Een cloudbeheerd FMC (cdFMC) implementeren in Cisco Defense Orchestrator (CDO)

Inhoud

Inleiding

In dit document worden de implementatie en het boordproces van Cloud-Delivery FMC op het CDO-platform beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van deze onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- cdFMC 7.2.0
- FTDv 7.2.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Cisco Defense Orchestrator (CDO) is het platform voor het door de cloud geleverde Firewall

Management Center (cdFMC). Het door de cloud geleverde Firewall Management Center is een software-as-a-service (SaaS) product dat Secure Firewall Threat Defence devices beheert. Het biedt veel van de zelfde functies zoals een op-gebouw Veilig Firewall Veilige Verdediging van de Dreiging van de Firewall. Het heeft dezelfde uitstraling en hetzelfde gedrag als een Secure Firewall Management Center op locatie en gebruikt dezelfde FMC Application Programming Interface (API).

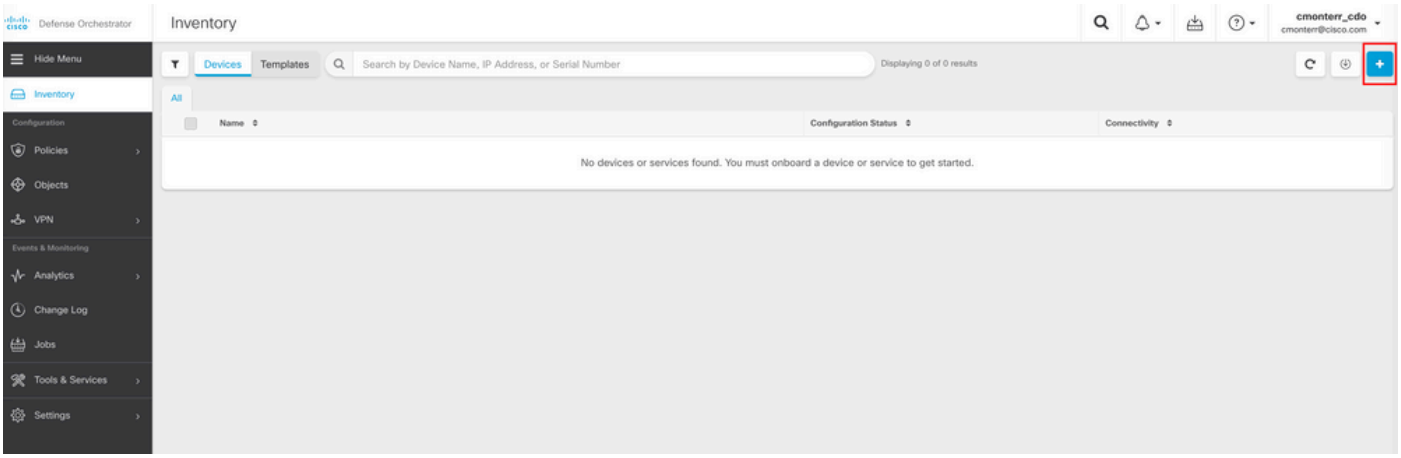
Dit product is ontworpen voor migratie van de Secure Firewall Management Centers op locatie naar de Secure Firewall Management Center SaaS-versie.

Configureren

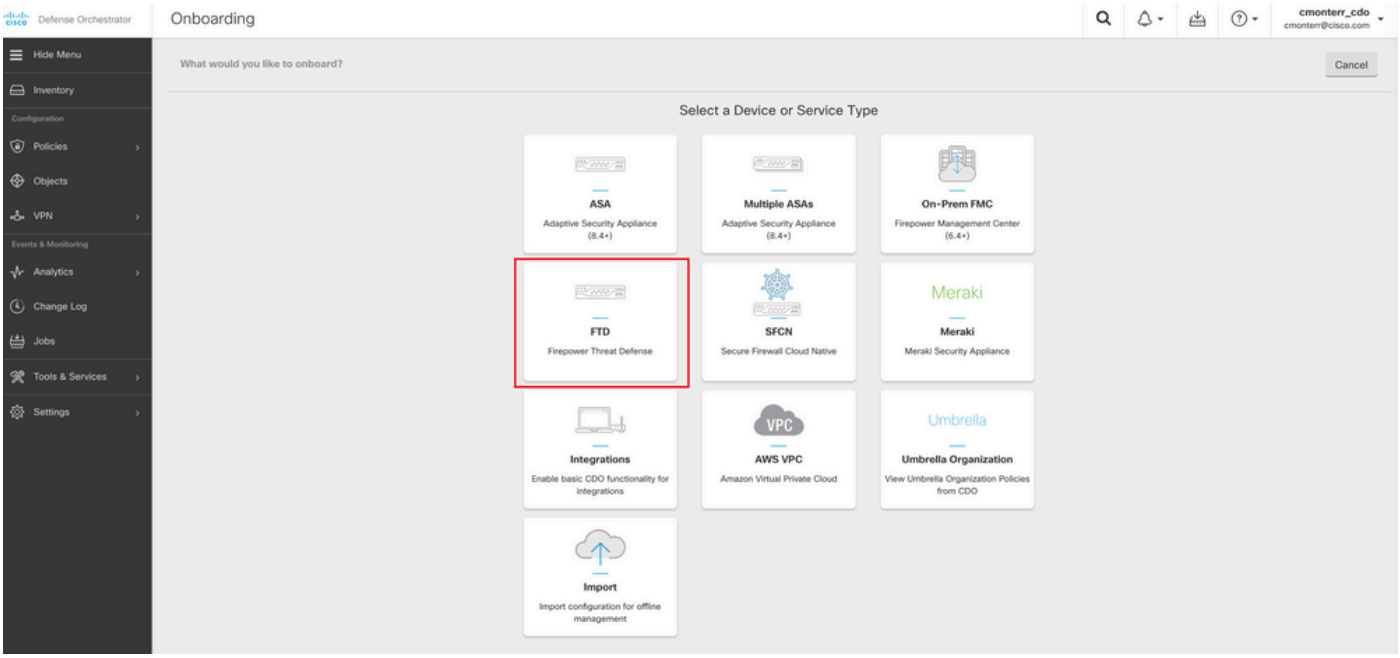
Implementeer een cloudbeheerd Firepower Management Center op CDO.

