

Bereitstellung eines Cloud-gestützten FMC (cdFMC) in Cisco Defense Orchestrator (CDO)

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Bereitstellung eines Cloud-basierten FirePOWER Management Center auf CDO](#)

[Integration einer FTD in einem Cloud-basierten FMC](#)

[Zugehörige Informationen](#)

Einleitung

Dieses Dokument beschreibt die Bereitstellung und den integrierten Prozess von Cloud-basiertem FMC auf der CDO-Plattform.

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

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

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- cdFMC 7.2.0
- FTDv 7.2.0

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Hintergrundinformationen

Cisco Defense Orchestrator (CDO) ist die Plattform für das Cloud-basierte Firewall Management Center (cdFMC). Das über die Cloud bereitgestellte Firewall Management Center ist ein Software-as-a-Service (SaaS)-Produkt, das die Verwaltung sicherer Firewall-Geräte zum Schutz vor Bedrohungen ermöglicht. Es bietet viele Funktionen wie eine sichere Firewall vor Ort und einen sicheren Schutz vor Bedrohungen durch die Firewall. Es bietet dasselbe Erscheinungsbild und Verhalten wie ein Secure Firewall Management Center vor Ort und verwendet dieselbe FMC Application Programming Interface (API).

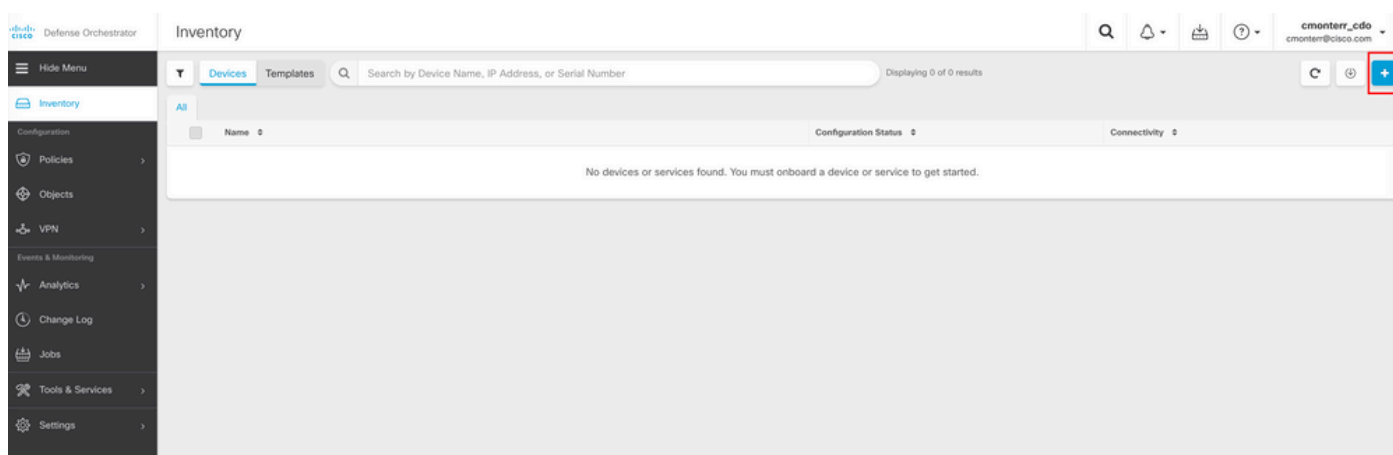
Dieses Produkt wurde für die Migration von den lokalen Secure Firewall Management Centern zur Secure Firewall Management Center SaaS-Version entwickelt.

