Déployer un contrôleur FMC fourni dans le cloud (cdFMC) dans Cisco Defense Orchestrator (CDO)

Table des matières

Introduction

Ce document décrit le processus de déploiement et d'intégration de FMC fourni dans le cloud sur la plate-forme CDO.

Conditions préalables

Exigences

Cisco recommande de connaître les sujets suivants :

- Centre de gestion Firepower (cdFMC) fourni dans le cloud
- Cisco Defense Orchestrator (CDO)
- Protection virtuelle contre les menaces Firepower (FTDv)

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- cdFMC 7.2.0
- FTDv 7.2.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Cisco Defense Orchestrator (CDO) est la plate-forme du centre de gestion des pare-feu (CdFMC) fourni dans le cloud. Le Centre de gestion des pare-feu, fourni dans le cloud, est un produit SaaS (Software-as-a-Service) qui gère les périphériques Secure Firewall Threat Defense. Il offre un grand nombre des mêmes fonctions qu'un pare-feu sécurisé sur site, Secure Firewall Threat Defense. Il a le même aspect et le même comportement qu'un centre de gestion de pare-feu sécurisé sur site et utilise la même interface de programmation d'application (API) FMC.

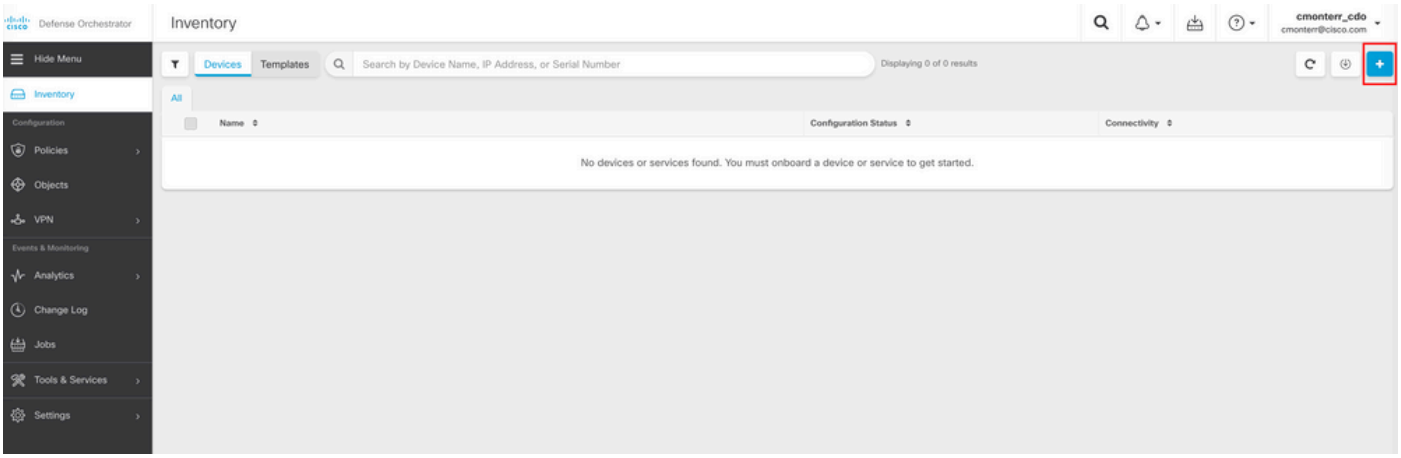
Ce produit est conçu pour la migration des centres de gestion de pare-feu sécurisés sur site vers la version SaaS du centre de gestion de pare-feu sécurisé.

