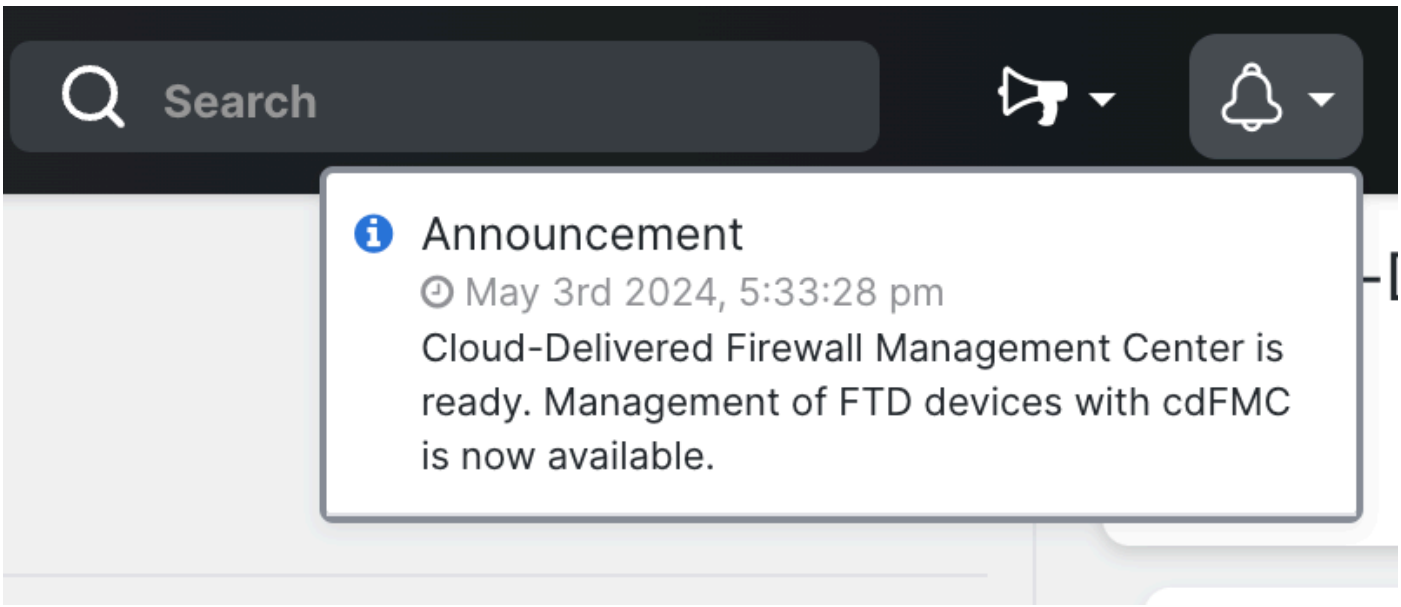
Select Enable Cloud-Delivered FMC.