Konfigurieren

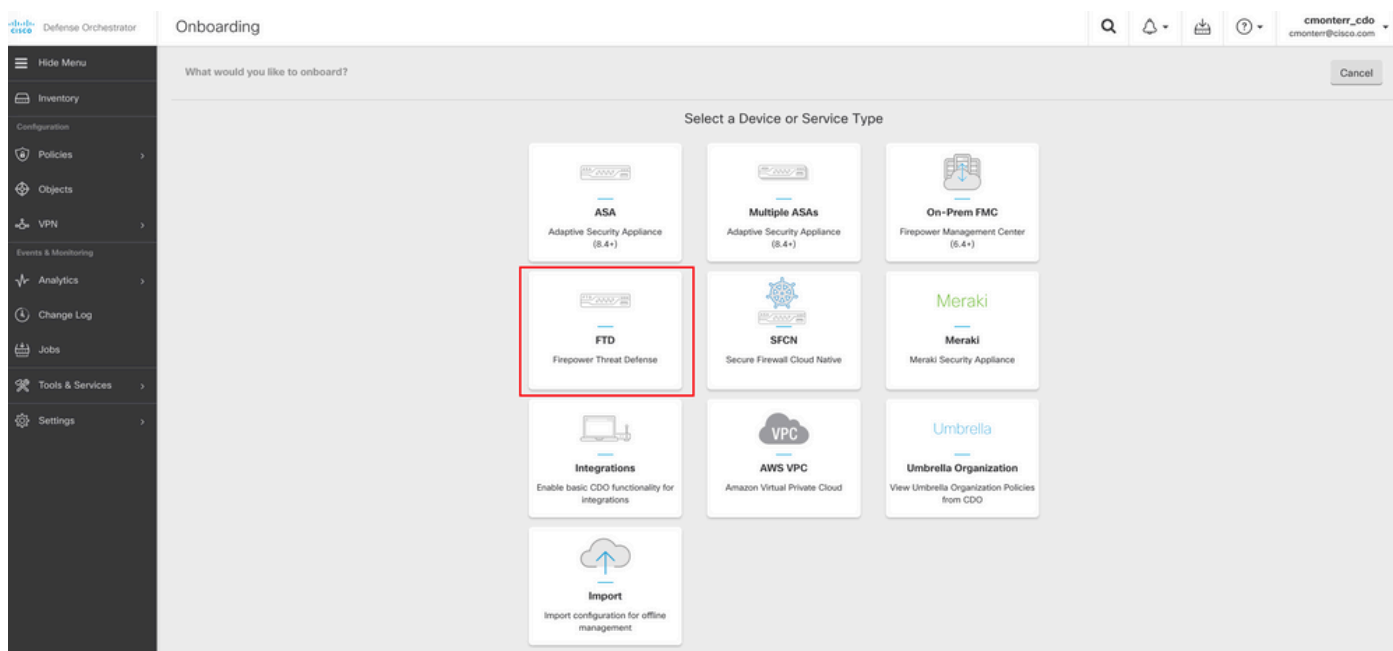
Bereitstellung eines Cloud-basierten FirePOWER Management Center auf CDO

Diese Bilder zeigen den anfänglichen Einrichtungsprozess, der für die Bereitstellung eines Cloud-basierten FMC auf CDO erforderlich ist.

