

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

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Implementeer een cloudbeheerd Firepower Management Center op CDO.](#)

[Aan boord van een FTD op een cloudbeheerd FMC](#)

[Gerelateerde informatie](#)

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).

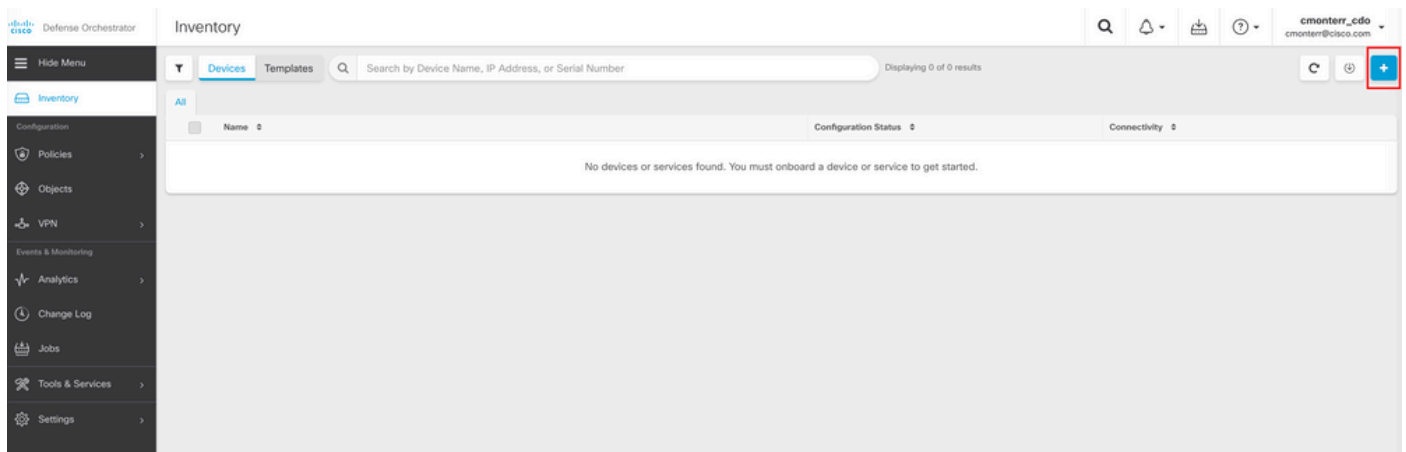
Dit product is ontworpen voor migratie van de Secure Firewall Management Centers op locatie naar de Secure Firewall Management Center SaaS-versie.

Configureren

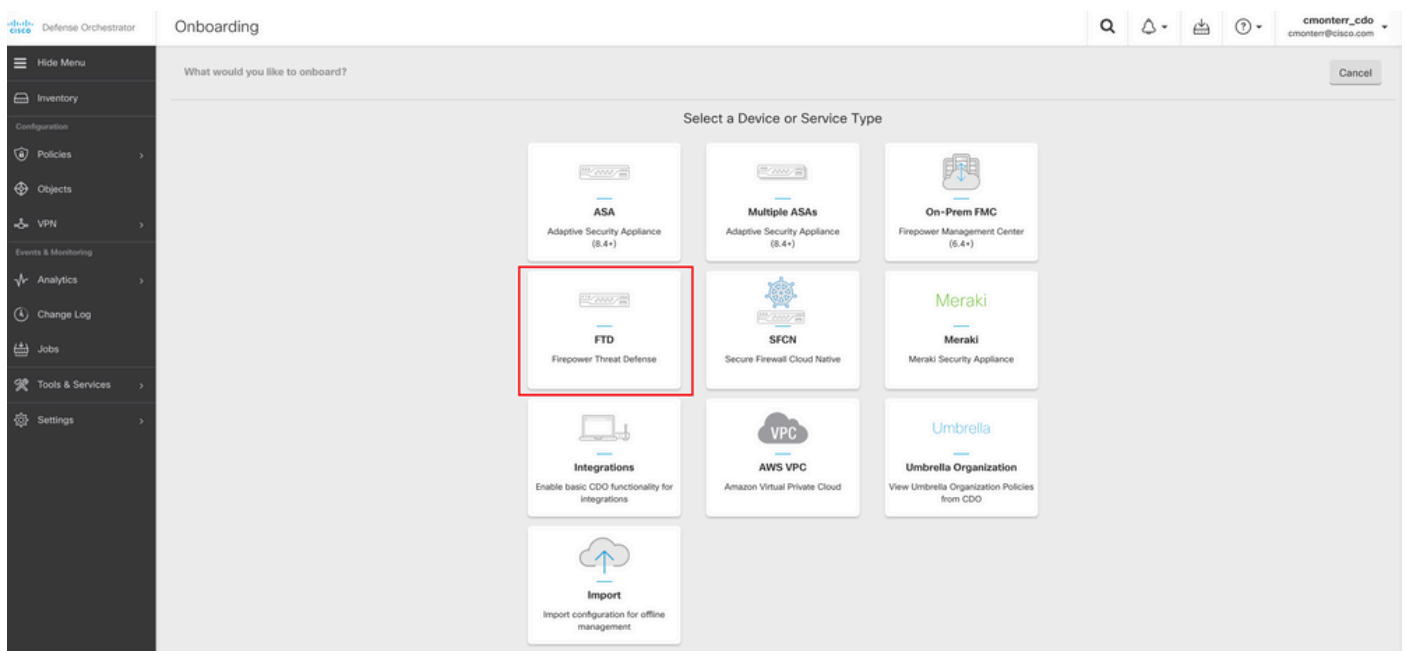
Implementeer een cloudbeheerd Firepower Management Center op CDO.

