Implementazione di un CFC (Cloud-Delivered FMC) in Cisco Defense Orchestrator (CDO)

Sommario

Introduzione

Questo documento descrive il processo di installazione e onboard di un CCP fornito tramite cloud sulla piattaforma CDO.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- cdFMC 7.2.0
- FTDv 7.2.0

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Cisco Defense Orchestrator (CDO) è la piattaforma per il centro di gestione dei firewall (cdFMC) distribuito nel cloud. Il centro di gestione dei firewall distribuito tramite cloud è un prodotto SaaS (Software-as-a-Service) che gestisce i dispositivi Secure Firewall Threat Defense. Offre molte delle stesse funzioni di una difesa contro le minacce Secure Firewall on-premises. Ha lo stesso aspetto e comportamento di un Centro di gestione Secure Firewall locale e utilizza la stessa API (Application Programming Interface) di FMC.

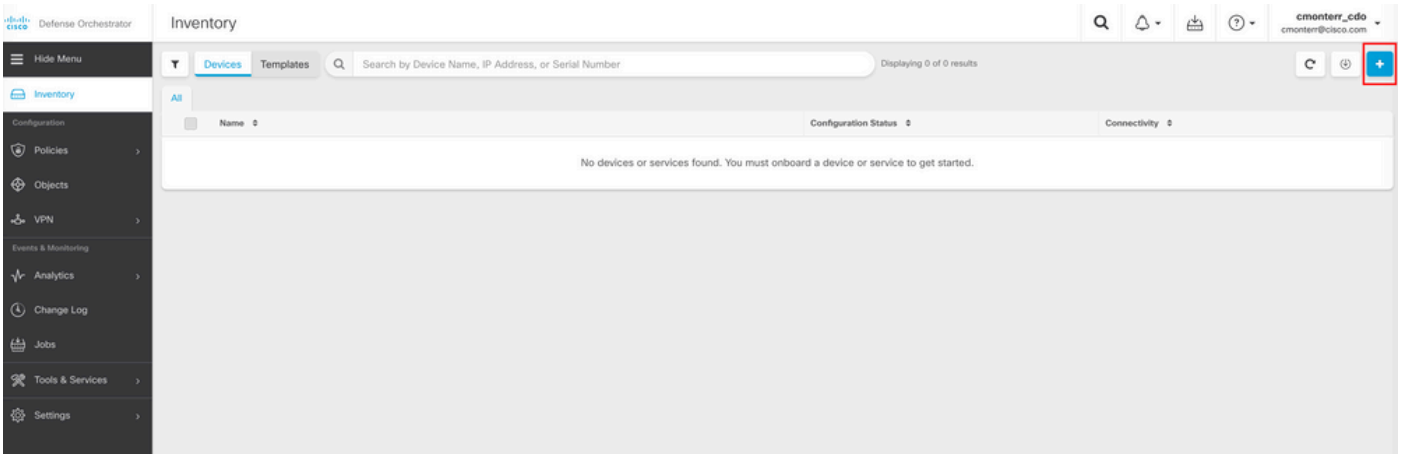
Questo prodotto è progettato per la migrazione dai Secure Firewall Management Center locali alla versione SaaS di Secure Firewall Management Center.

Configurazione

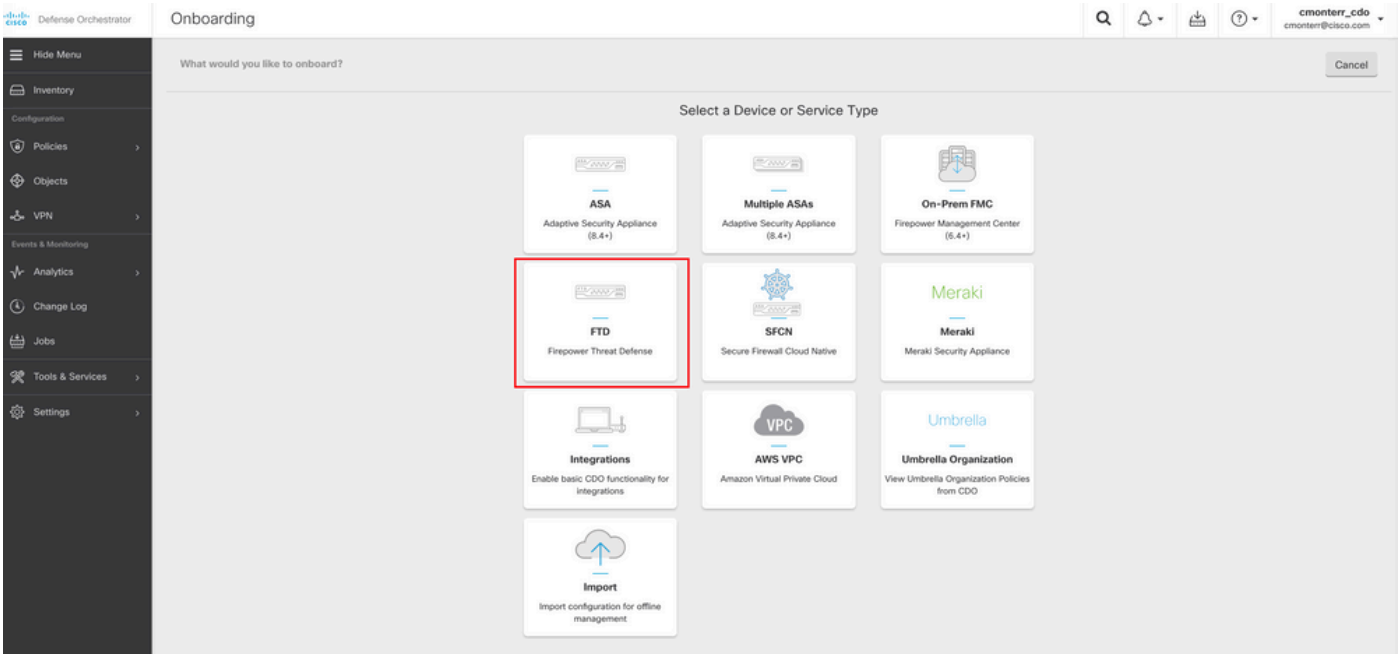
Distribuire un Firepower Management Center distribuito tramite cloud su CDO.