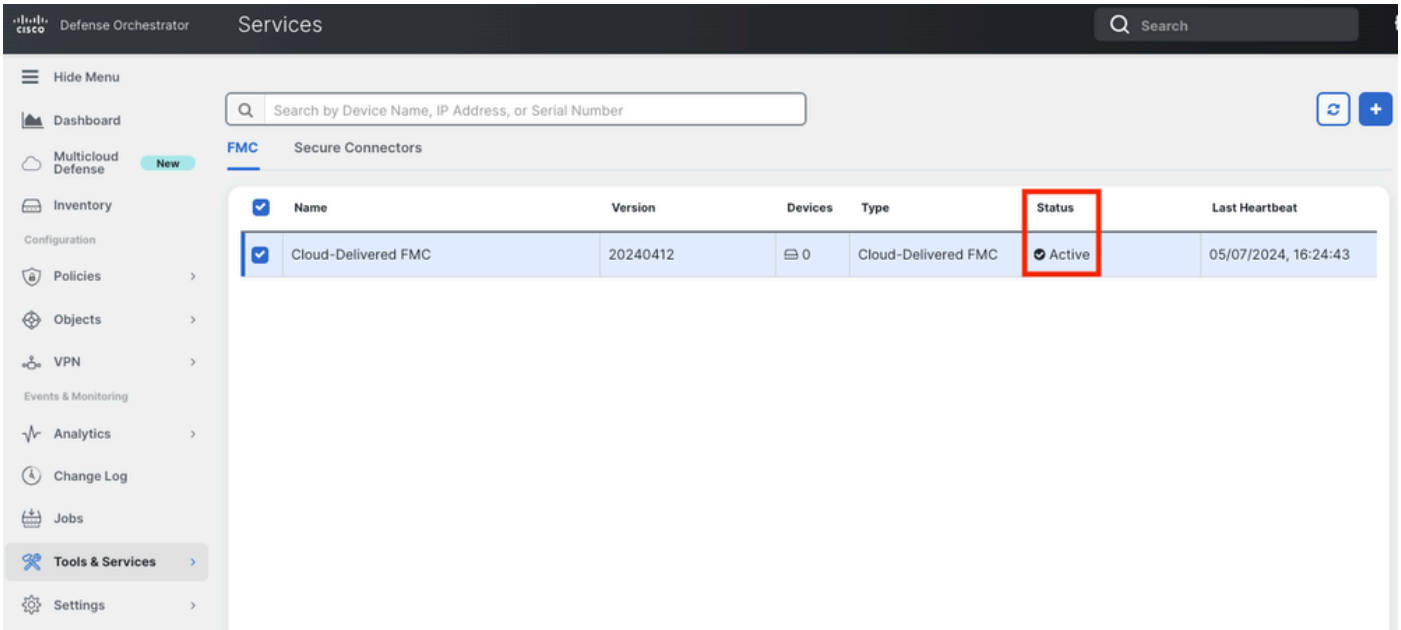


CDO privisions a cloud-delivered Firewall Management Center instance in the background; it typically takes 15 to 30 minutes for this to be complete. You can track the provisioning progress on the Status column of Cloud-Delivered FMC.



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.

