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

Inhalt

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).

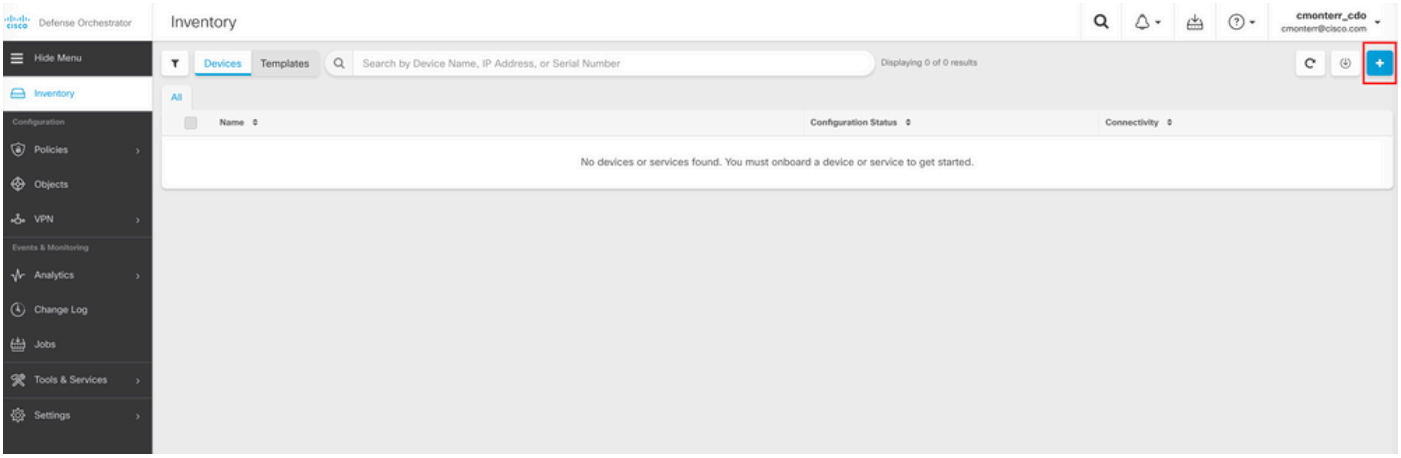
Dieses Produkt wurde für die Migration von den lokalen Secure Firewall Management Centern zur Secure Firewall Management Center SaaS-Version entwickelt.

Konfigurieren

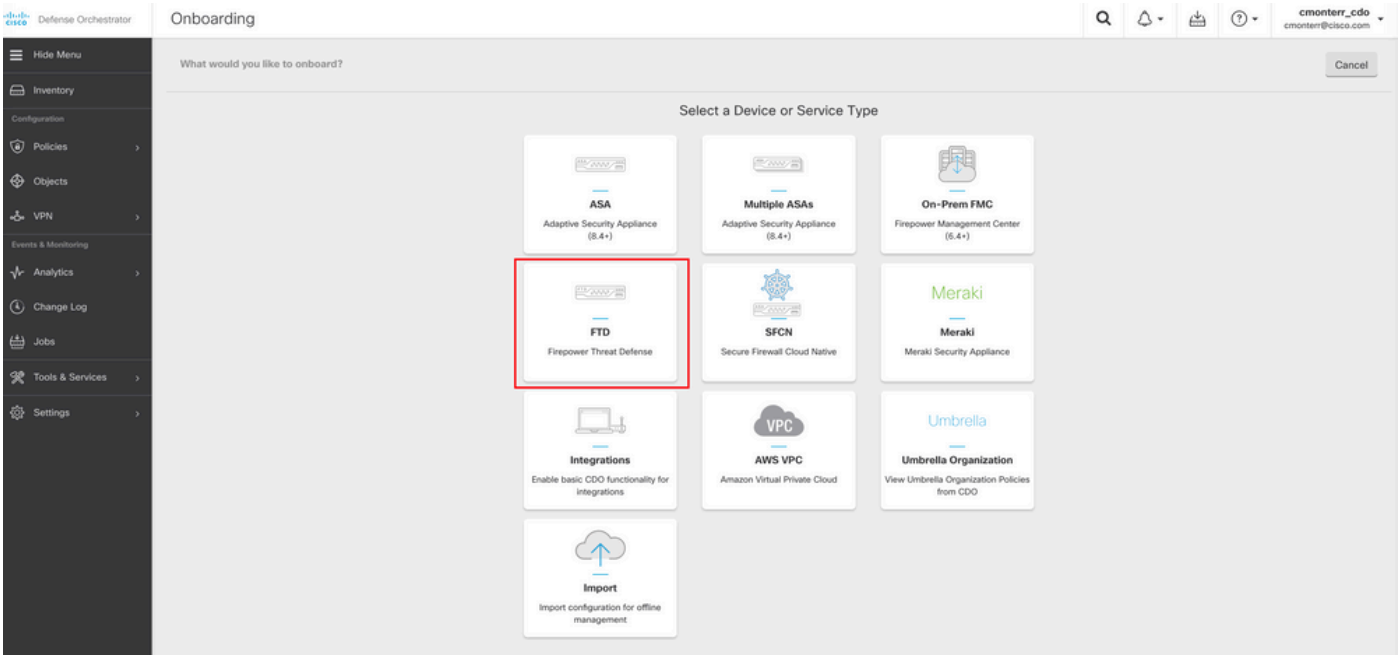
Bereitstellung eines Cloud-basierten FirePOWER Management Center auf CDO