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

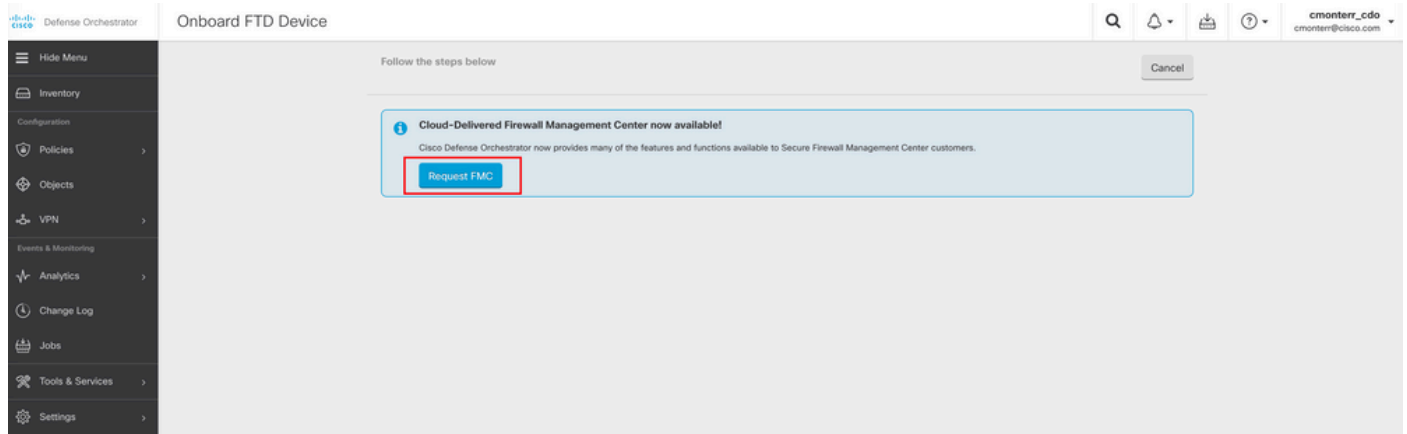
Eerst navigeren naar **Menu > Inventory** om een nieuw apparaat toe te voegen.



Kiezen Firepower Threat Defense (FTD).