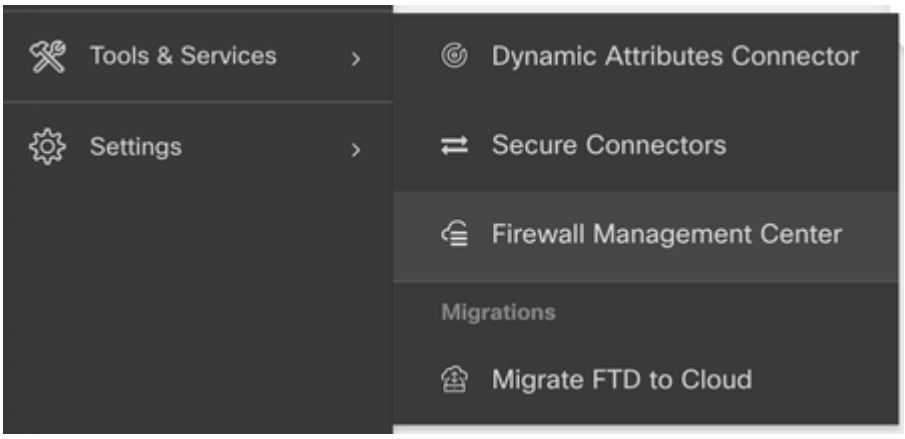




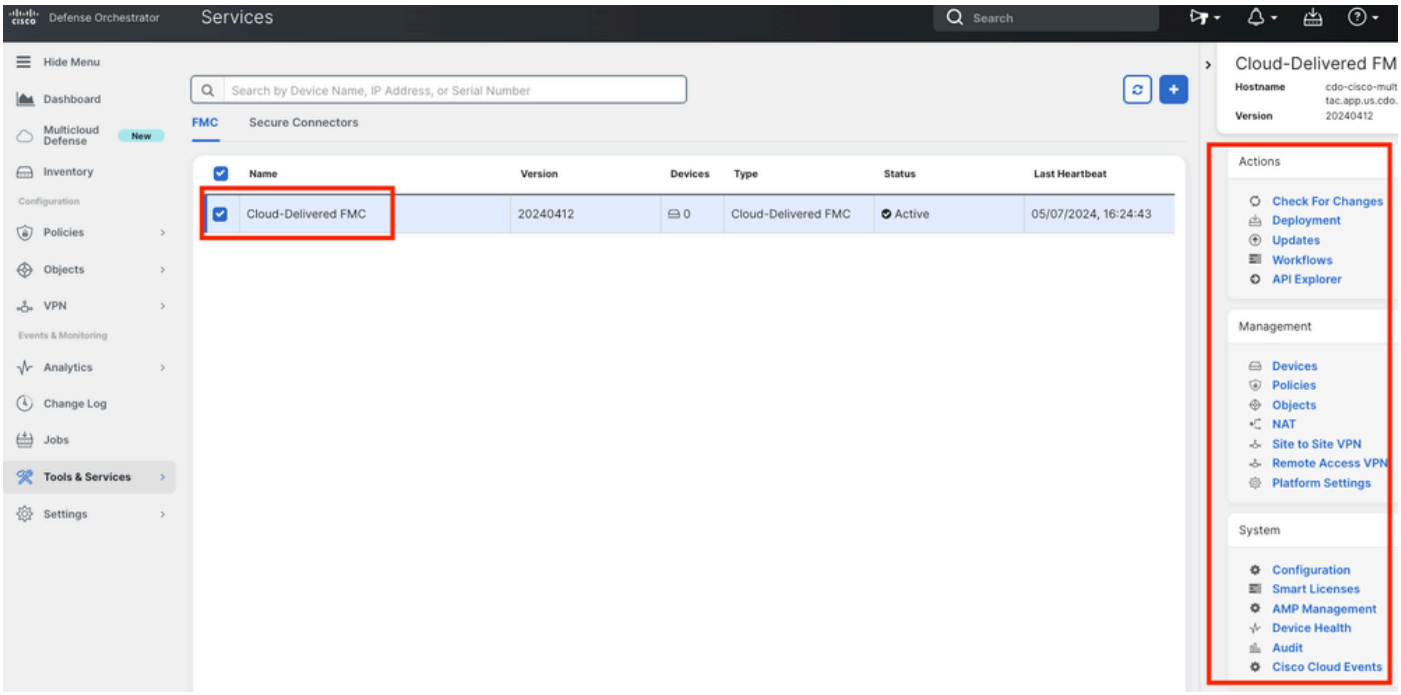
You can then onboard your threat defense devices to the cloud-delivered Firewall Management Center and

manage them.

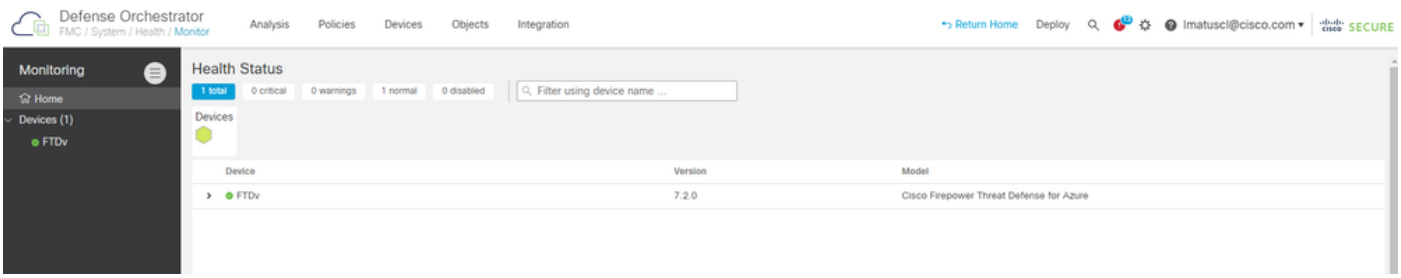
Navigate to **Menu > Tools & Services > Firewall Management Center.**



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.