Configurer

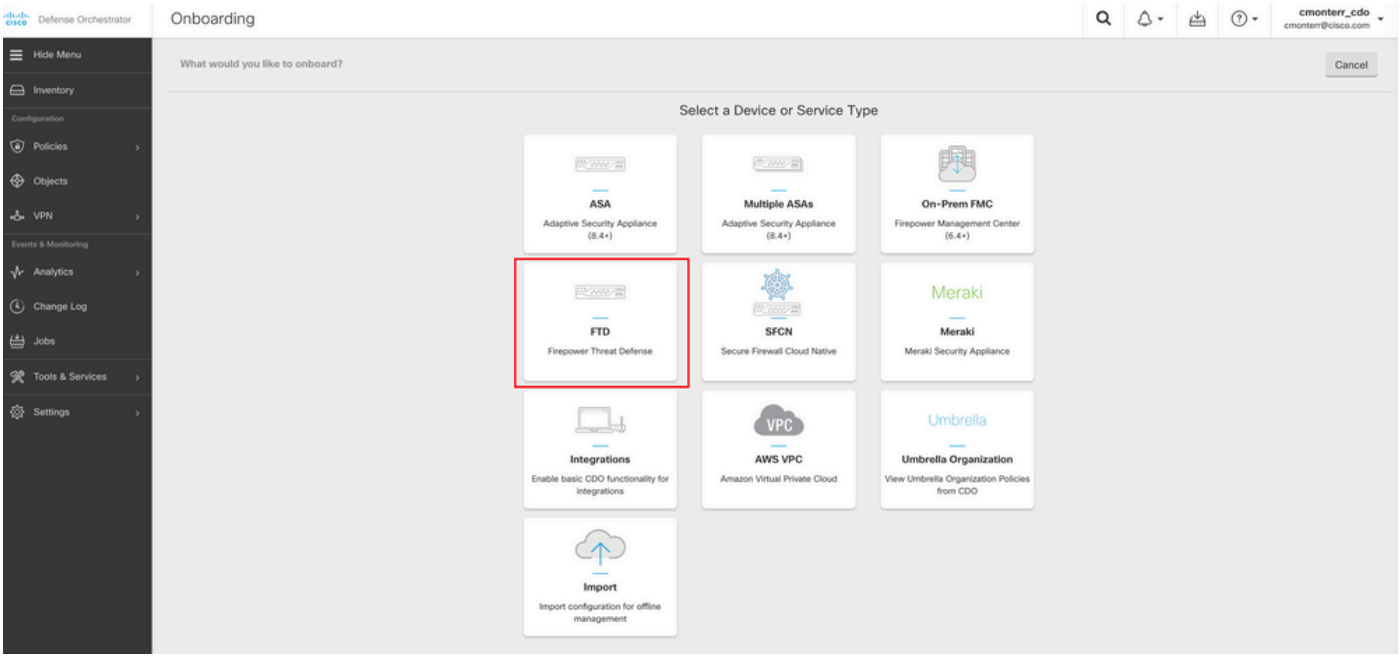
Déployez un centre de gestion Firepower fourni dans le cloud sur CDO.

Ces images montrent le processus de configuration initiale nécessaire pour déployer un FMC fourni dans le cloud sur CDO.

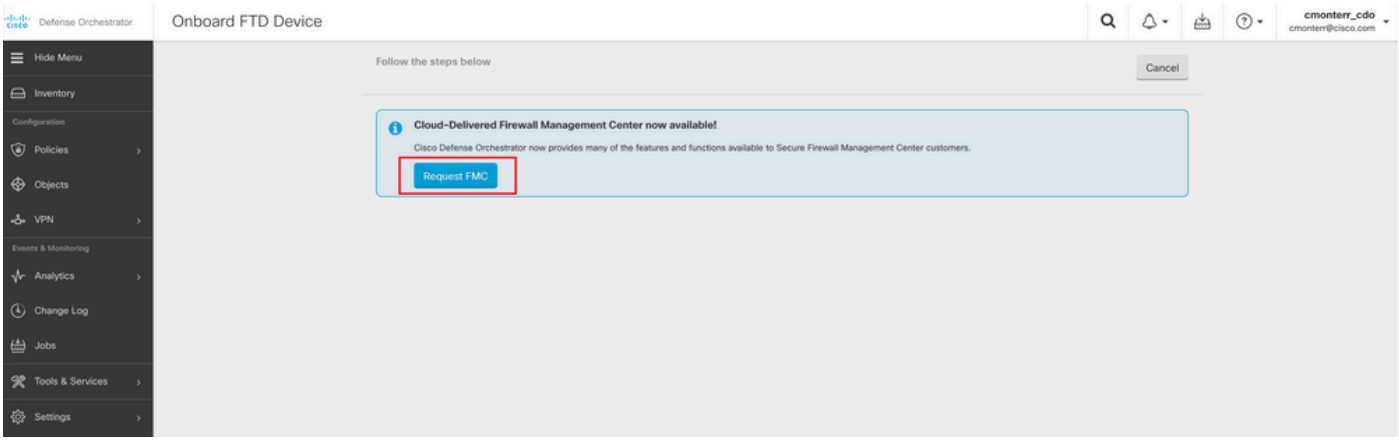
Tout d'abord, accédez à **Menu > Inventory** afin d'ajouter un nouveau périphérique.