Queste immagini mostrano il processo di configurazione iniziale necessario per installare un FMC distribuito tramite cloud su CDO.

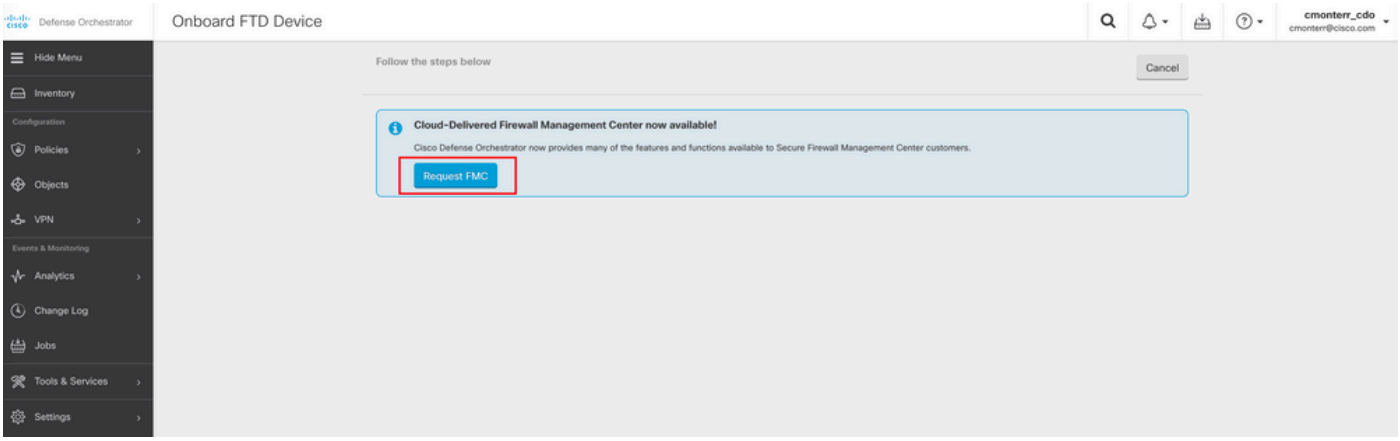
Innanzitutto, passare a **Menu > Inventory** per aggiungere una nuova periferica.



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

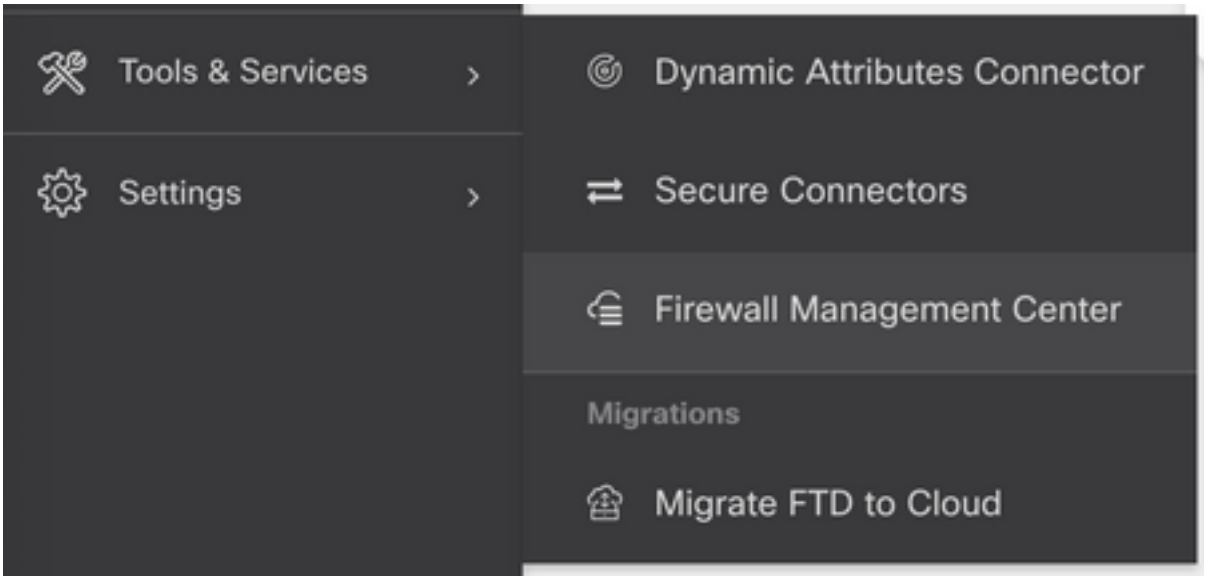


Seleziona **Request FMC** per richiedere il Cloud-Delivered Firepower Management Center.