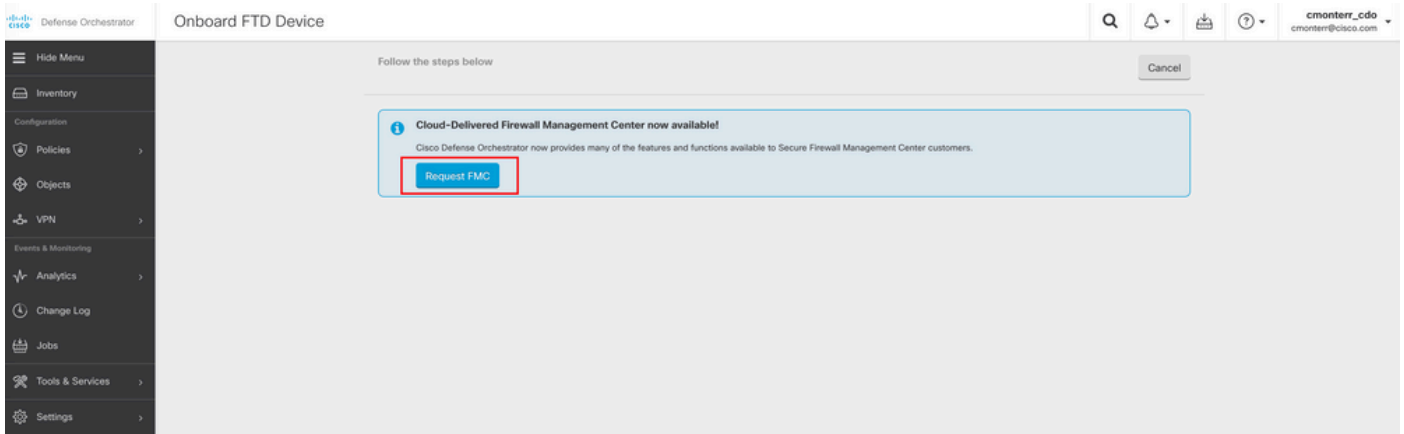
Navigieren Sie zunächst zu **Menu > Inventory** um ein neues Gerät hinzuzufügen.



Auswählen Firepower Threat Defense (FTD).

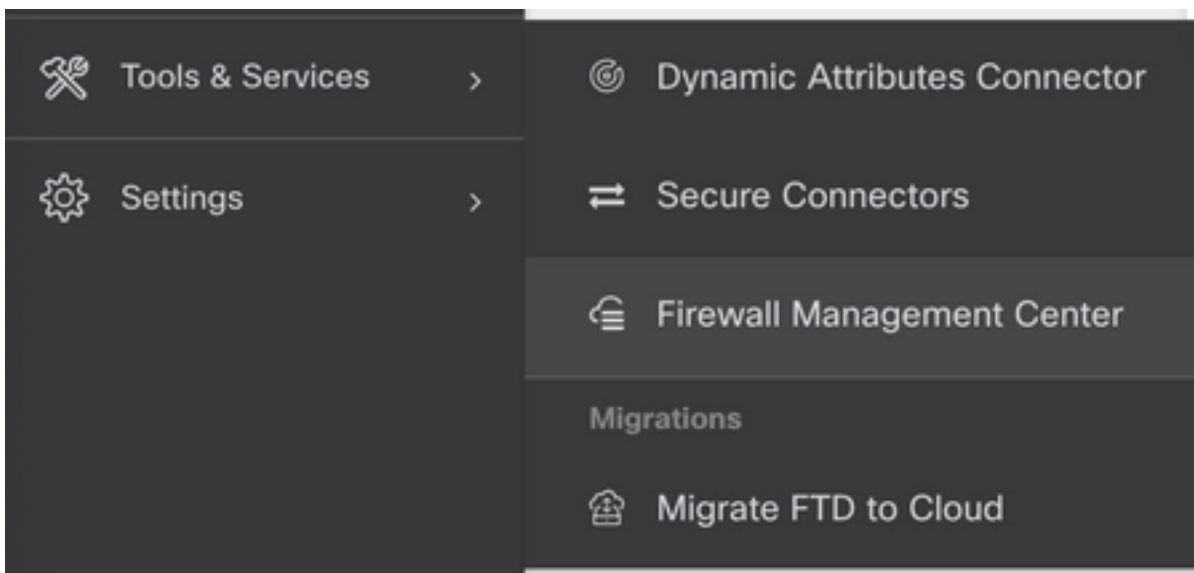


Auswählen **Request FMC** um das Cloud-basierte FirePOWER Management Center anzufordern.