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

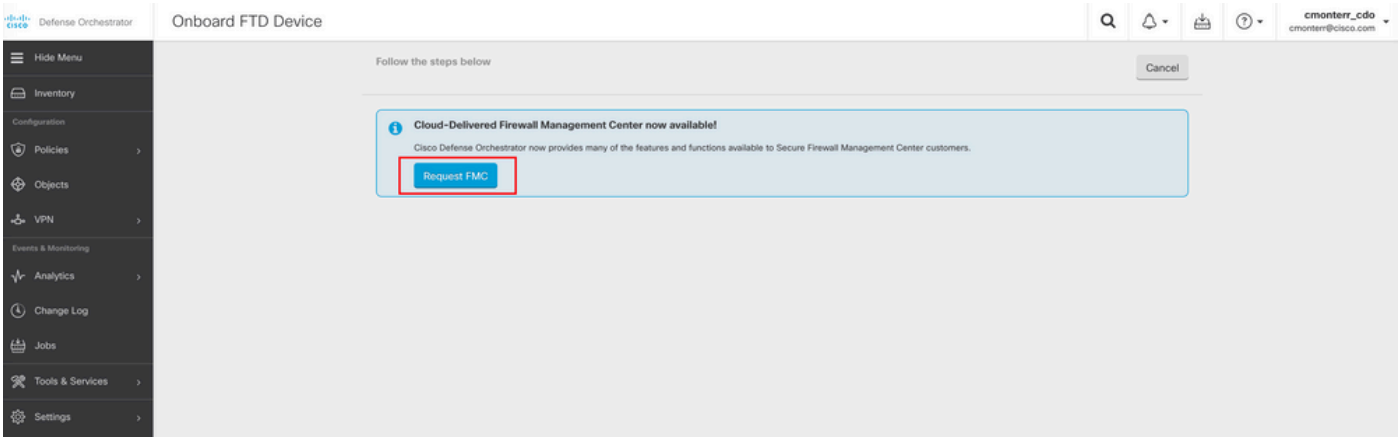
Navigieren Sie zunächst zu **Menu > Inventory** um ein neues Gerät hinzuzufügen.



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

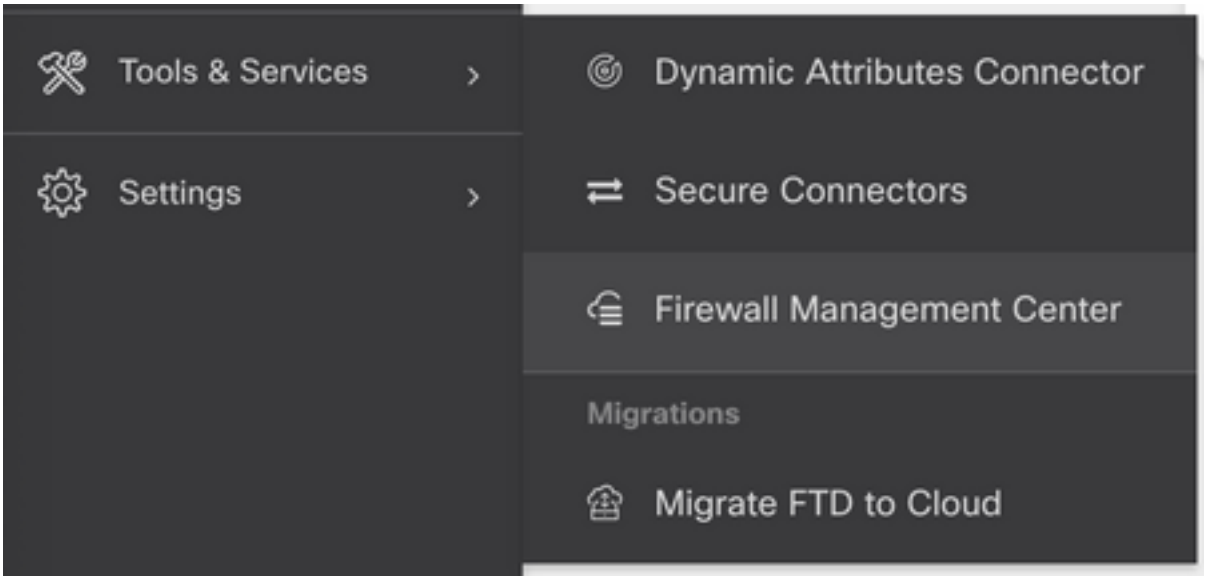


Auswählen **Request FMC** um das Cloud-basierte FirePOWER Management Center anzufordern.