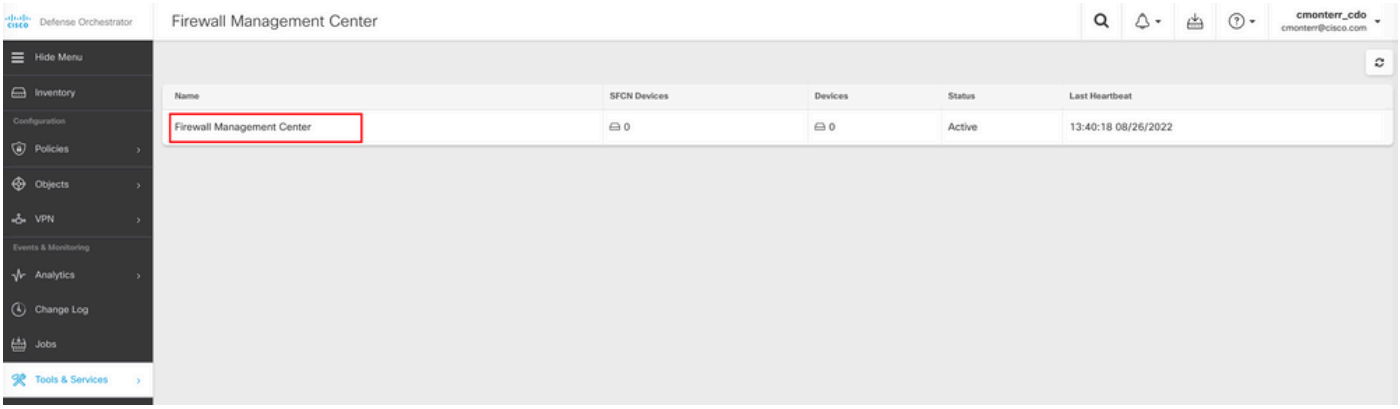


> **Nota**: l'opzione "Request FMC" (Richiedi FMC) viene visualizzata solo se nel tenant non è presente alcun cdFMC.

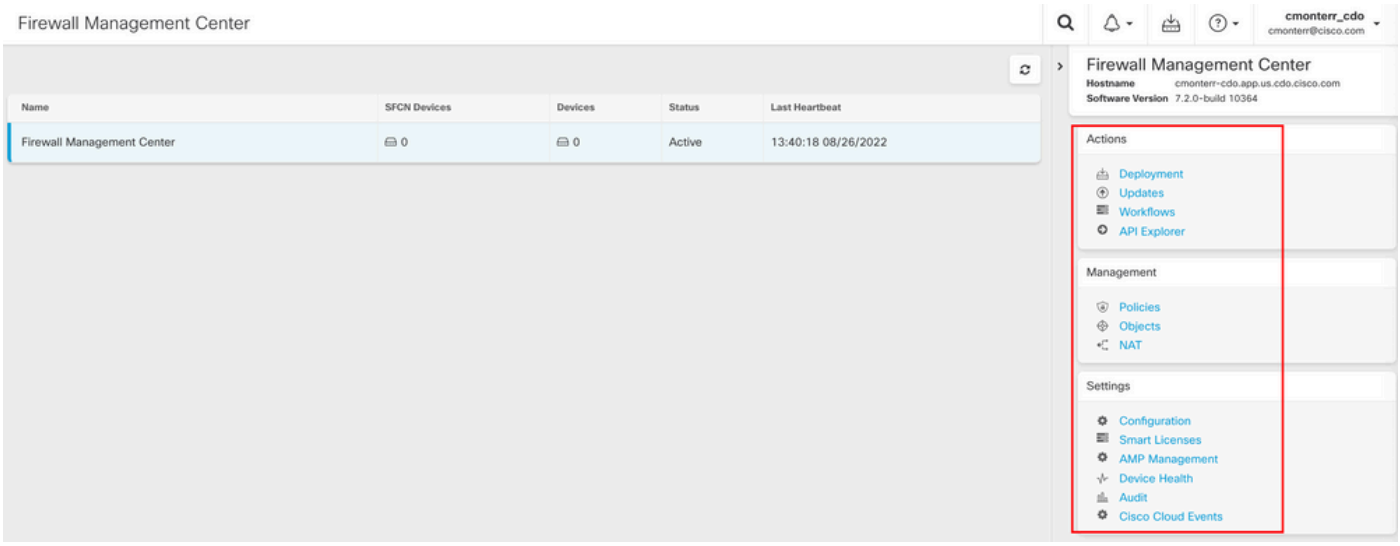
Passa a **Menu > Tools & Services > Firewall Management Center** quando il cdFMC è pronto per l'uso.