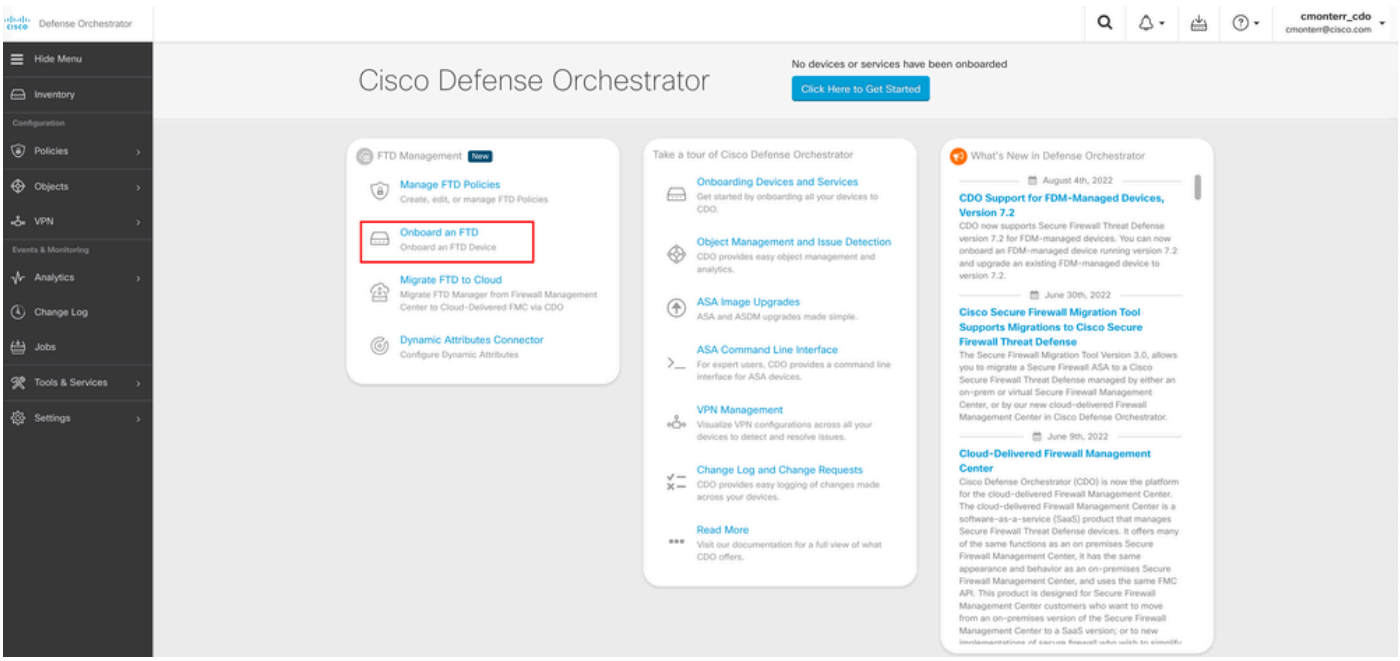
Now you can see the cdFMC GUI.