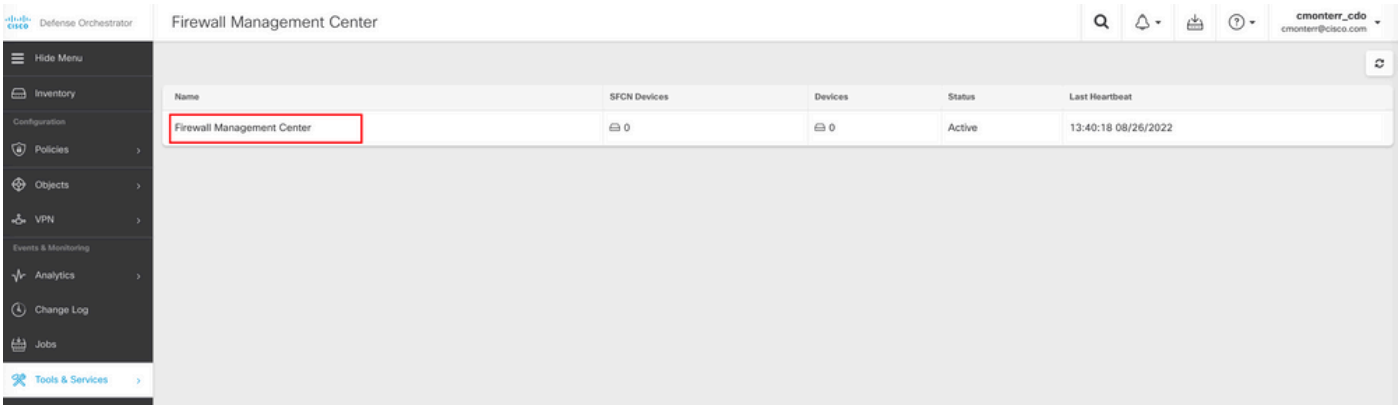


> **Hinweis**: Die Option "Request FMC" wird nur angezeigt, wenn im Tenant kein cdFMC vorhanden ist.

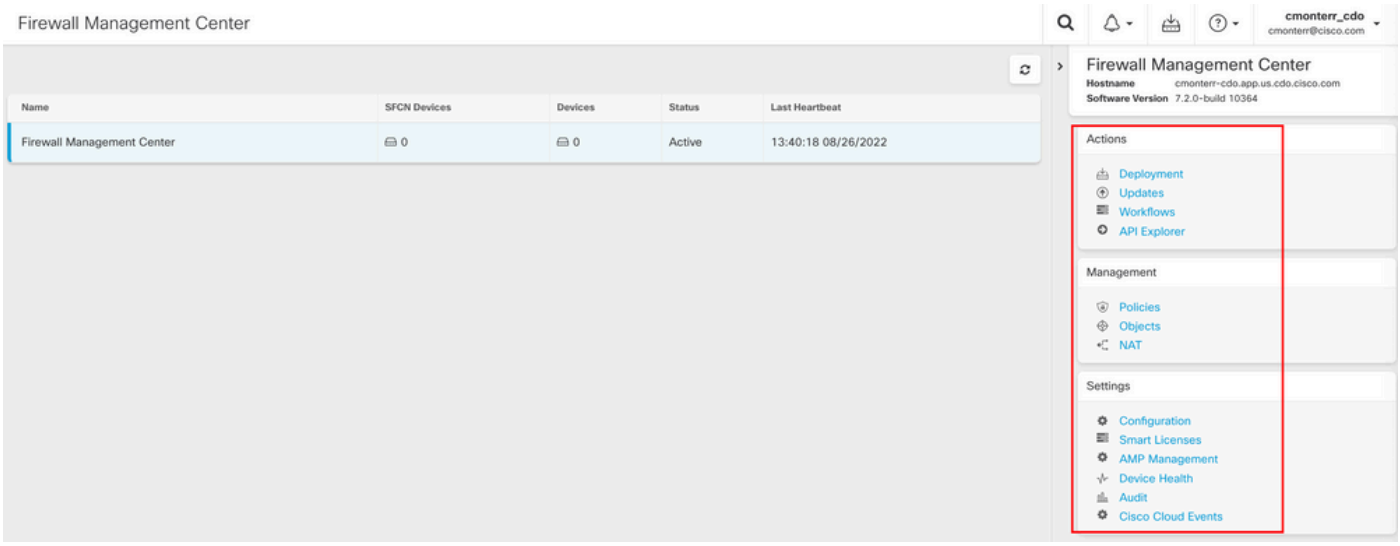
Navigieren Sie zu **Menu > Tools & Services > Firewall Management Center** wenn das cdFMC einsatzbereit ist.