Deze foto's tonen het instelproces dat nodig is om een cloudgeleverd FMC op CDO te implementeren.

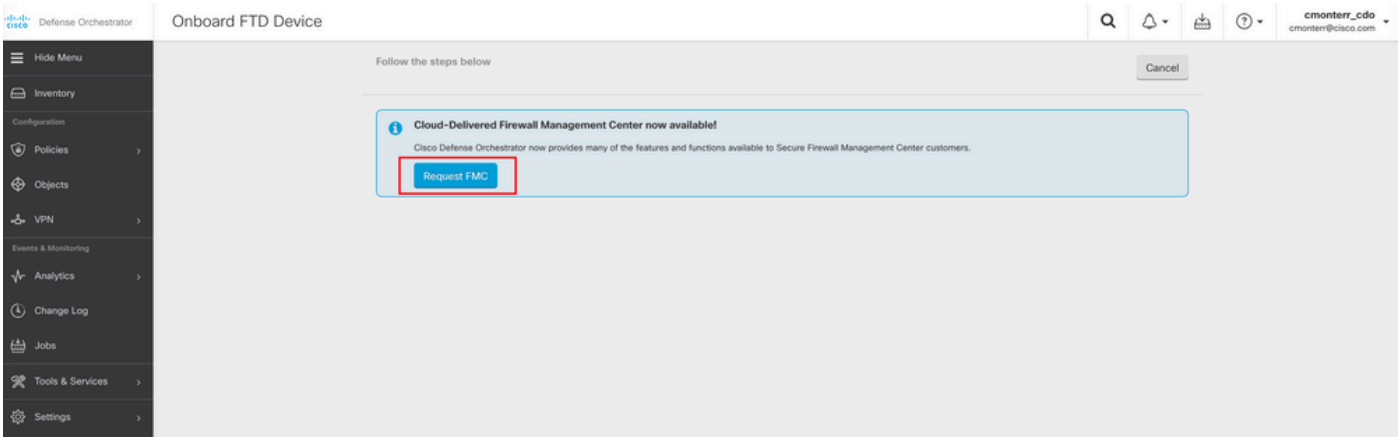
Eerst navigeren naar **Menu > Inventory** om een nieuw apparaat toe te voegen.



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

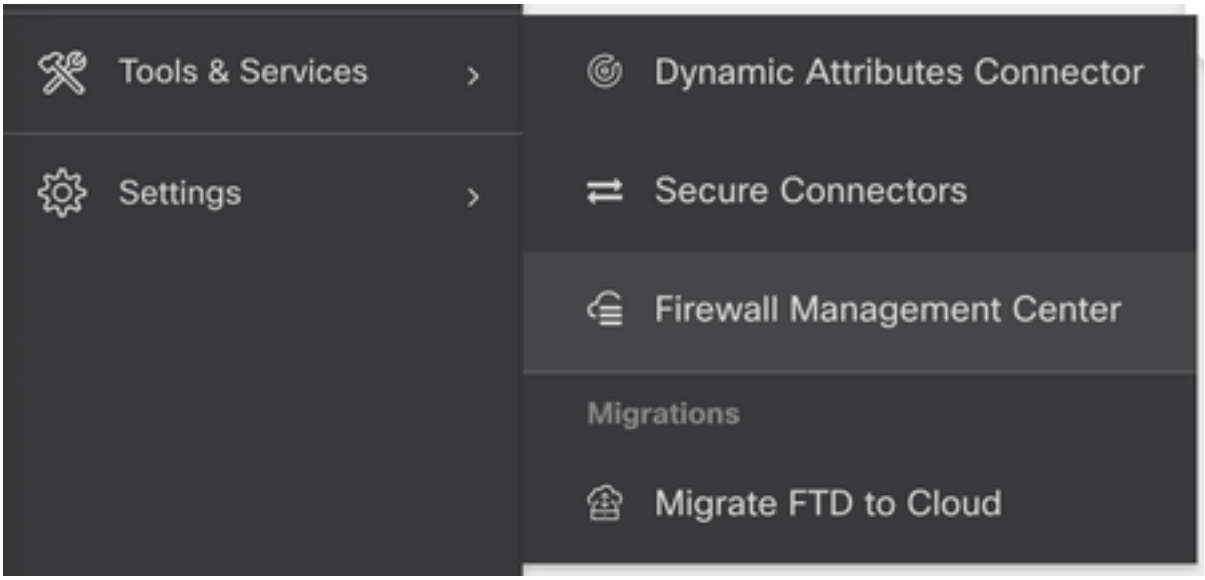


Kiezen **Request FMC** om het Cloud-Delivery Firepower Management Center aan te vragen.