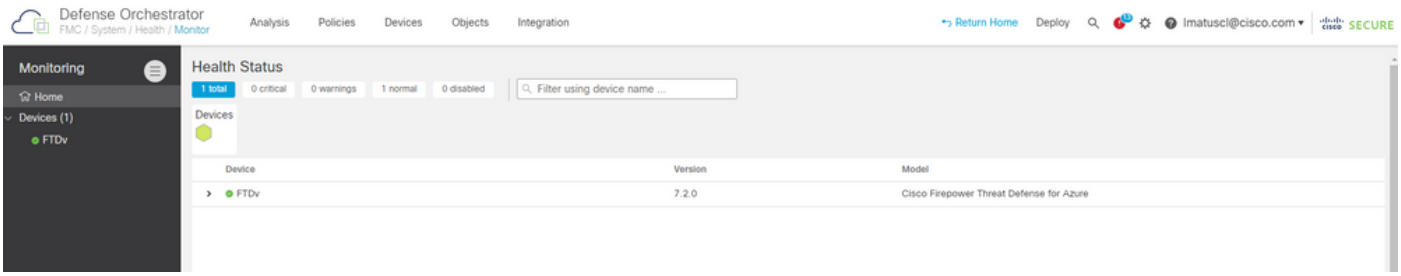
Selezionare il cdFMC desiderato per visualizzare le informazioni sul cdFMC.



Per accedere all'interfaccia grafica dell'utente (GUI) di cdFMC, selezionare una delle opzioni disponibili sul lato destro.



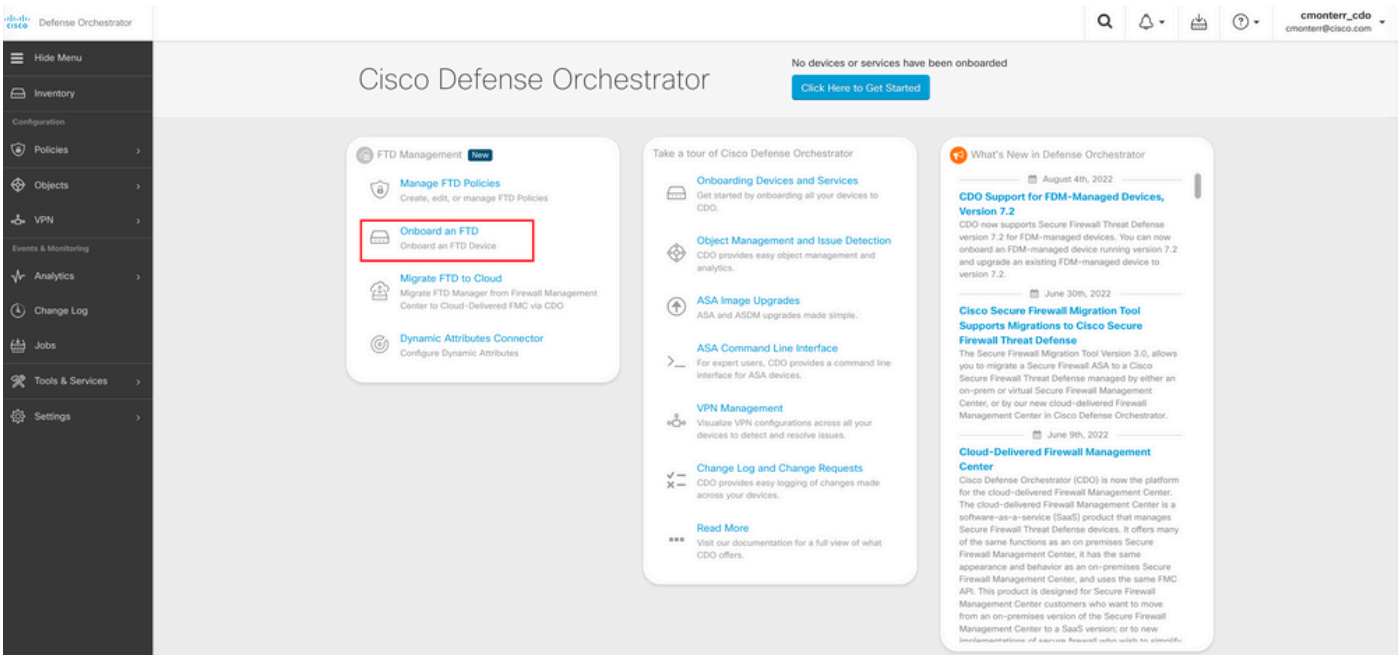
Ora è possibile vedere l'interfaccia utente di cdFMC.