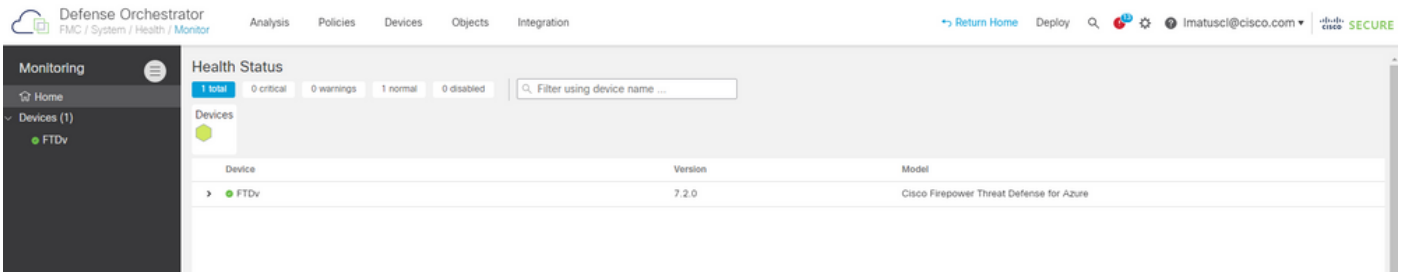
Wählen Sie das gewünschte cdFMC, um die cdFMC-Informationen anzuzeigen.



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



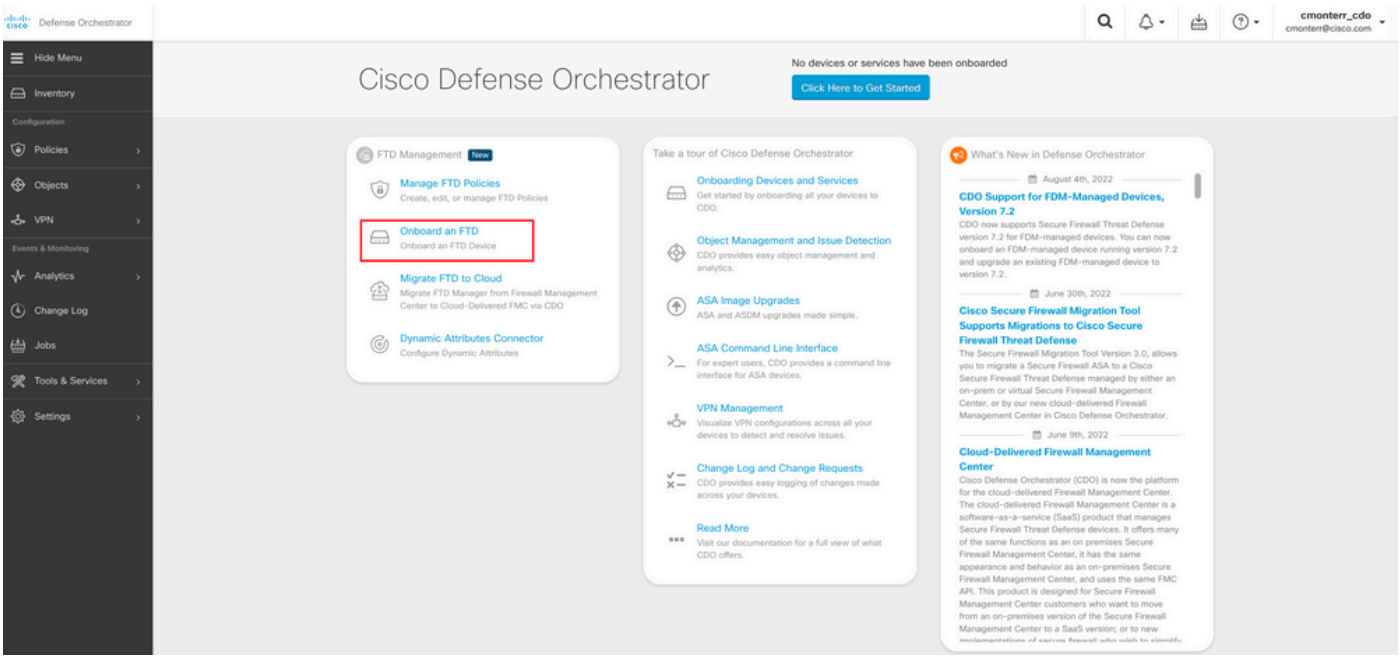
Nun sehen Sie die Benutzeroberfläche von cdFMC.



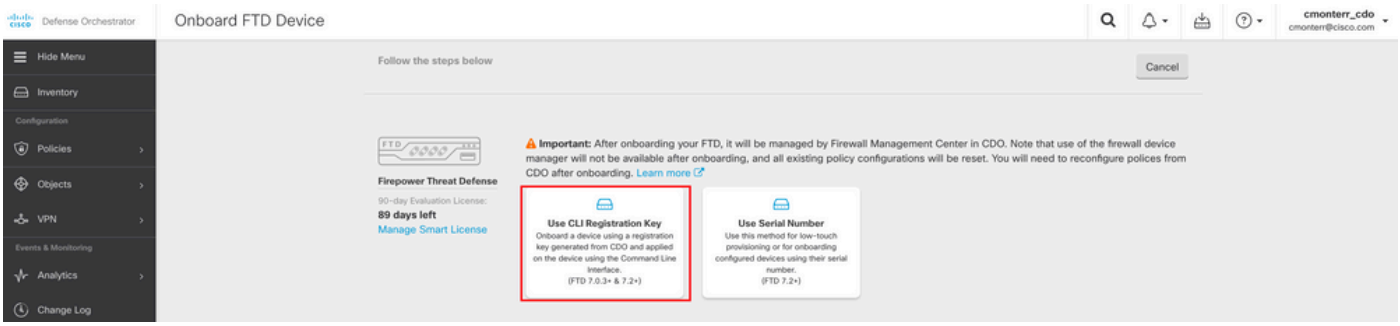
Integration einer FTD in einem Cloud-basierten FMC