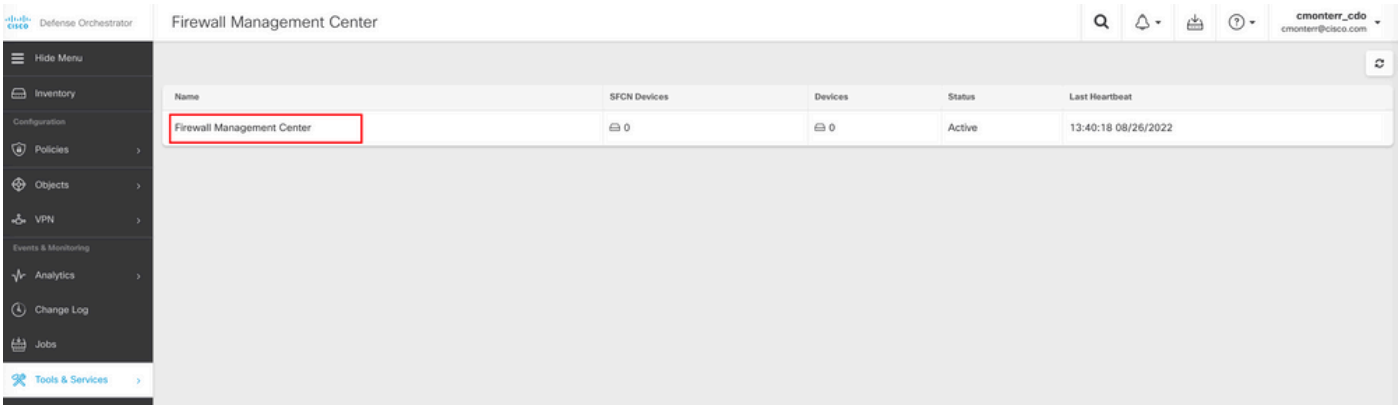


Opmerking: de optie "Aanvraag VCC" wordt alleen getoond als u geen cdFMC in de huurder hebt.

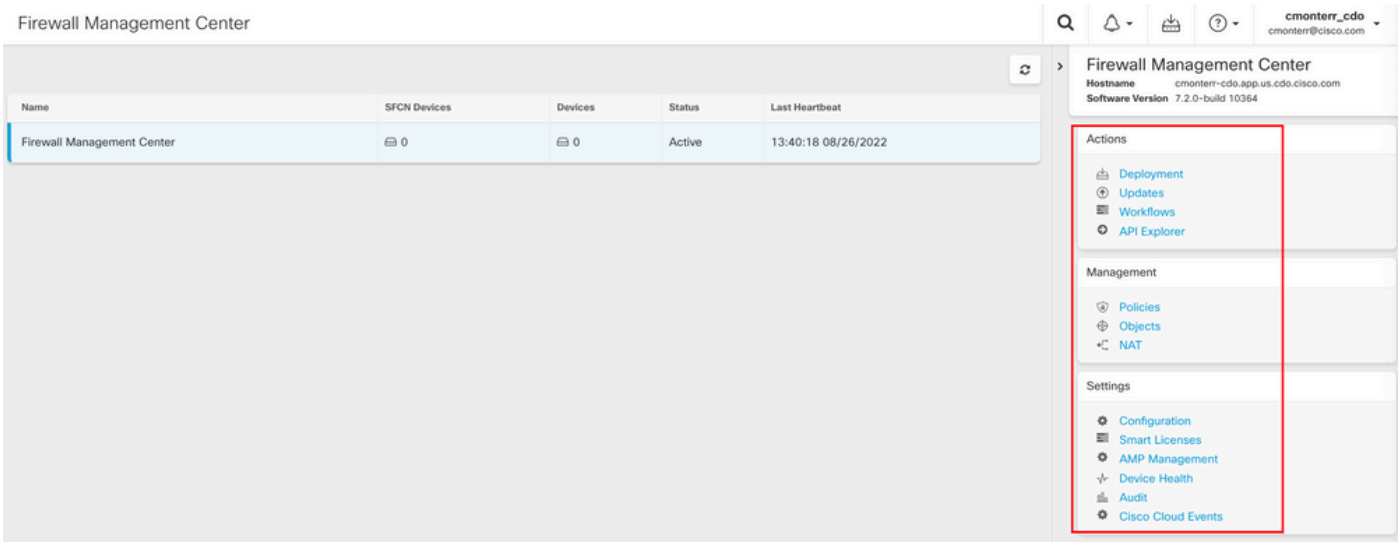
Naar navigeren **Menu > Tools & Services > Firewall Management Center** wanneer de cdFMC klaar is voor gebruik.