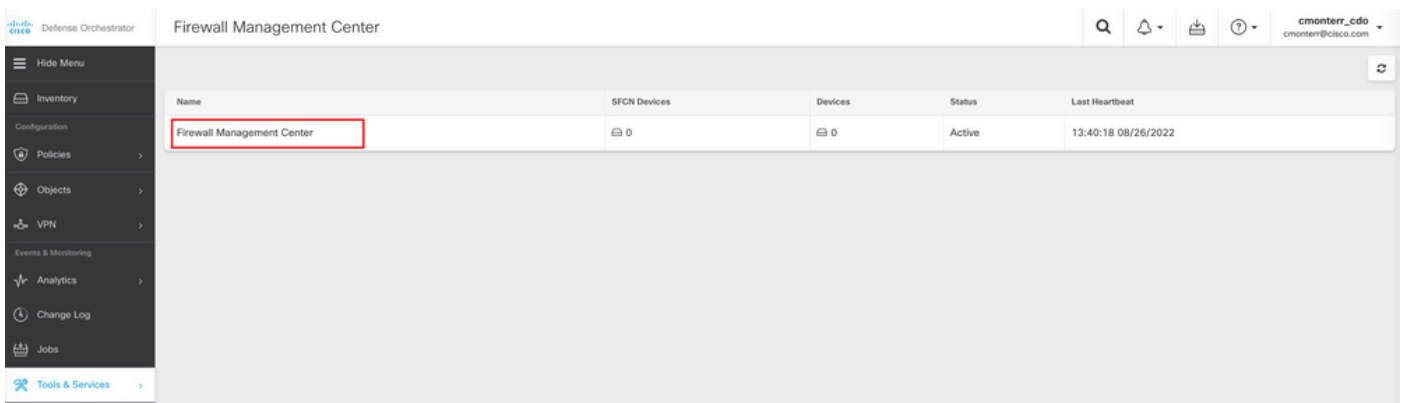


Hinweis: Die Option "Request FMC" wird nur angezeigt, wenn im Tenant kein cdFMC vorhanden ist.

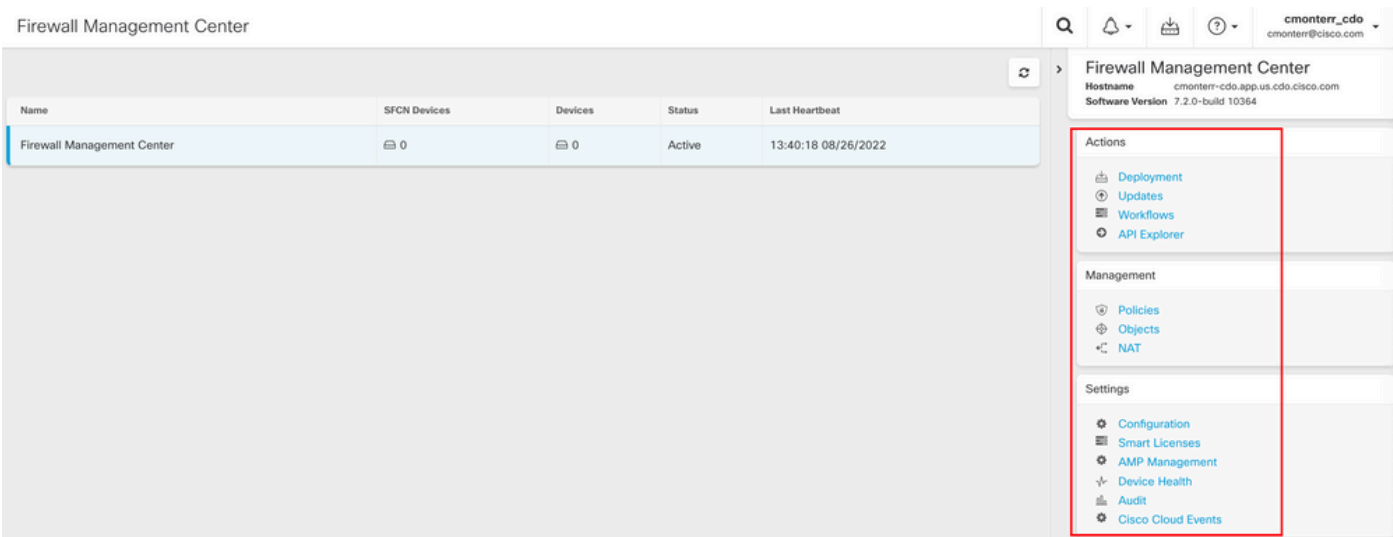
Navigieren Sie zu **Menu > Tools & Services > Firewall Management Center** wenn das cdFMC einsatzbereit ist.