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

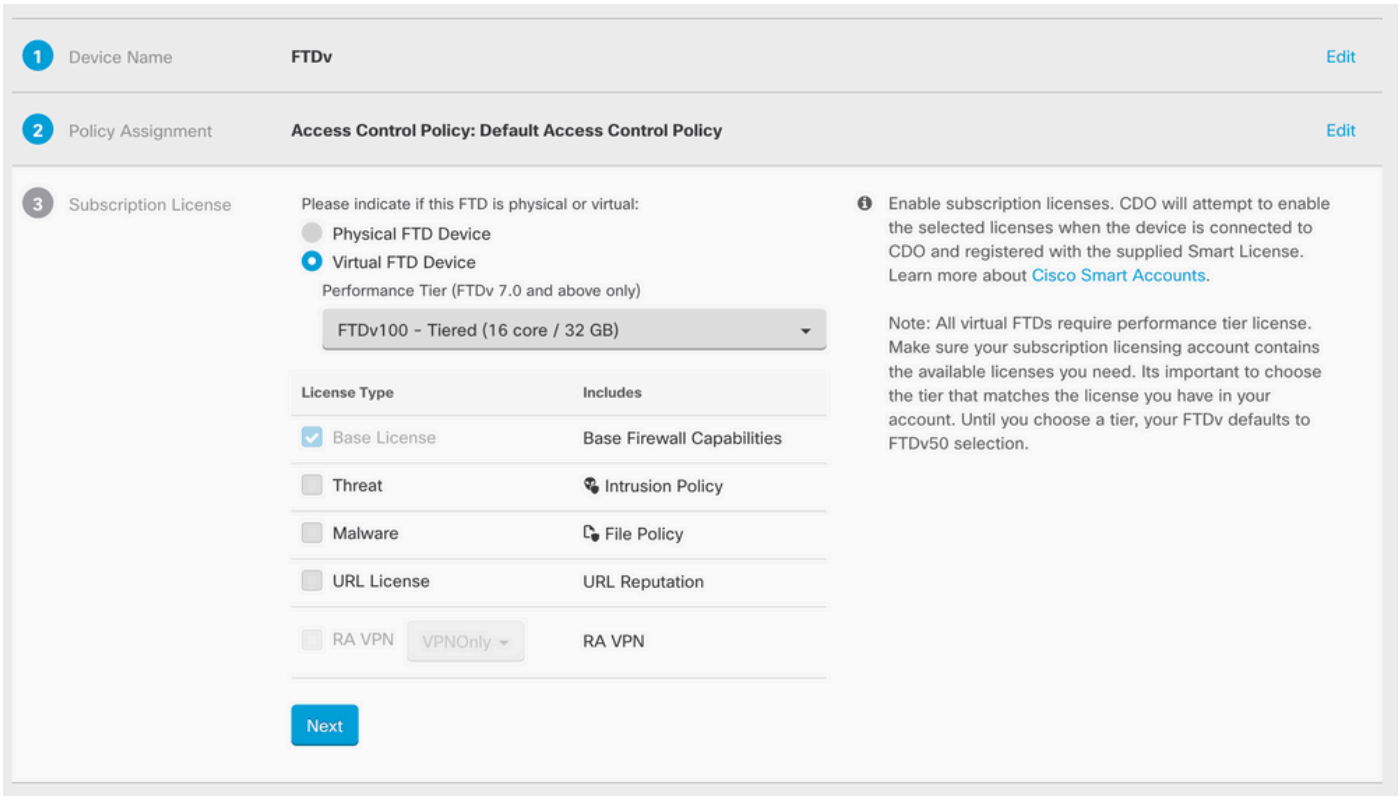
Wählen Sie zunächst **Onboard an FTD** auf der CDO-Startseite.