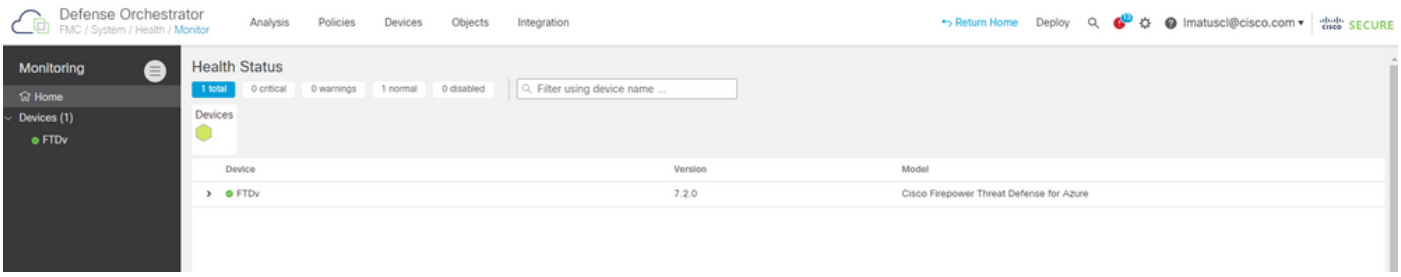
Selecteer de gewenste cdFMC om de cdFMC-informatie weer te geven.



Selecteer een van de opties aan de rechterkant om toegang te krijgen tot de grafische gebruikersinterface (GUI) van de cdFMC.



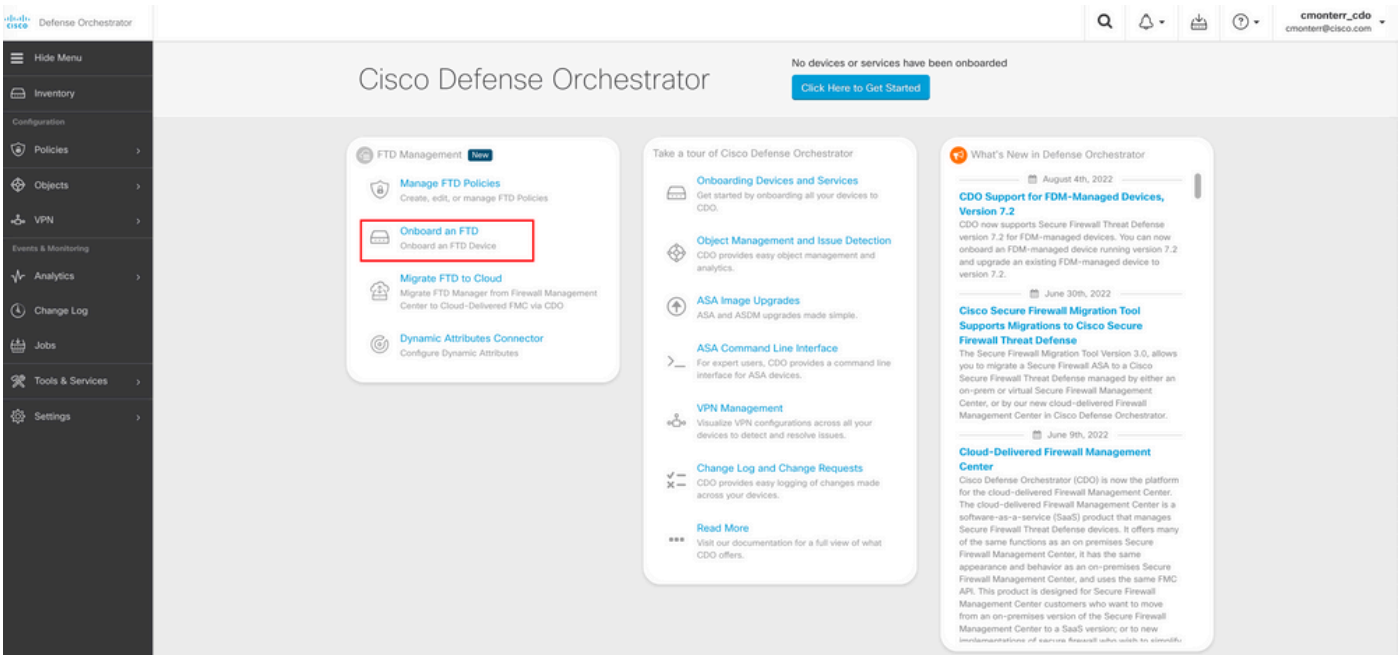
Nu kunt u de CDFMC GUI zien.