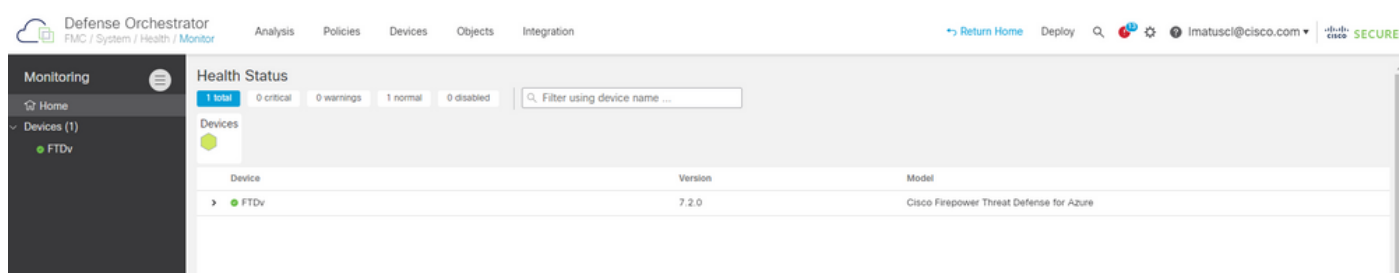
Wählen Sie das gewünschte cdFMC, um die cdFMC-Informationen anzuzeigen.



Um auf die grafische Benutzeroberfläche (GUI) des cdFMC zuzugreifen, wählen Sie eine der Optionen auf der rechten Seite aus.



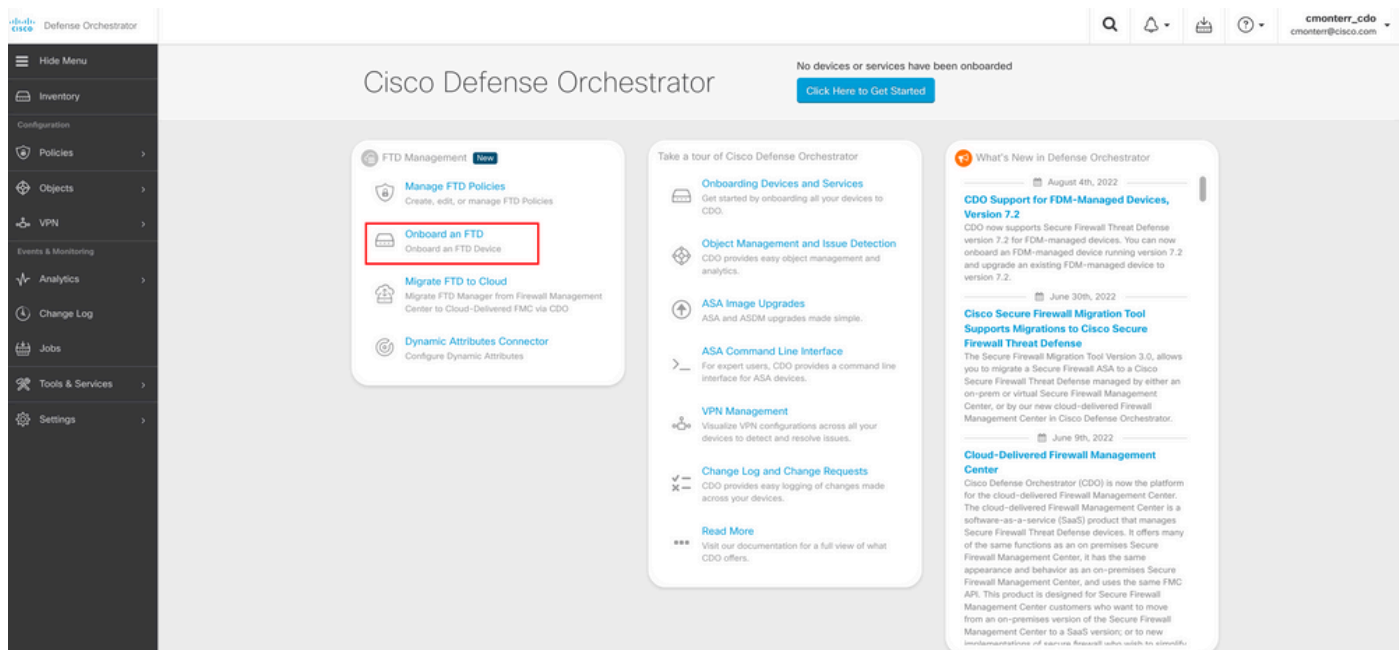
Nun sehen Sie die Benutzeroberfläche von cdFMC.