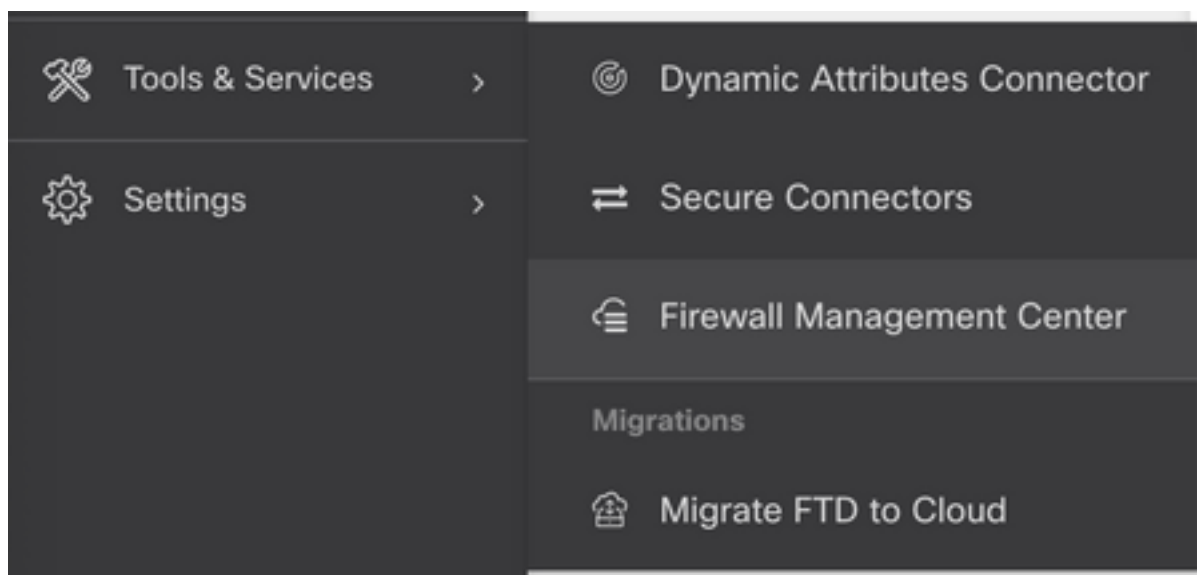


Kiezen **Request FMC** om het Cloud-Delivery Firepower Management Center aan te vragen.

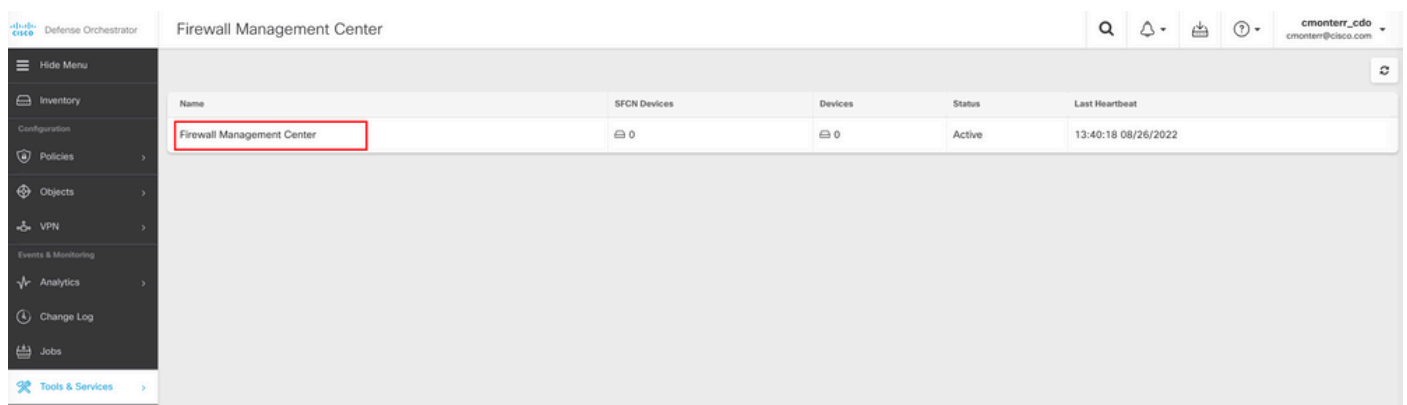


Opmerking: de optie "Aanvraag VCC" wordt alleen getoond als u geen cdFMC in de huurder hebt.