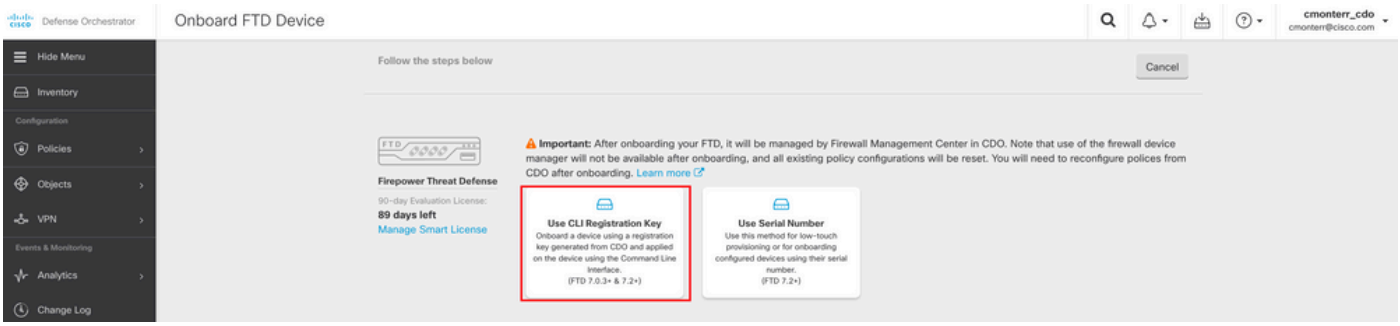
Aan boord van een FTD op een cloudbeheerd FMC

Deze beelden tonen hoe u aan boord van een FTD moet zijn om te worden geregistreerd op een cdFMC met de registratiesleutel Command Line Interface (CLI).

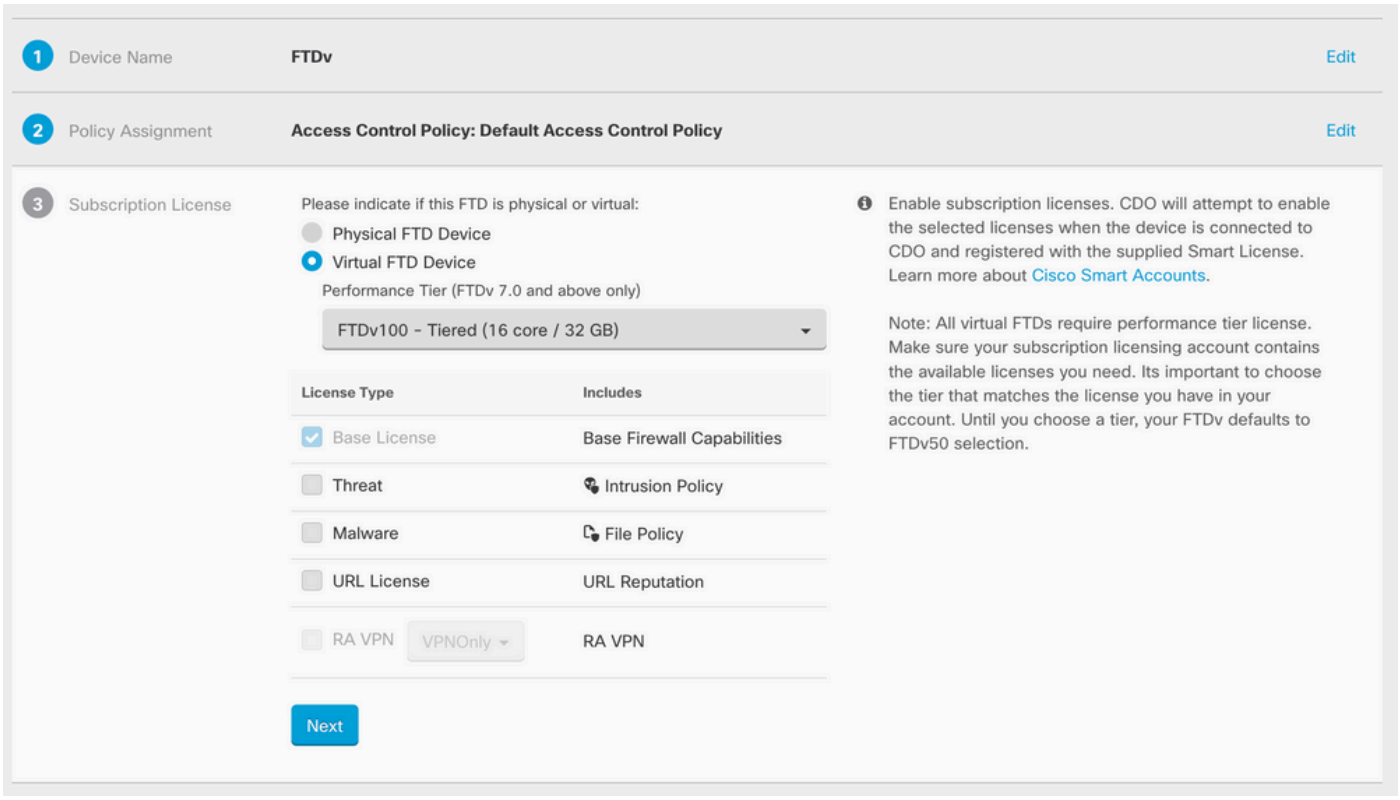
Selecteer eerst **Onboard an FTD** op de CDO startpagina.