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

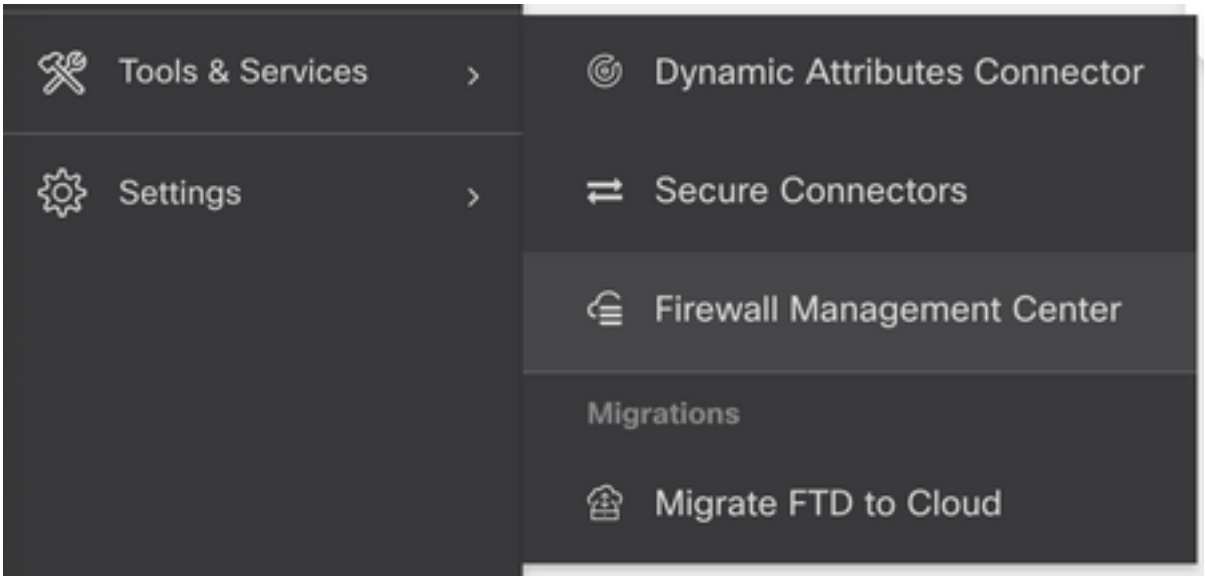


Sélectionner **Request FMC** afin de demander le centre de gestion Firepower fourni dans le cloud.

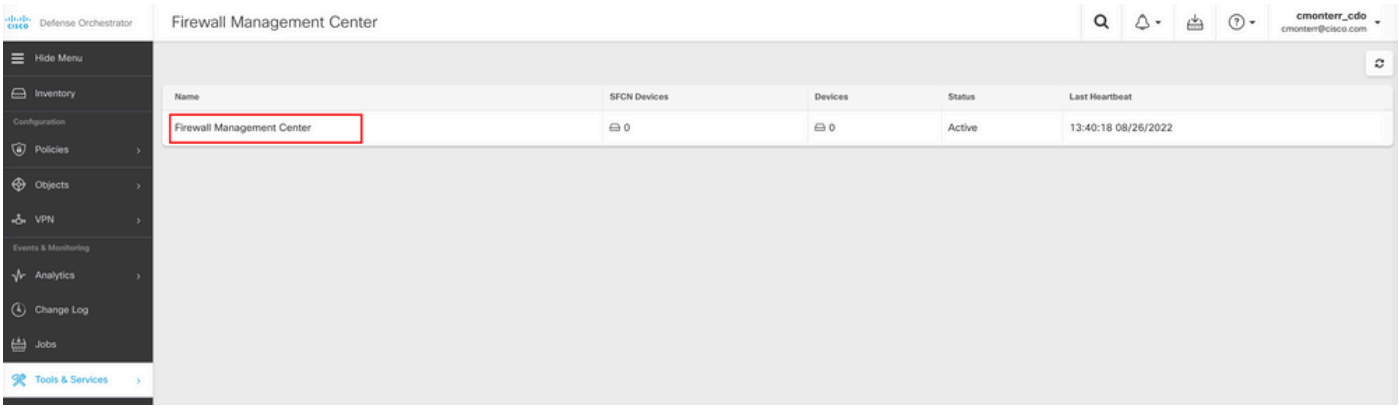


> **Remarque** : l'option « Request FMC » (Demander FMC) n'est présentée que si vous n'avez aucun cdFMC dans le service partagé.