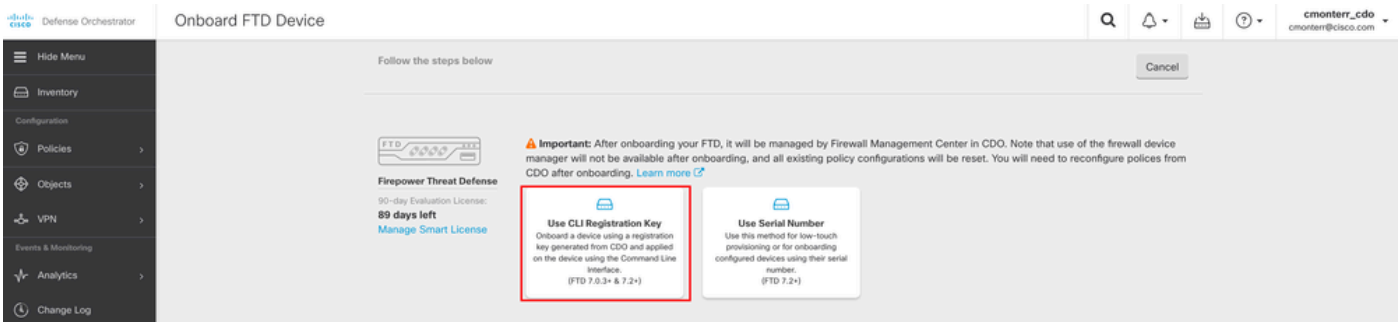
Onboard an FTD on a Cloud-Delivered FMC

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

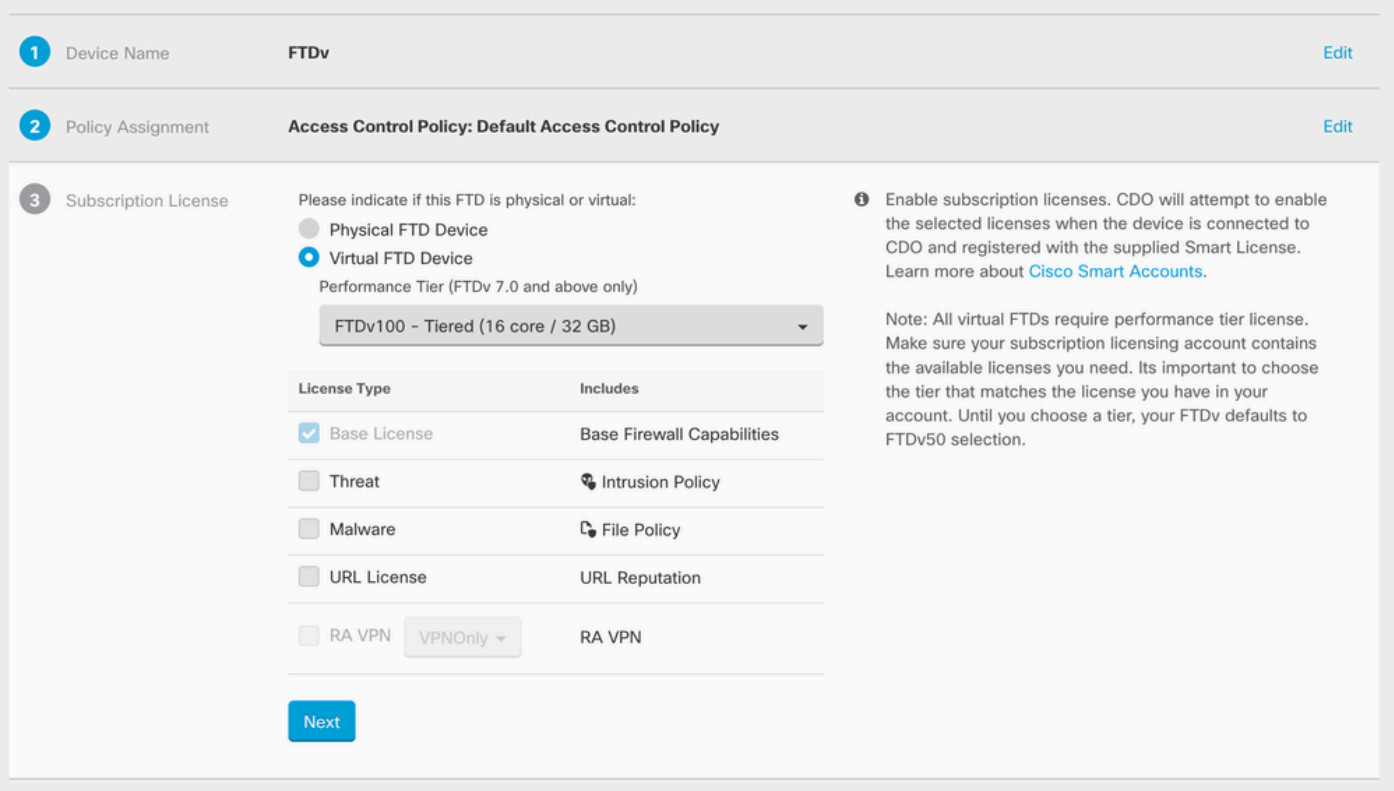
First, select **Onboard an FTD** on the CDO home page.



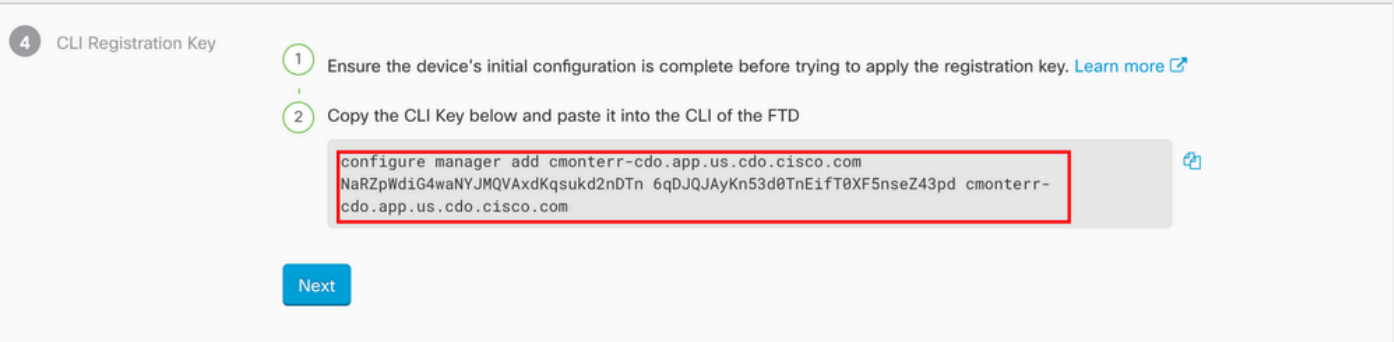
Then, select the **Use CLI Registration Key** option.



Proceed to enter the requested and desired FTDv information.