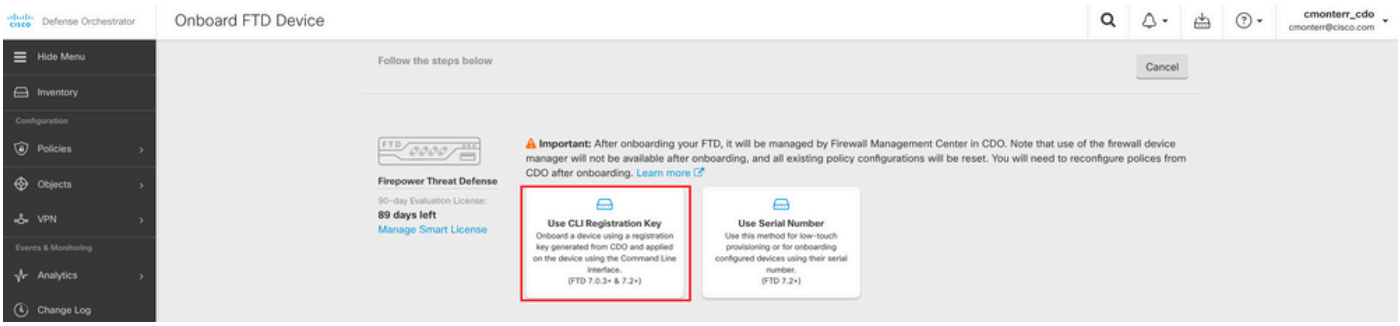
Integrazione di un FTD su un FMC fornito tramite cloud

Nelle immagini viene mostrato come integrare un FTD per la registrazione su un CdFMC con una chiave di registrazione CLI (Command Line Interface).

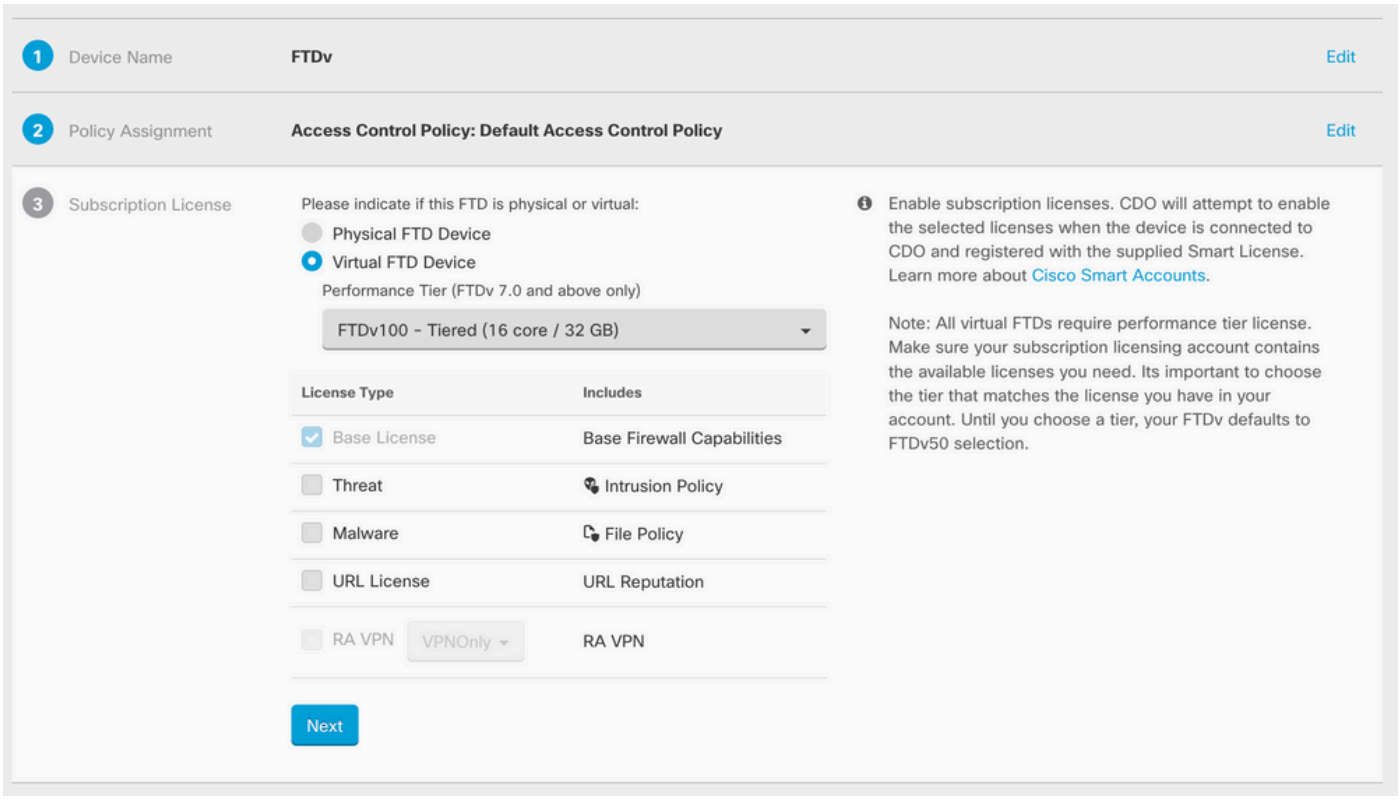
Selezionare innanzitutto **Onboard an FTD** nella home page CDO.