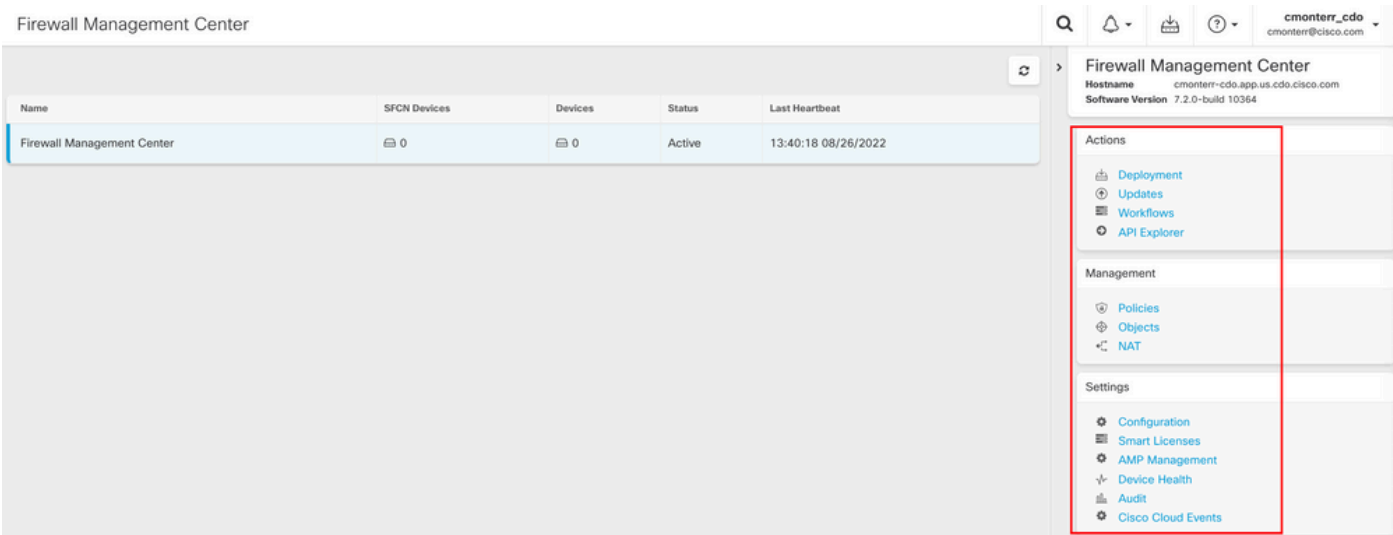
Naar navigeren **Menu > Tools & Services > Firewall Management Center** wanneer de cdFMC klaar is voor gebruik.



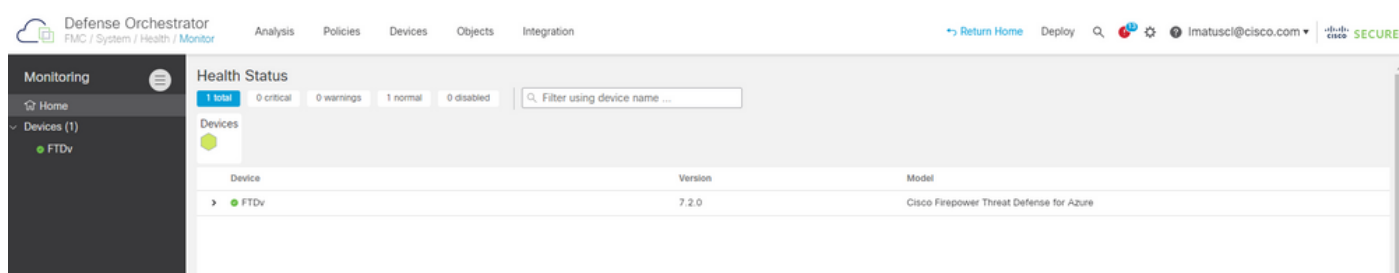
Selecteer de gewenste cdFMC om de cdFMC-informatie weer te geven.



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



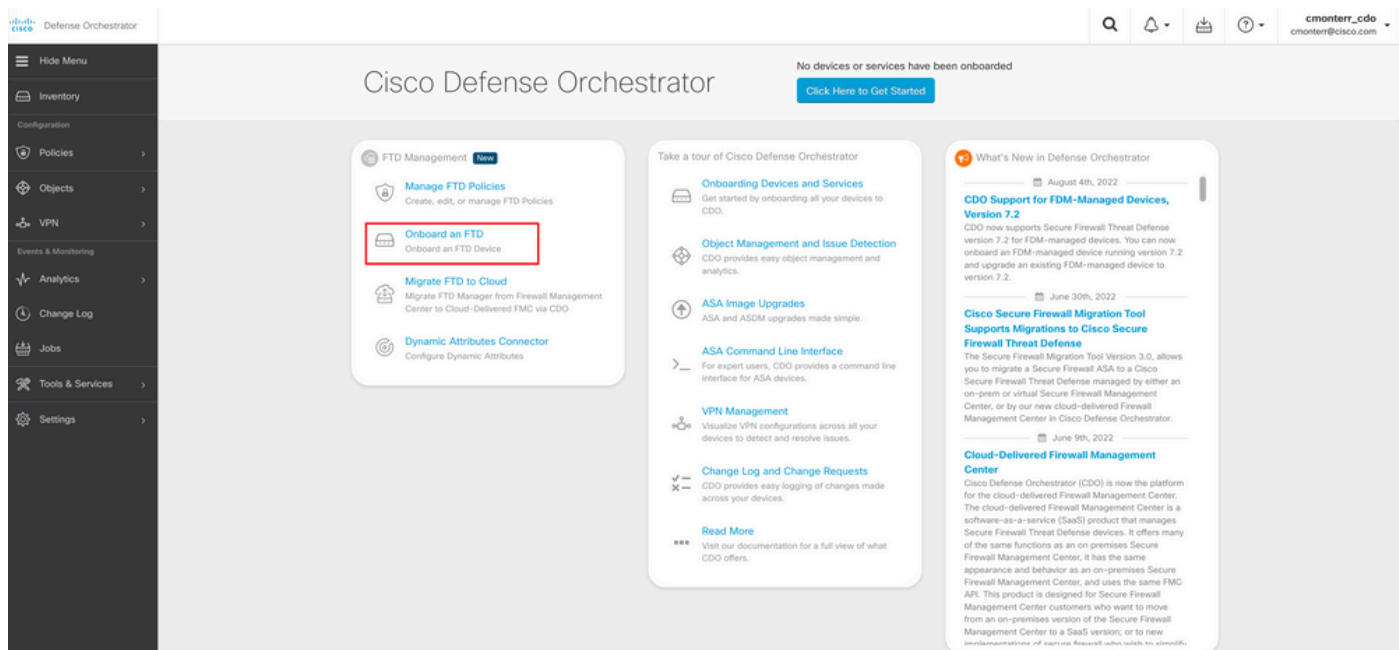
Nu kunt u de CDFMC GUI zien.