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



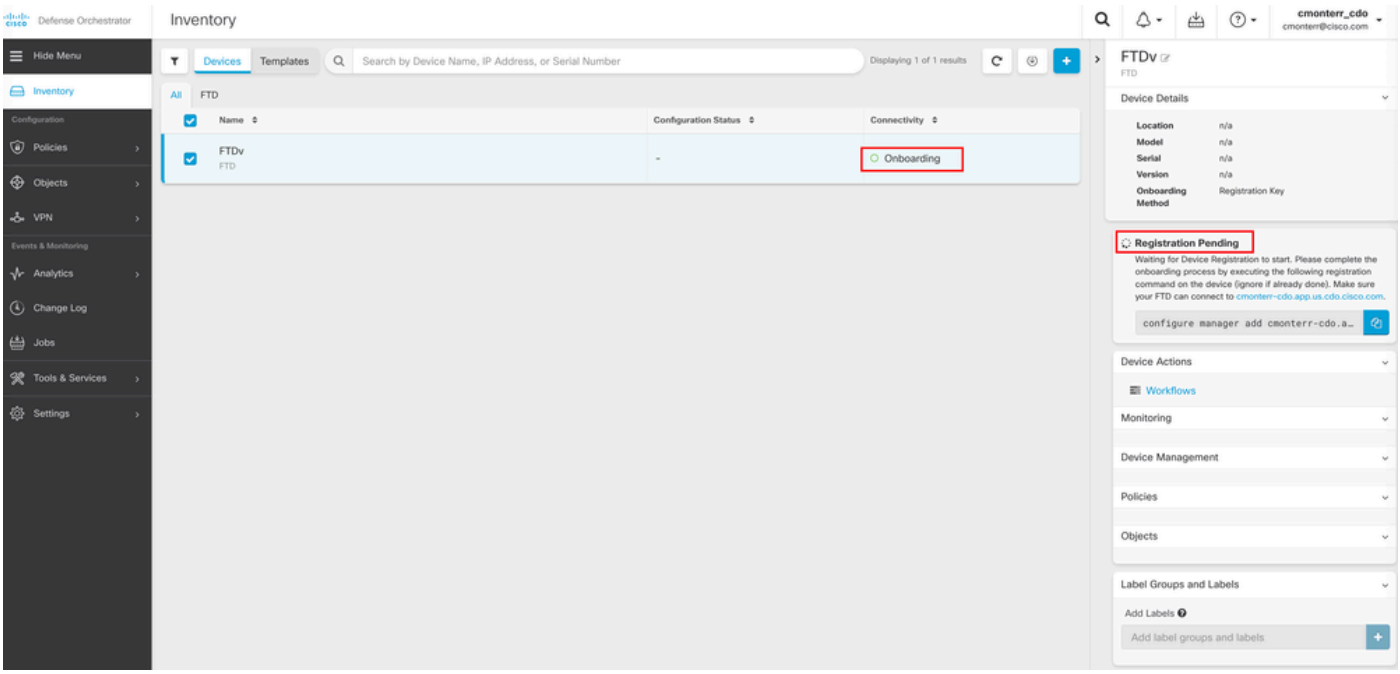
Copy the **CLI Key** into the CLI of your managed device.

```
> 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
```

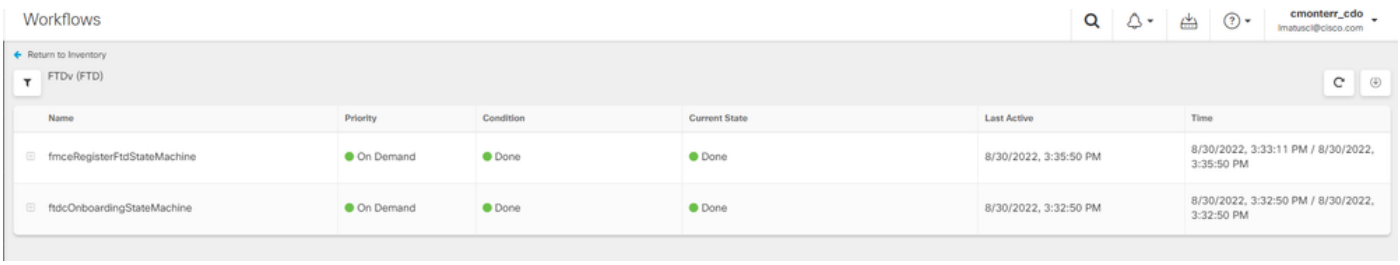
The cdFMC initiates a registration task.