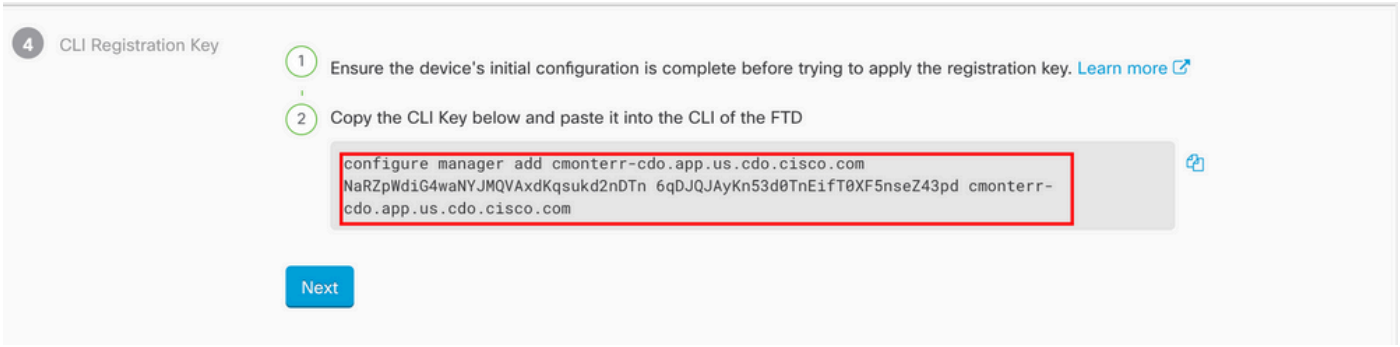
Wählen Sie anschließend die **Use CLI Registration Key** Option.



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



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



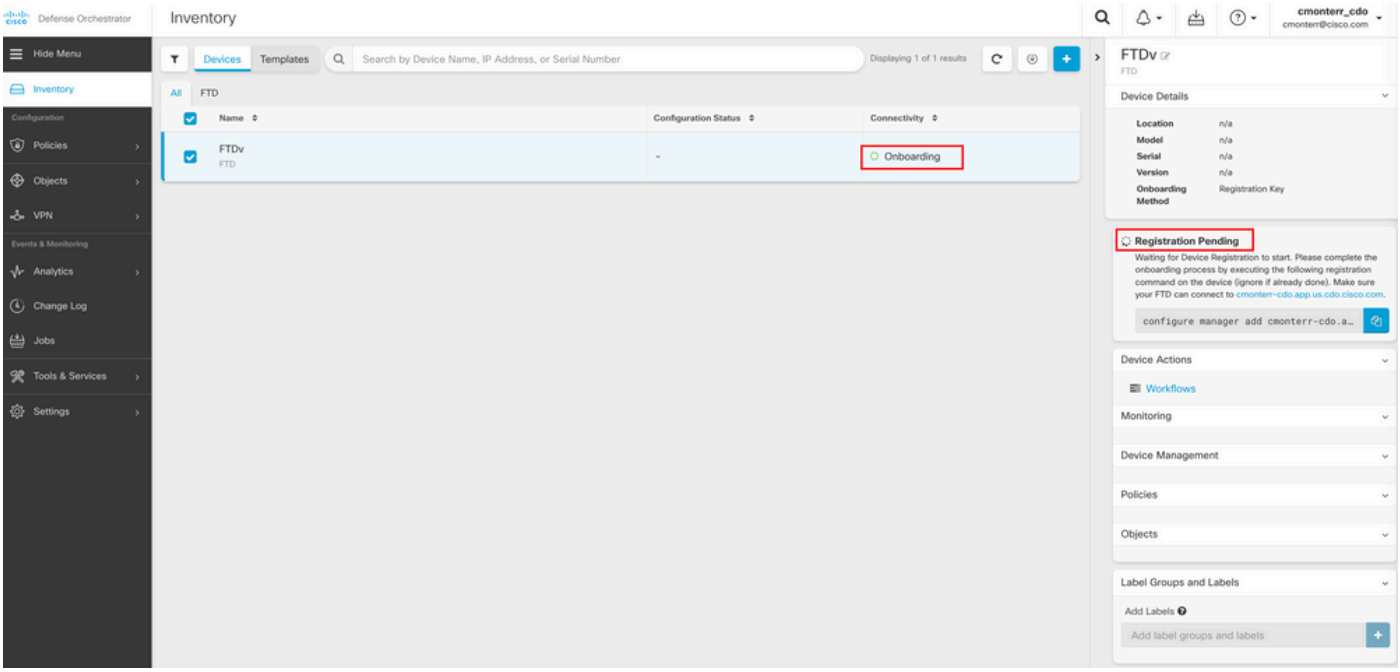
Kopieren Sie **CLI Key** in die CLI des verwalteten Geräts ein.

```
> 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
```

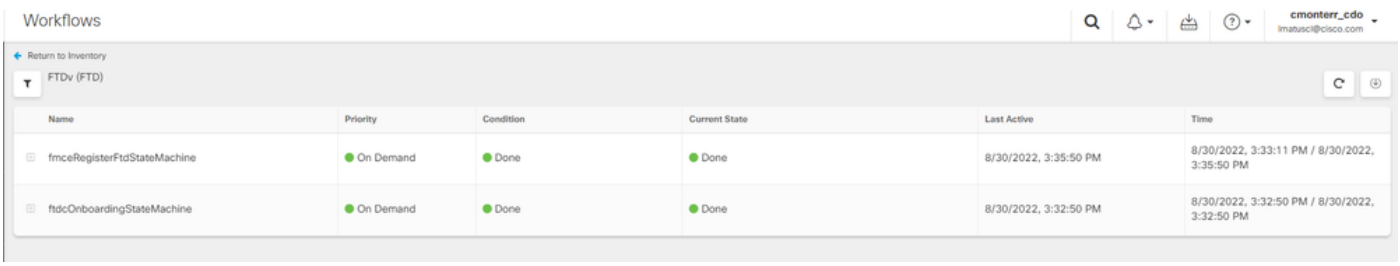
Das cdFMC initiiert eine Registrierungsaufgabe.