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.

Onboard FTD Device

Follow the steps below

Cancel

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 policies from CDO after onboarding. [Learn more](#)

Firepower Threat Defense
90-day Evaluation License:
89 days left
[Manage Smart License](#)

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+)

Voer de gevraagde en gewenste FTDv-informatie in.

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
<input checked="" type="checkbox"/> Base License	Base Firewall Capabilities
<input type="checkbox"/> Threat	Intrusion Policy
<input type="checkbox"/> Malware	File Policy
<input type="checkbox"/> URL License	URL Reputation
<input type="checkbox"/> RA VPN VPNOnly	RA VPN

[Next](#)

Info: 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.

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

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
NaRZpWdiG4waNYJMVAxdKqsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-
cdo.app.us.cdo.cisco.com
```

[Next](#)

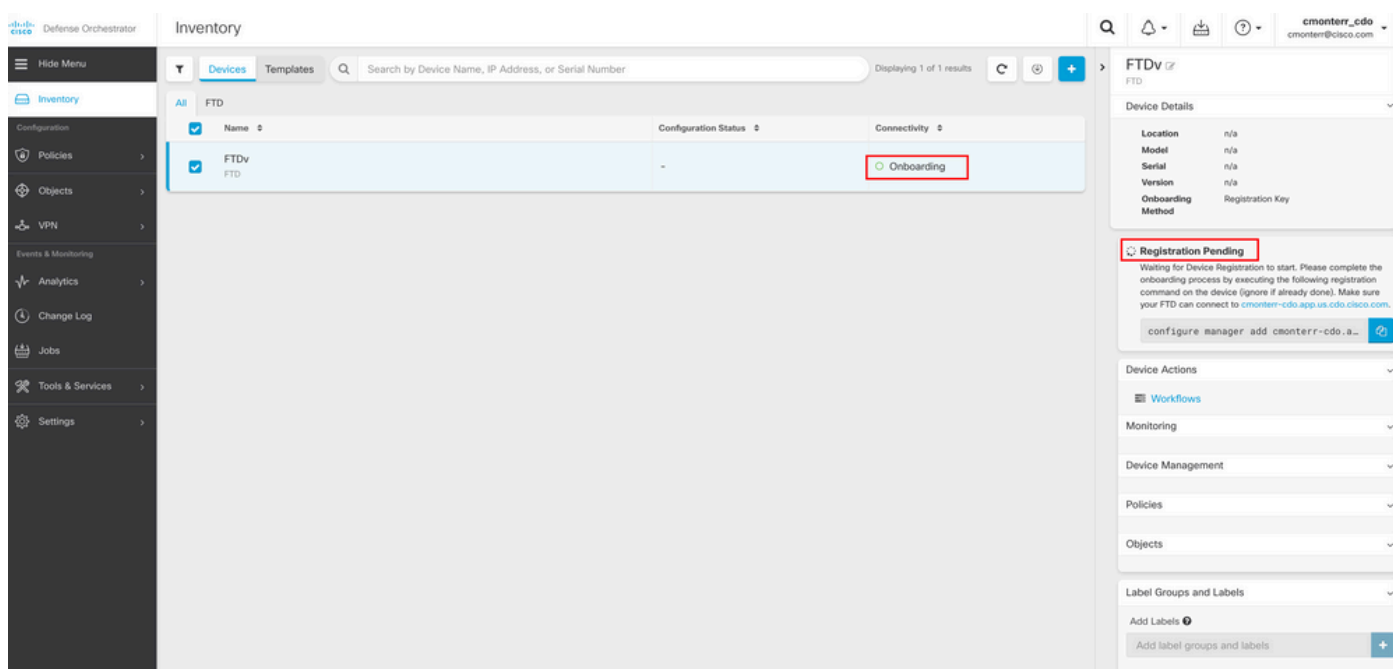
Kopieert de CLI key in de CLI van uw beheerde apparaat.