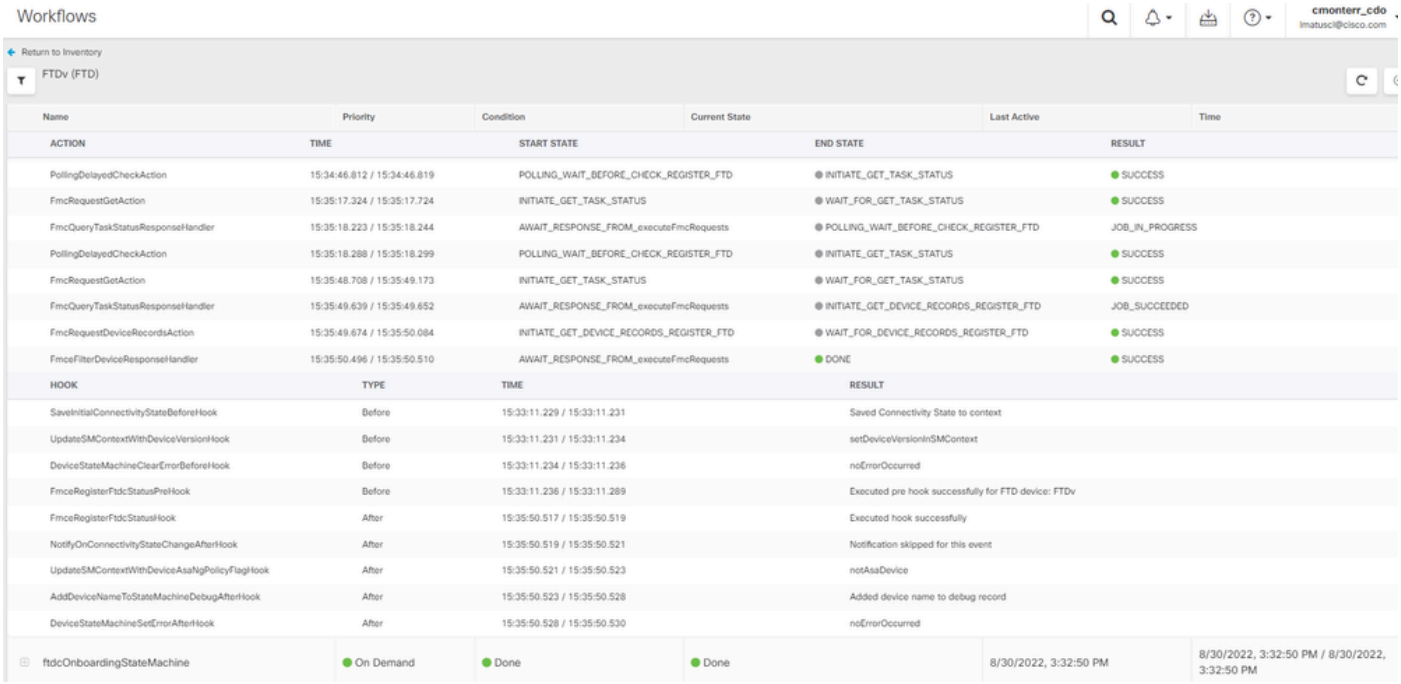
Note: Make sure your FTD device has communication over ports 8305 (sftunnel) and 443 to the CDO tenant in order to complete the registration process. Consult the full Network Requirements.