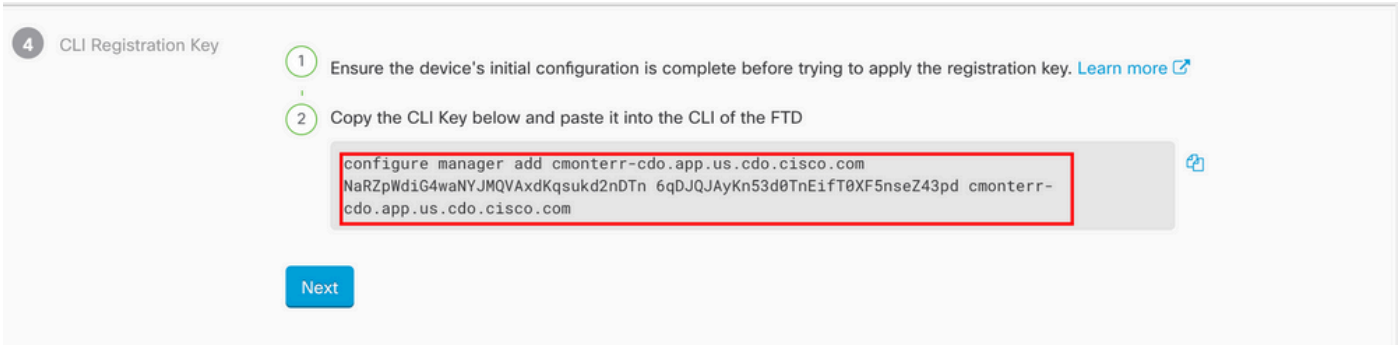
Quindi, selezionare **Use CLI Registration Key** opzione.



Procedere per immettere le informazioni FTDv richieste e desiderate.



Infine, il CdFMC crea un **CLI Key**Chiave CLI per il dispositivo.



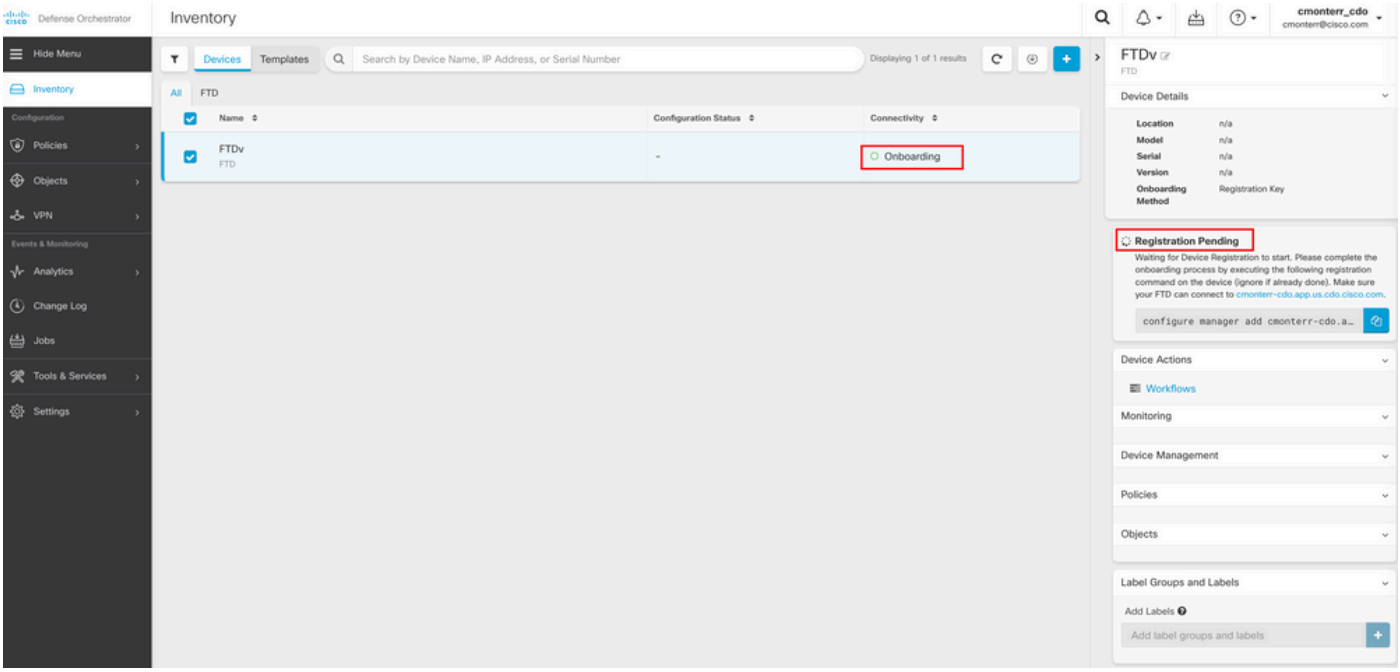
Copiare **CLI Key** nella CLI del dispositivo gestito.

```
> 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
```

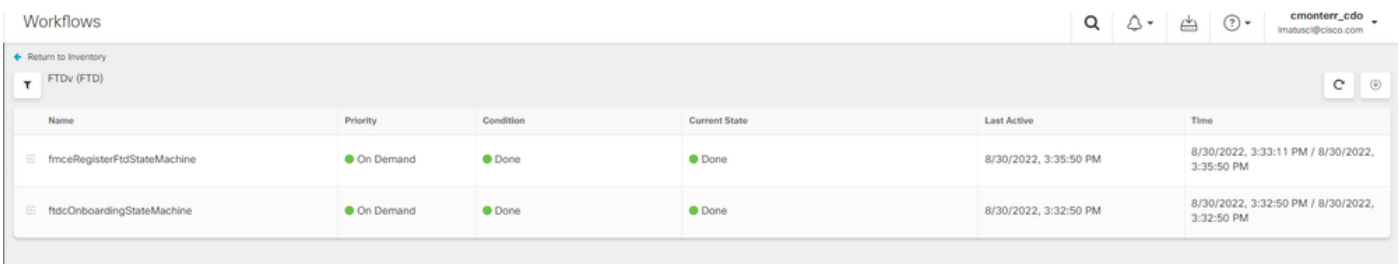
CdFMC avvia un'attività di registrazione.