Integration einer FTD in einem Cloud-basierten FMC

Diese Bilder zeigen, wie man eine FTD einbindet, um auf einem cdFMC mit CLI-Registrierungsschlüssel registriert zu werden.

Wählen Sie zunächst **Onboard an FTD** auf der CDO-Startseite.



Wählen Sie anschließend die **Use CLI Registration Key Option**.

Onboard FTD Device

Follow the steps below

Cancel

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 policies 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+)

Fahren Sie mit der Eingabe der angeforderten und gewünschten FTDv-Informationen fort.

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.

Schließlich erstellt das cdFMC eine bestimmte CLI key CLI-Schlüssel für Ihr Gerät.

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](#)

Kopieren Sie CLI key in die CLI des verwalteten Geräts ein.

```

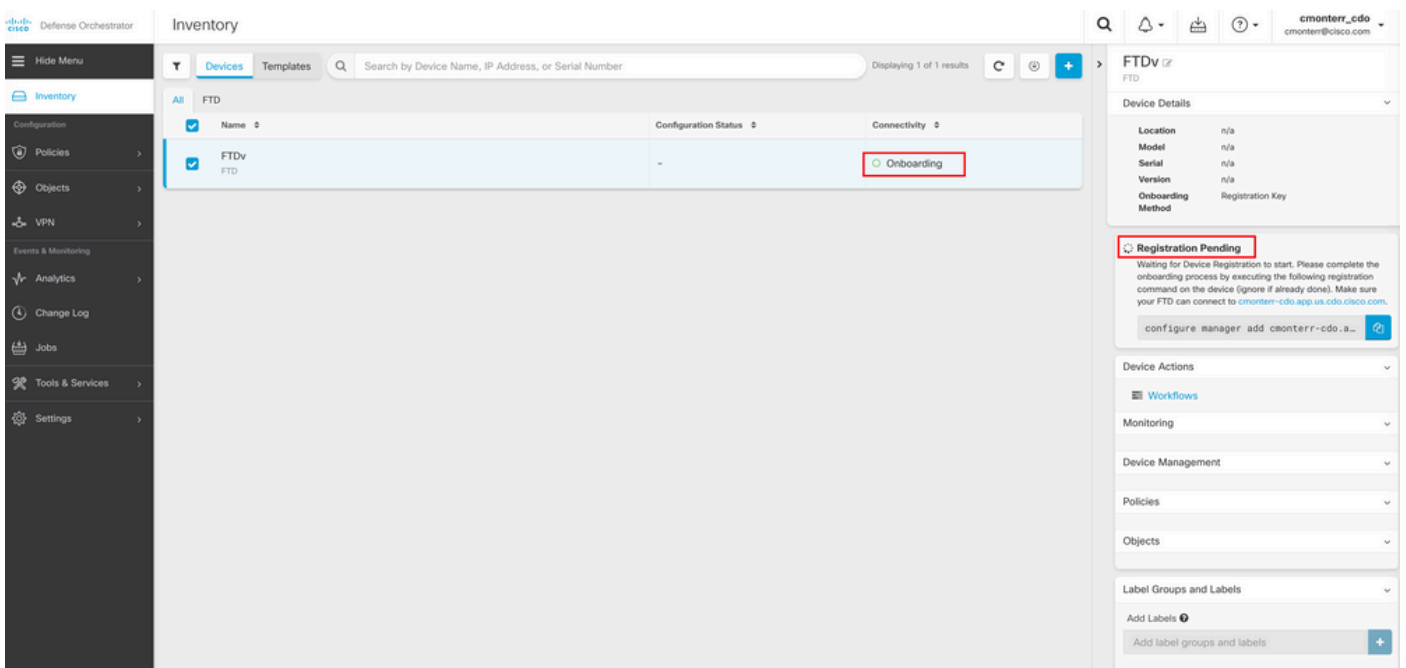
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAXdK
qsukd2nDTn 6qDJQJAYKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.

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