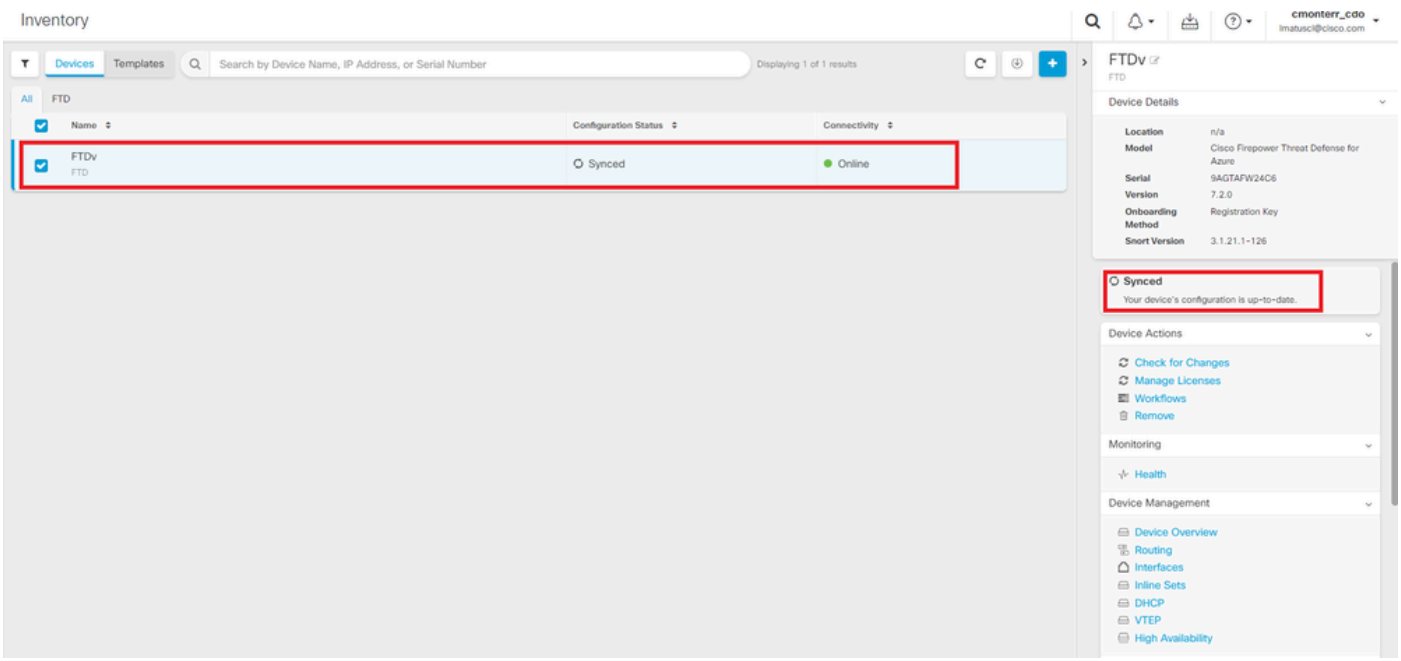
Note: If you can not connect to the host, you can rectify the DNS configuration in the FTD-CLI with this command: **configure network dns <address>**.

To monitor the registration process, navigate to **Device Actions > Workflows..**

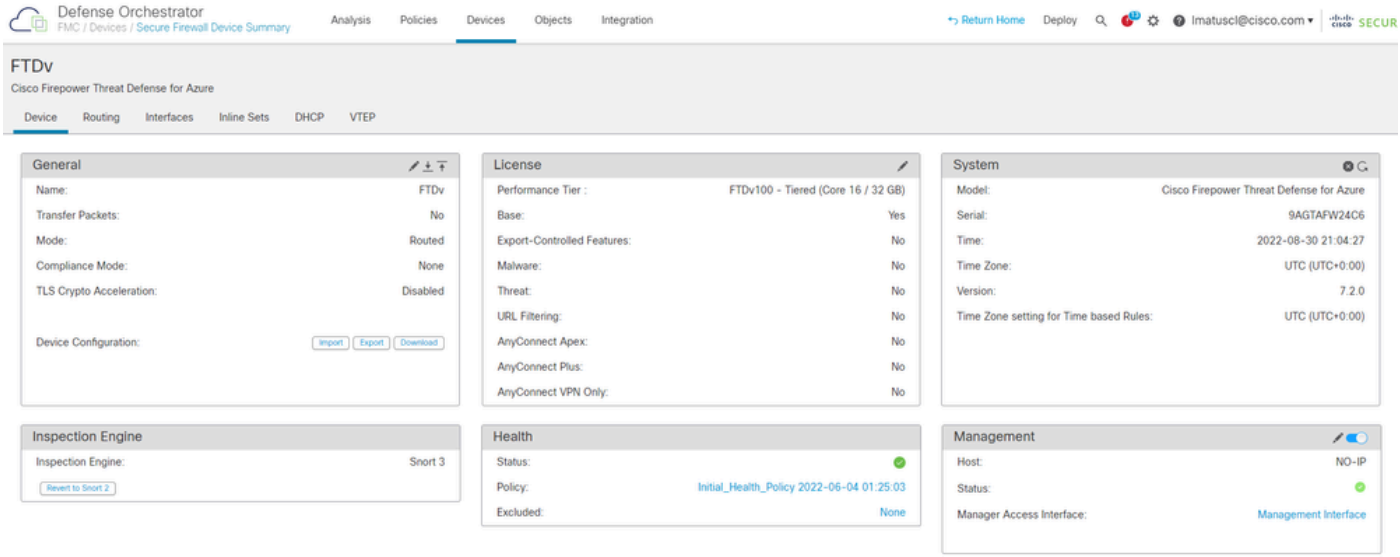


Expand the **Active** state to have additional information, these pictures show how the FTDv was successfully registered.





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



Related Information

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