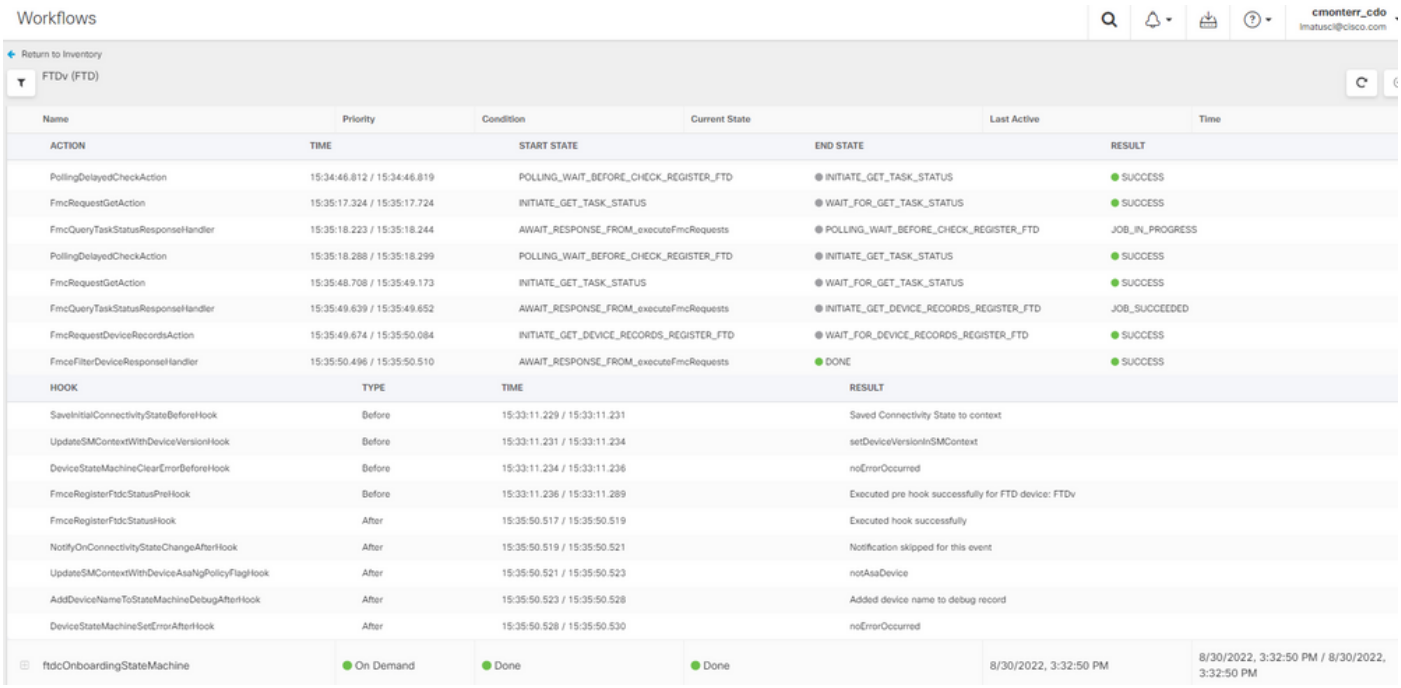
Nota: per completare il processo di registrazione, verificare che il dispositivo FTD in uso abbia la comunicazione sulle porte 8305 (sftunnel) e 443 al tenant CDO. Consultare i requisiti di rete completi.