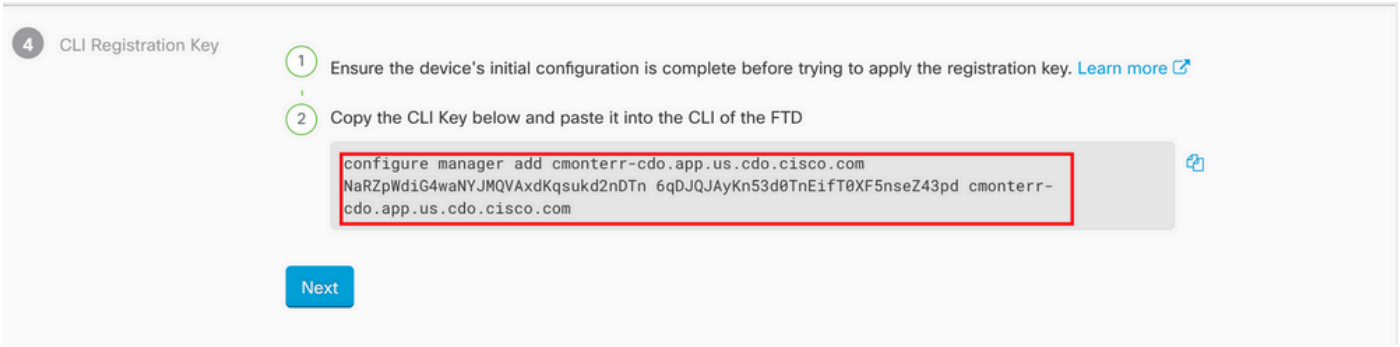
Selecteer vervolgens de **Use CLI Registration Key** optie.



Voer de gevraagde en gewenste FTDv-informatie in.



Ten slotte creëert de cdFMC een specifieke **CLI Key**CLI-sleutel voor uw apparaat.



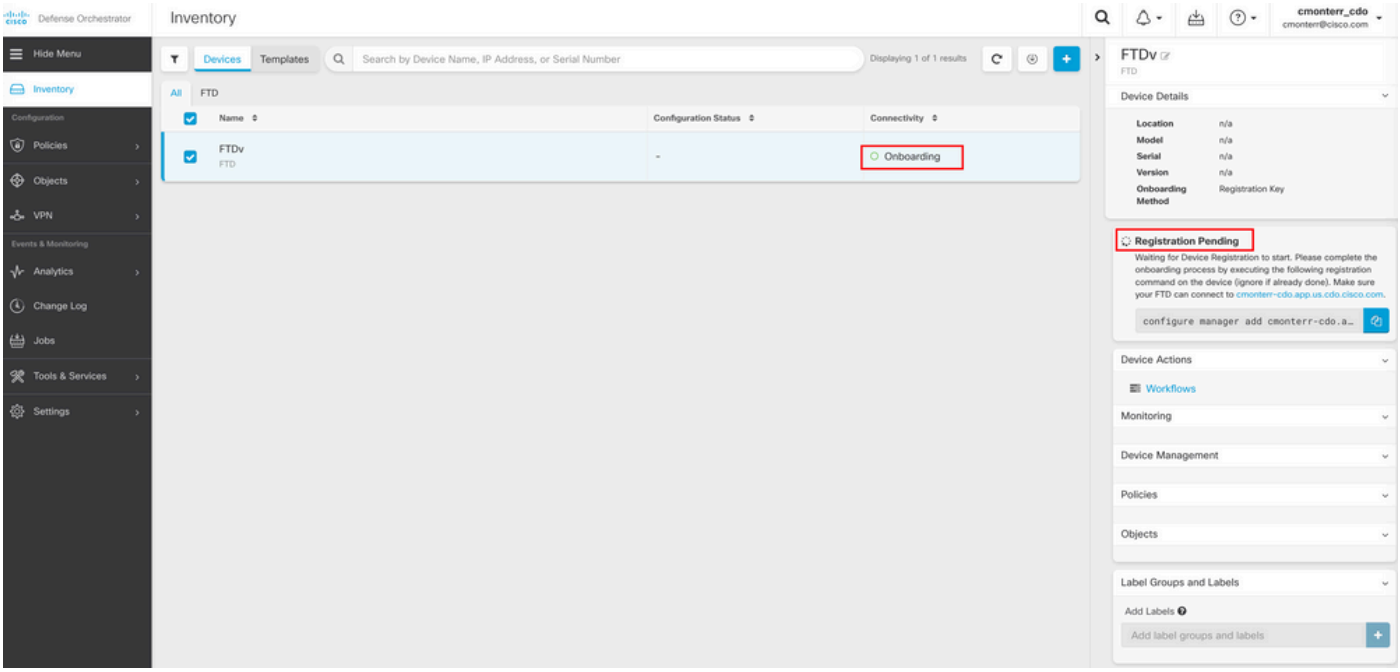
Kopieert de **CLI Key** in de CLI van uw beheerde apparaat.

```
> 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
```

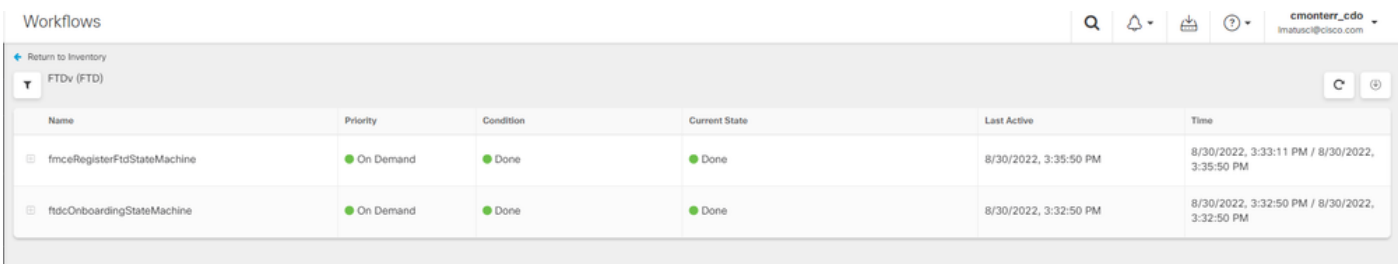
Het CVFMC start een registratietaak.