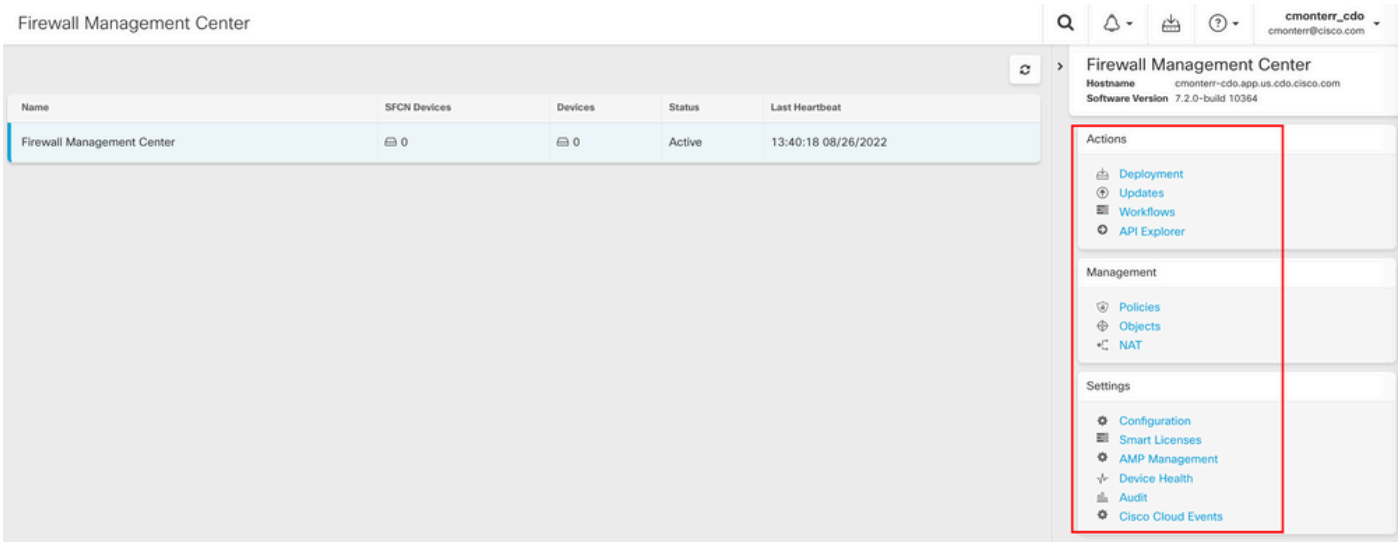
Naviguez jusqu'à **Menu > Tools & Services > Firewall Management Center** lorsque le cdFMC est prêt à être utilisé.



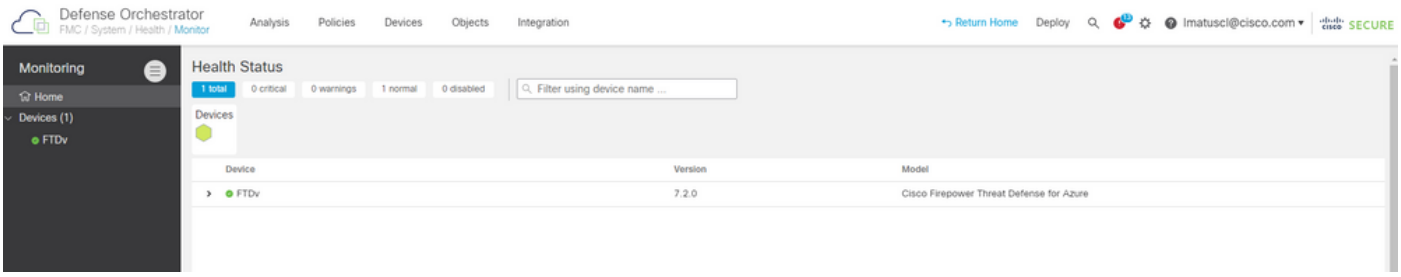
Sélectionnez le cdFMC souhaité pour afficher les informations du cdFMC.



Afin d'accéder à l'interface graphique utilisateur (GUI) du cdFMC, sélectionnez l'une des options disponibles sur le côté droit.