```

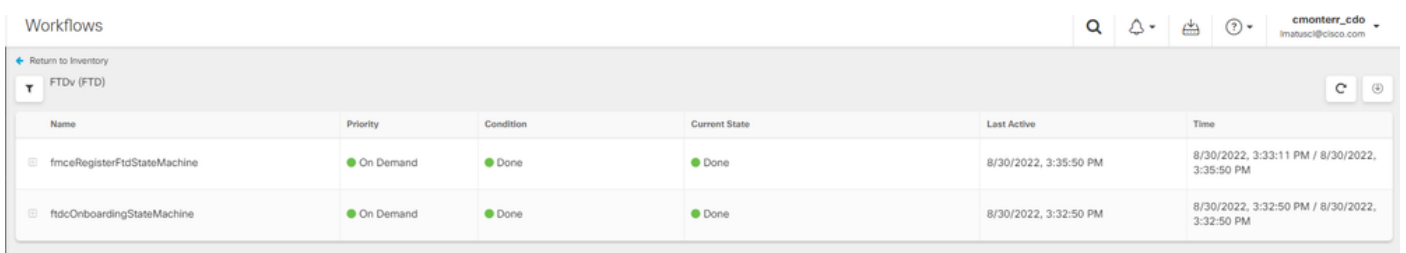
Das cdFMC initiiert eine Registrierungs Aufgabe.



Hinweis: Stellen Sie sicher, dass Ihr FTD-Gerät über die Ports 8305 (Sftunnel) und 443 mit dem CDO-Tenant kommuniziert, um den Registrierungsprozess abzuschließen. Lesen Sie die vollständigen [Netzwerkanforderungen](#).

Hinweis: Wenn Sie keine Verbindung zum Host herstellen können, können Sie die DNS-Konfiguration in der FTD-CLI mit dem folgenden Befehl korrigieren: `configure network dns <Adresse>`.

Um den Registrierungsprozess zu überwachen, navigieren Sie zu **Device Actions > Workflows**.



Erweitern Sie die **Active** angeben, um zusätzliche Informationen zu erhalten, zeigen diese Bilder, wie die FTDv erfolgreich registriert wurde.

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

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

Navigieren Sie abschließend zu **Device Management > Device Overview** um auf das cdFMC zuzugreifen und den FTDv-Übersichtsstatus zu überprüfen.

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>

Zugehörige Informationen

- [Technischer Support und Dokumentation für Cisco Systeme](#)
- [Management von Cisco Secure Firewall Threat Defense-Geräten mit Cloud-basiertem Firewall-Management Center](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.