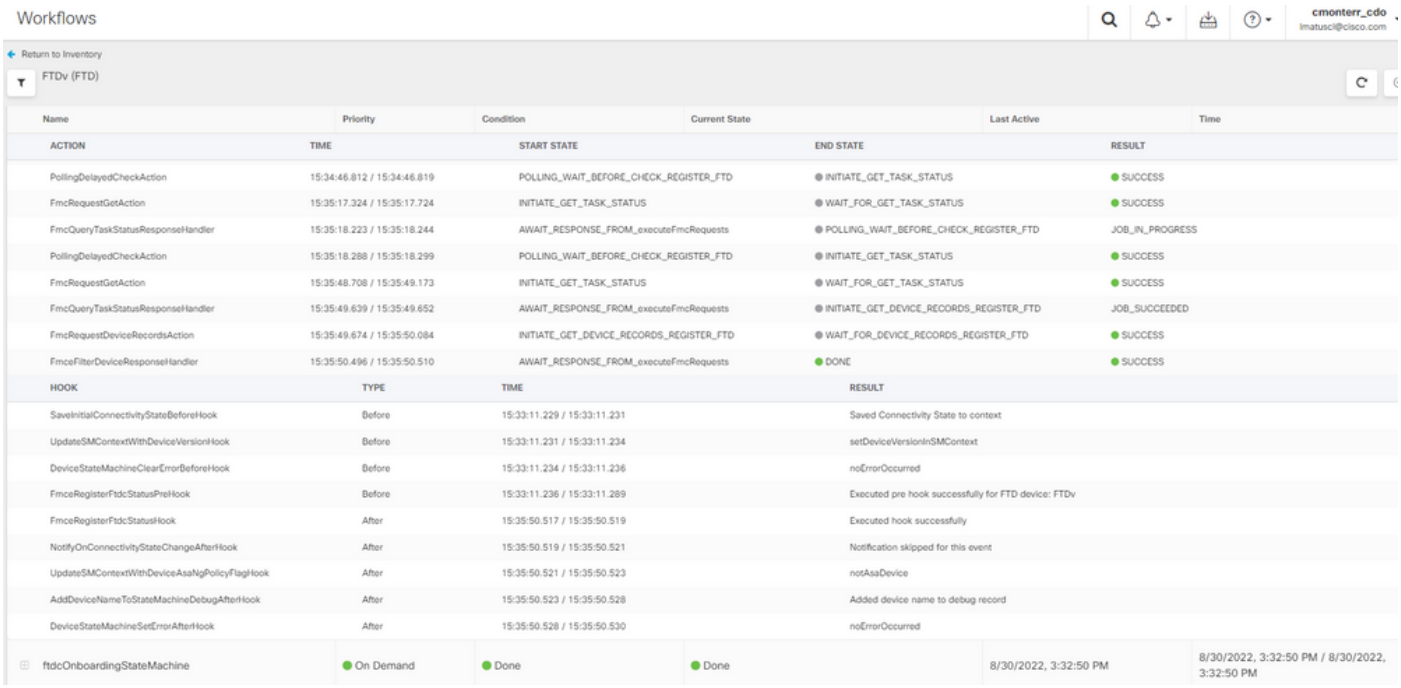
> **Opmerking**: Zorg ervoor dat uw FTD-apparaat communicatie over poorten 8305 (sftunnel) en 443 heeft naar de CDO-huurder om het registratieproces te voltooien. Raadpleeg de volledige netwerkvereisten.