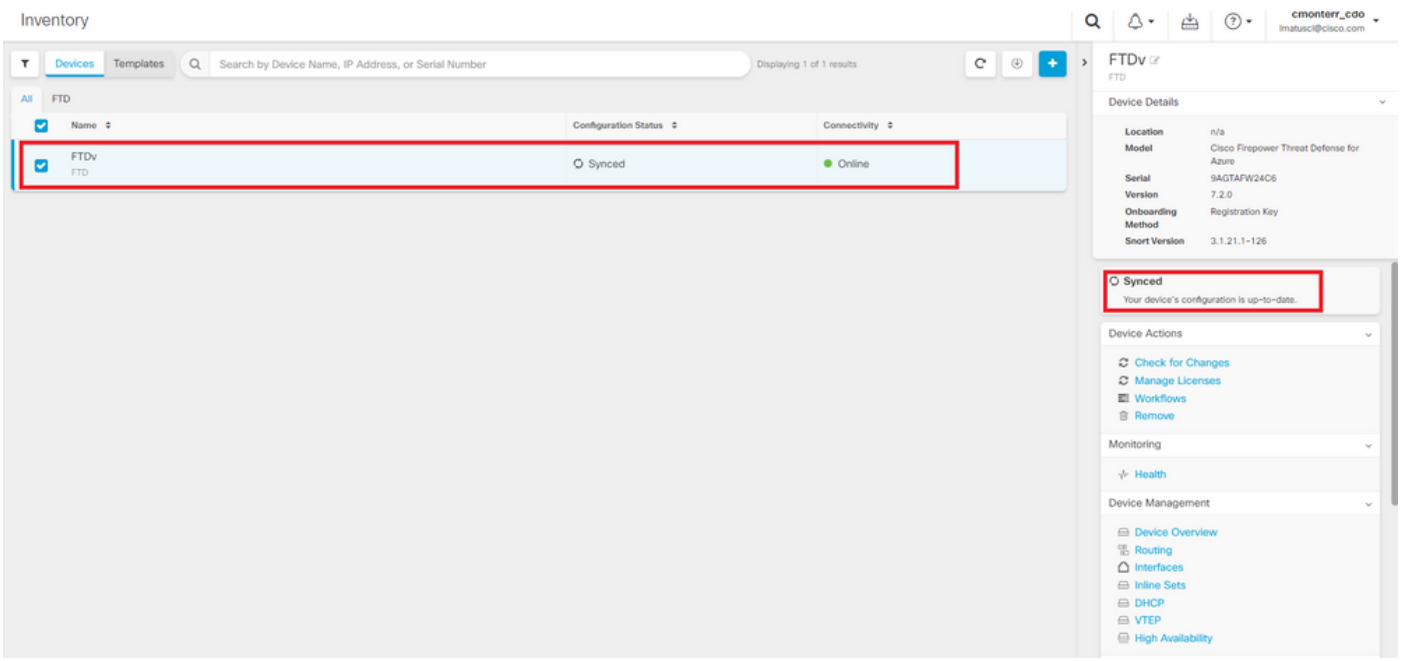
Nota: se non è possibile connettersi all'host, è possibile rettificare la configurazione DNS nell'FTD-CLI con questo comando: **configure network dns <indirizzo>**.

Per monitorare il processo di registrazione, passare a **Device Actions > Workflows.**.

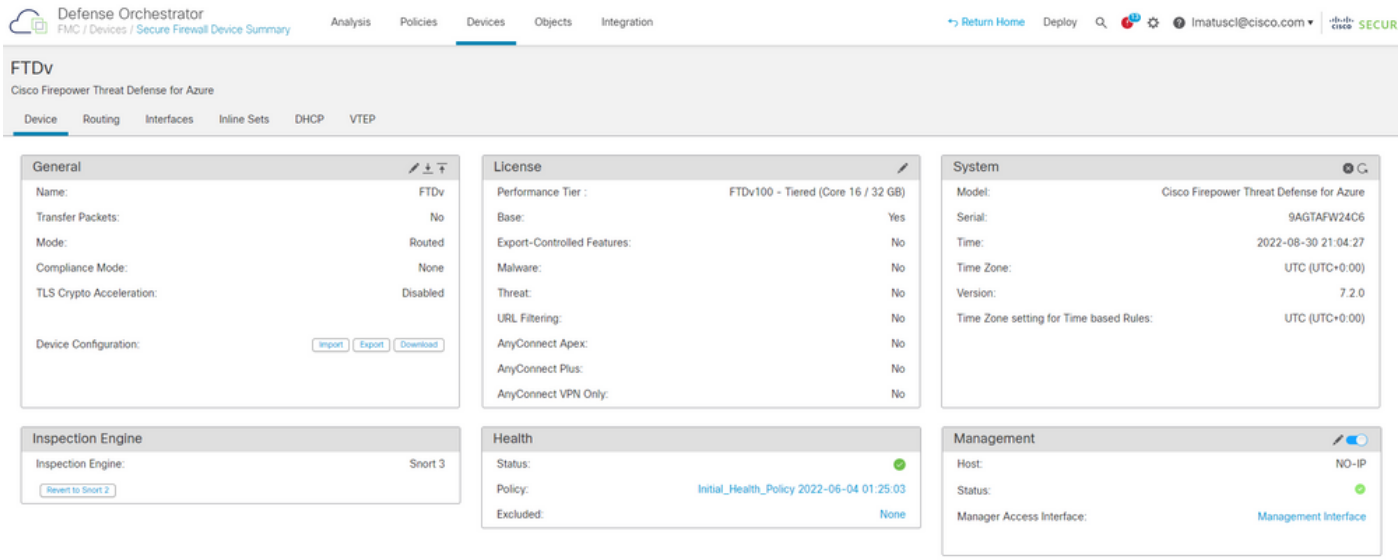


Espandere la **Active** per avere ulteriori informazioni, queste immagini mostrano come l'FTDv è stato registrato correttamente.





Infine, passare a **Device Management > Device Overview** per accedere a cdFMC e rivedere lo stato della panoramica FTDv.



Informazioni correlate

- [Documentazione e supporto tecnico – Cisco Systems]
- [Gestione dei dispositivi Cisco Secure Firewall Threat Defense con Cloud Management Center]

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).