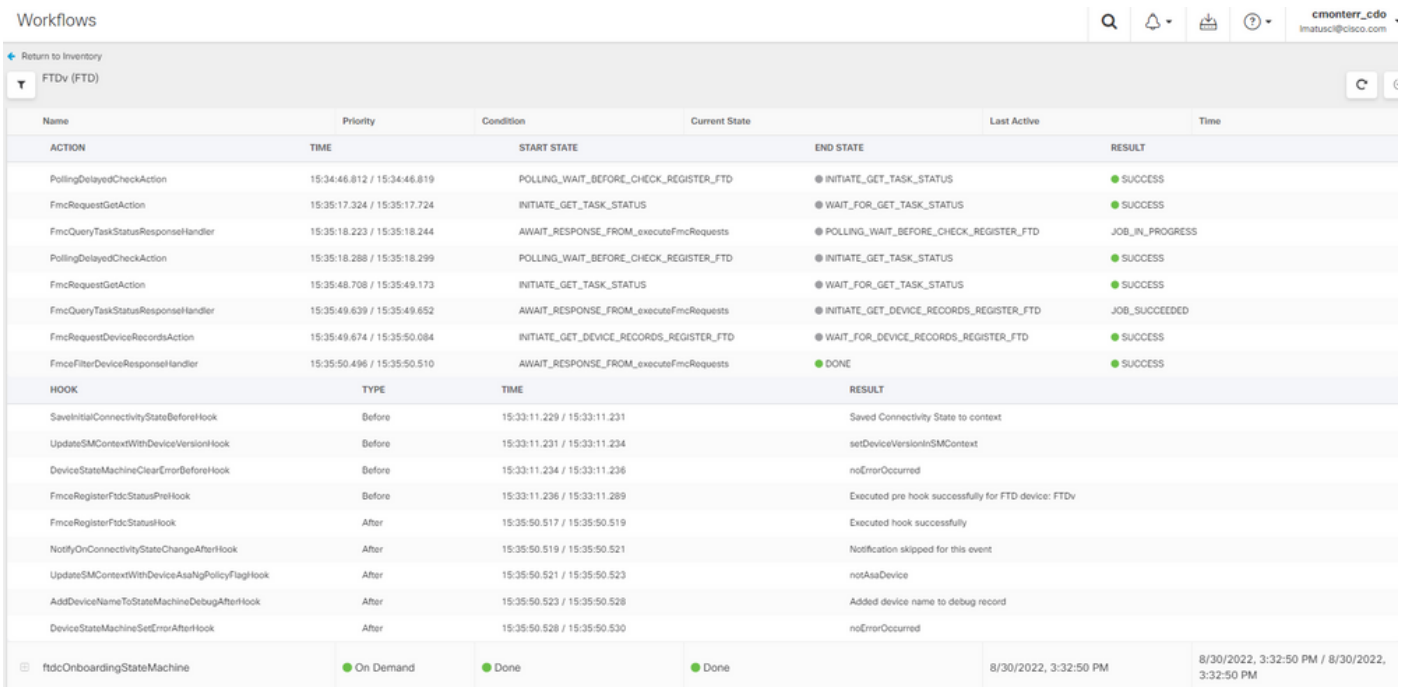
Hinweis: Stellen Sie sicher, dass Ihr FTD-Gerät über die Ports 8305 (Sftunnel) und 443 mit dem CDO-Tenant kommuniziert, um den Registrierungsprozess abzuschließen. Lesen Sie die vollständigen Netzwerkanforderungen.