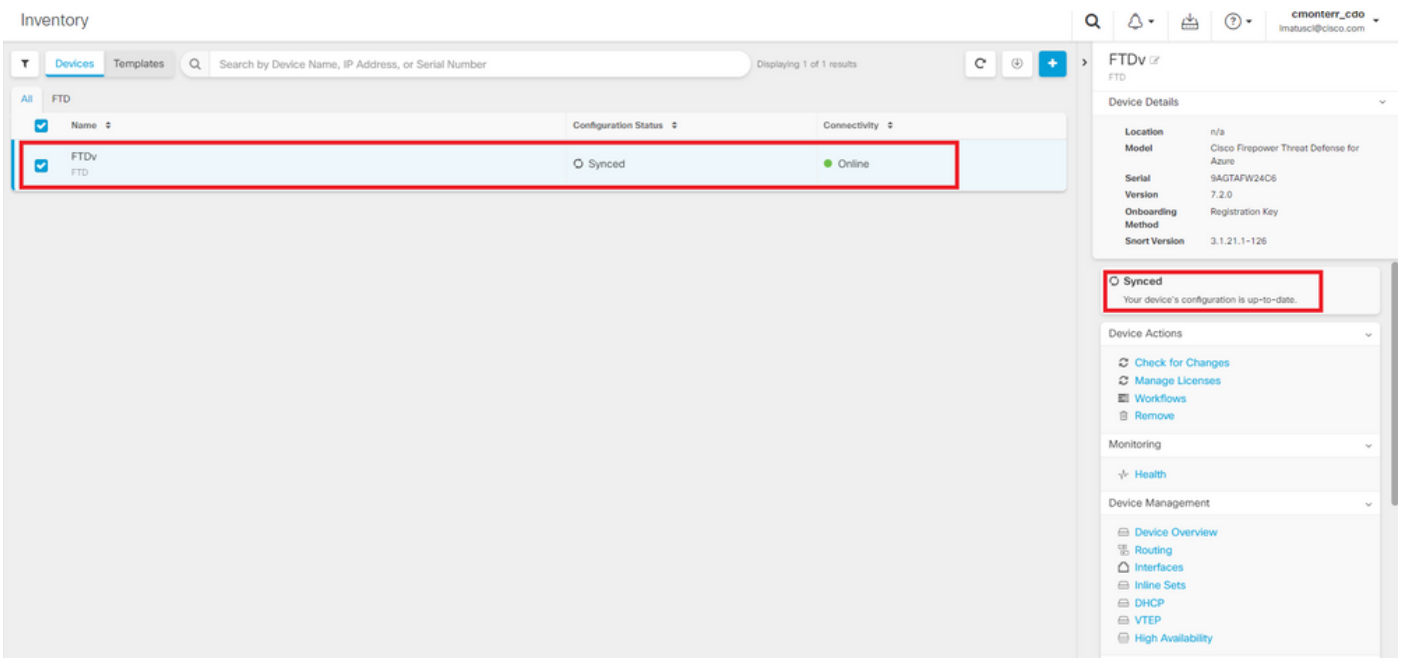
> **Opmerking**: Als u geen verbinding kunt maken met de host, kunt u de DNS-configuratie in de FTD-CLI corrigeren met deze opdracht: **netwerk-dns <adres>configureren**.

Om het registratieproces te bewaken, bladert u naar **Device Actions > Workflows.**.

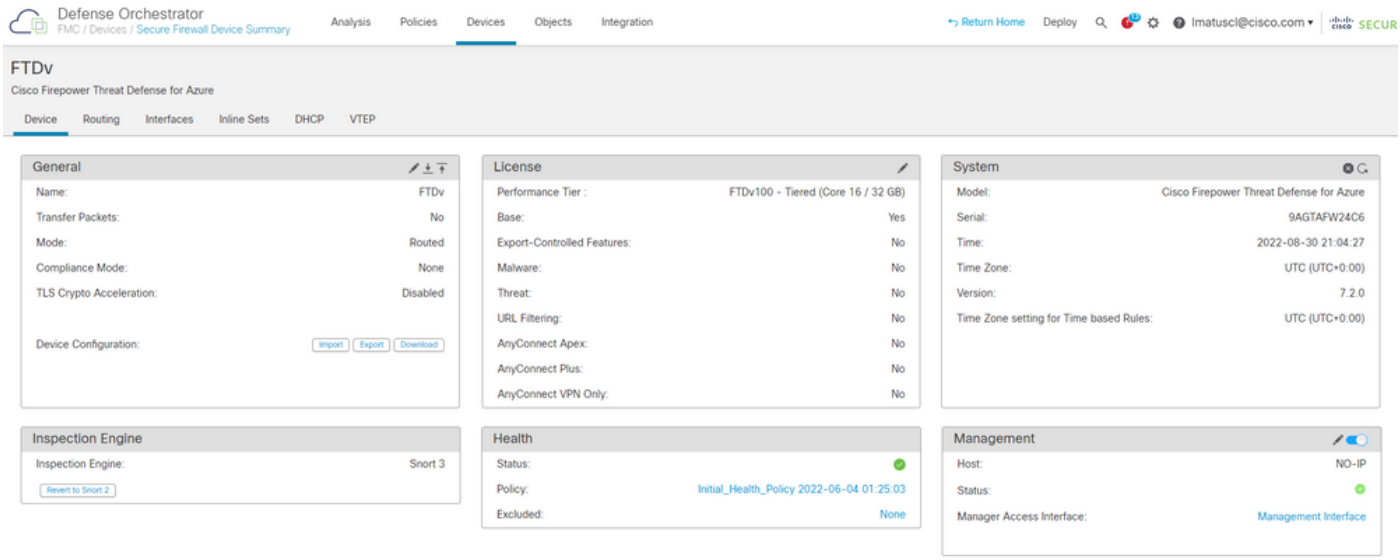


Breid de **Active** staat om aanvullende informatie, deze foto's tonen hoe de FTDv met succes is geregistreerd.





Uiteindelijk navigeren naar **Device Management > Device Overview** om toegang te krijgen tot het CdFMC en de overzichtsstatus van de FTDv te bekijken.



Gerelateerde informatie

- [Technische ondersteuning en documentatie – Cisco Systems]
- [Cisco Secure Firewall Threat Defense-apparaten beheren met cloudbeheerd Firewall Management Center]

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.