```
> 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
```

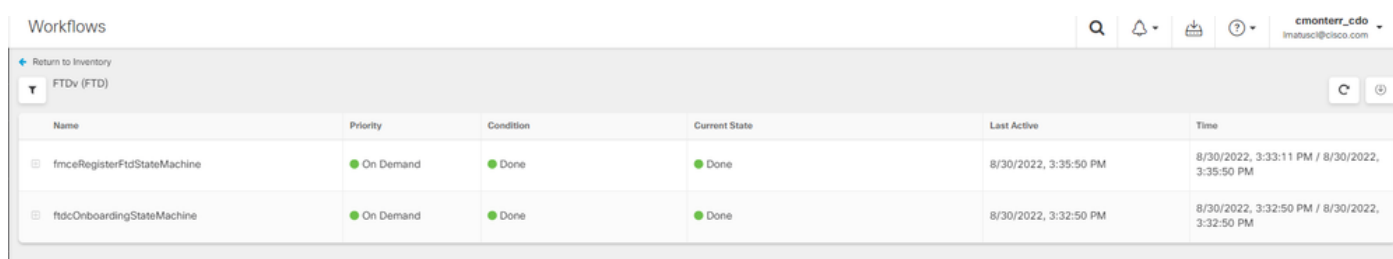
Het CVFMC start een registratietaak.



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.

Workflows

Return to Inventory

FTDv (FTD)

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	
FmcFilterDeviceResponseHandler	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		
FmcRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FTD device: FTDv		
FmcRegisterFtdcStatusHook	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		
DeviceStateMachineSetEmpirAfterHook	After	15:35:50.528 / 15:35:50.530	noErrorOccurred		
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

Devices Templates

Search by Device Name, IP Address, or Serial Number

Displaying 1 of 1 results

FTDv

Name	Configuration Status	Connectivity
FTDv FTD	○ Synced	● Online

Device Details

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

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

Device Actions

- Check for Changes
- Manage Licenses
- Workflows
- Remove

Monitoring

- Health

Device Management

- Device Overview
- Routing
- Interfaces
- Inline Sets
- DHCP
- VTEP
- High Availability

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

FTDv

Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

<p>General </p> <p>Name: FTDv</p> <p>Transfer Packets: No</p> <p>Mode: Routed</p> <p>Compliance Mode: None</p> <p>TLS Crypto Acceleration: Disabled</p> <p>Device Configuration: Import Export Download</p>	<p>License </p> <p>Performance Tier : FTDv100 - Tiered (Core 16 / 32 GB)</p> <p>Base: Yes</p> <p>Export-Controlled Features: No</p> <p>Malware: No</p> <p>Threat: No</p> <p>URL Filtering: No</p> <p>AnyConnect Apex: No</p> <p>AnyConnect Plus: No</p> <p>AnyConnect VPN Only: No</p>	<p>System </p> <p>Model: Cisco Firepower Threat Defense for Azure</p> <p>Serial: 9AGTAFW2406</p> <p>Time: 2022-08-30 21:04:27</p> <p>Time Zone: UTC (UTC+0:00)</p> <p>Version: 7.2.0</p> <p>Time Zone setting for Time based Rules: UTC (UTC+0:00)</p>
<p>Inspection Engine</p> <p>Inspection Engine: Snort 3</p> <p>Revert to Snort 2</p>	<p>Health</p> <p>Status: </p> <p>Policy: Initial_Health_Policy 2022-06-04 01:25:03</p> <p>Excluded: None</p>	<p>Management </p> <p>Host: NO-IP</p> <p>Status: </p> <p>Manager Access Interface: Management Interface</p>

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.