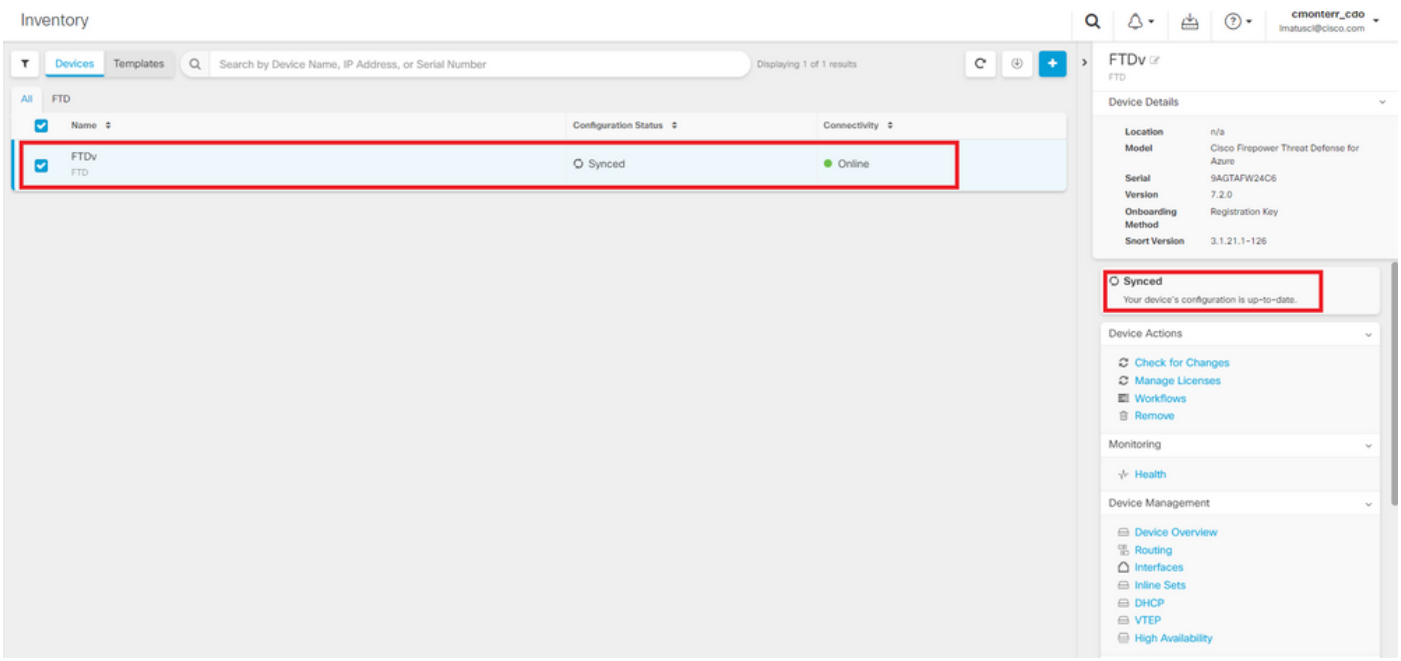
Hinweis: Wenn Sie keine Verbindung zum Host herstellen können, können Sie die DNS-Konfiguration in der FTD-CLI mit dem folgenden Befehl korrigieren: **configure network dns <Adresse>**.

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

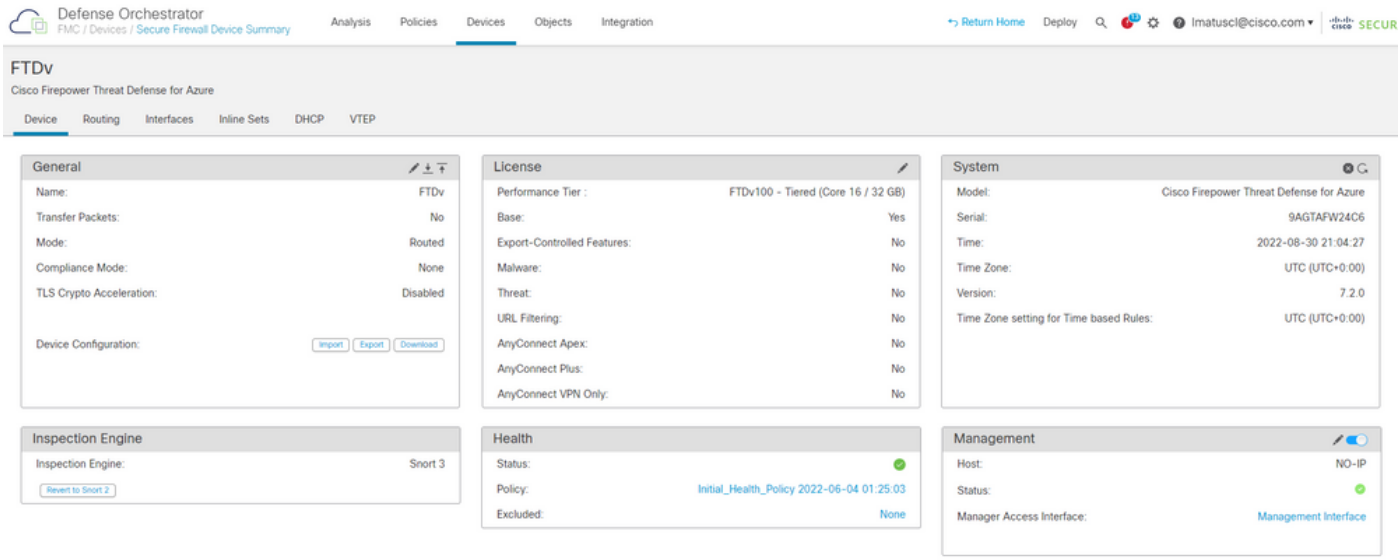


Erweitern Sie die **Active** angeben, um zusätzliche Informationen zu erhalten, zeigen diese Bilder, wie die FTDv erfolgreich registriert wurde.





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



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.