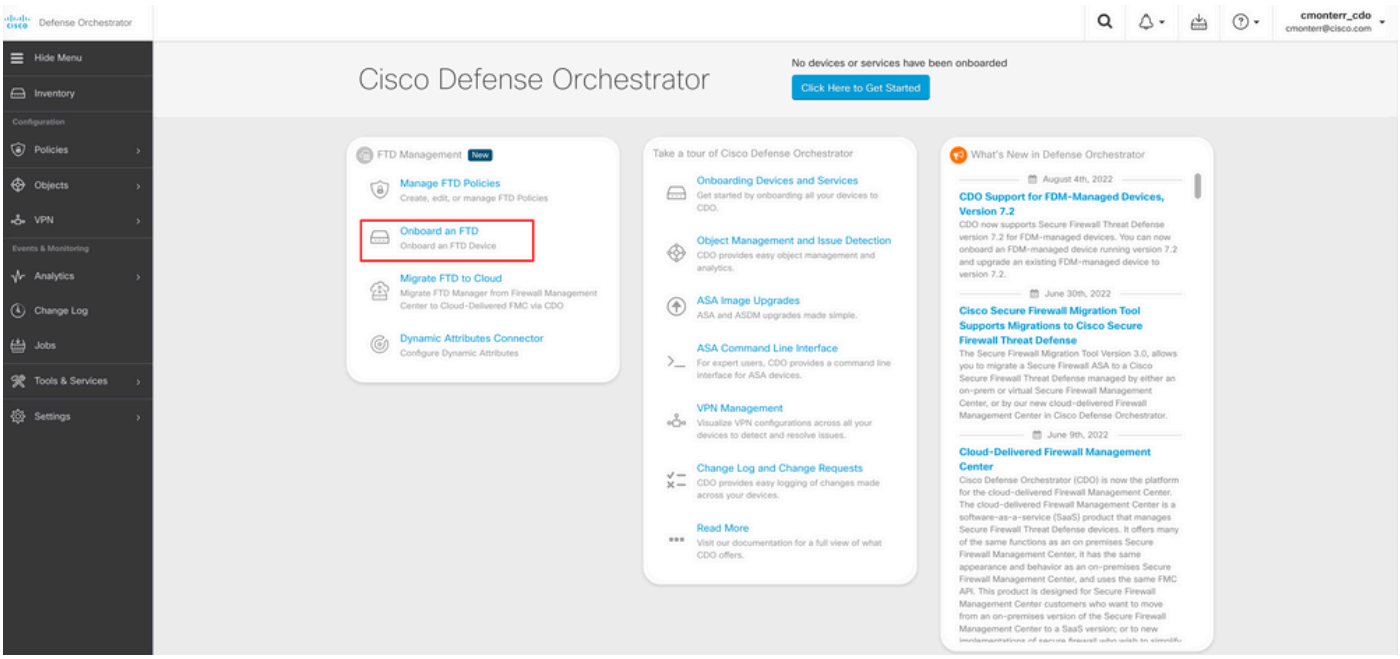
Vous pouvez maintenant voir l'interface graphique utilisateur de cdFMC.



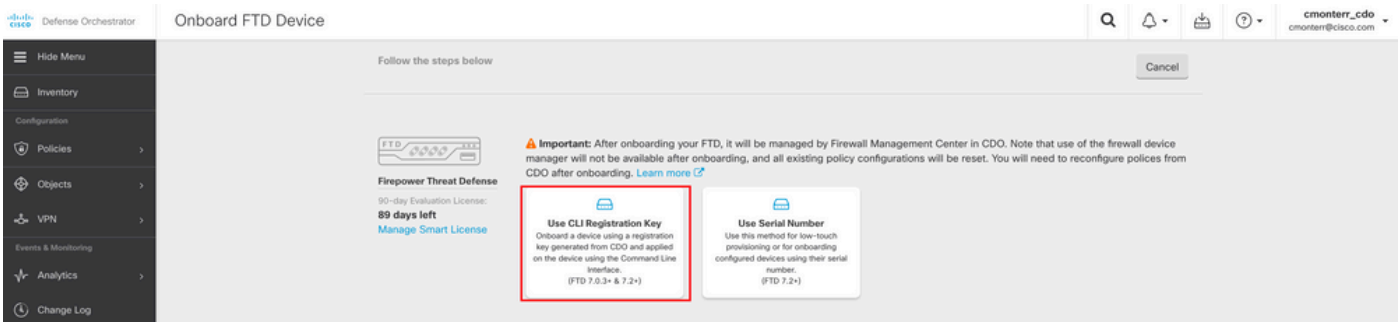
Intégration d'un FTD sur un FMC fourni dans le cloud

Ces images montrent comment intégrer un FTD afin d'être enregistré sur un cdFMC avec une clé d'enregistrement de l'interface de ligne de commande (CLI).

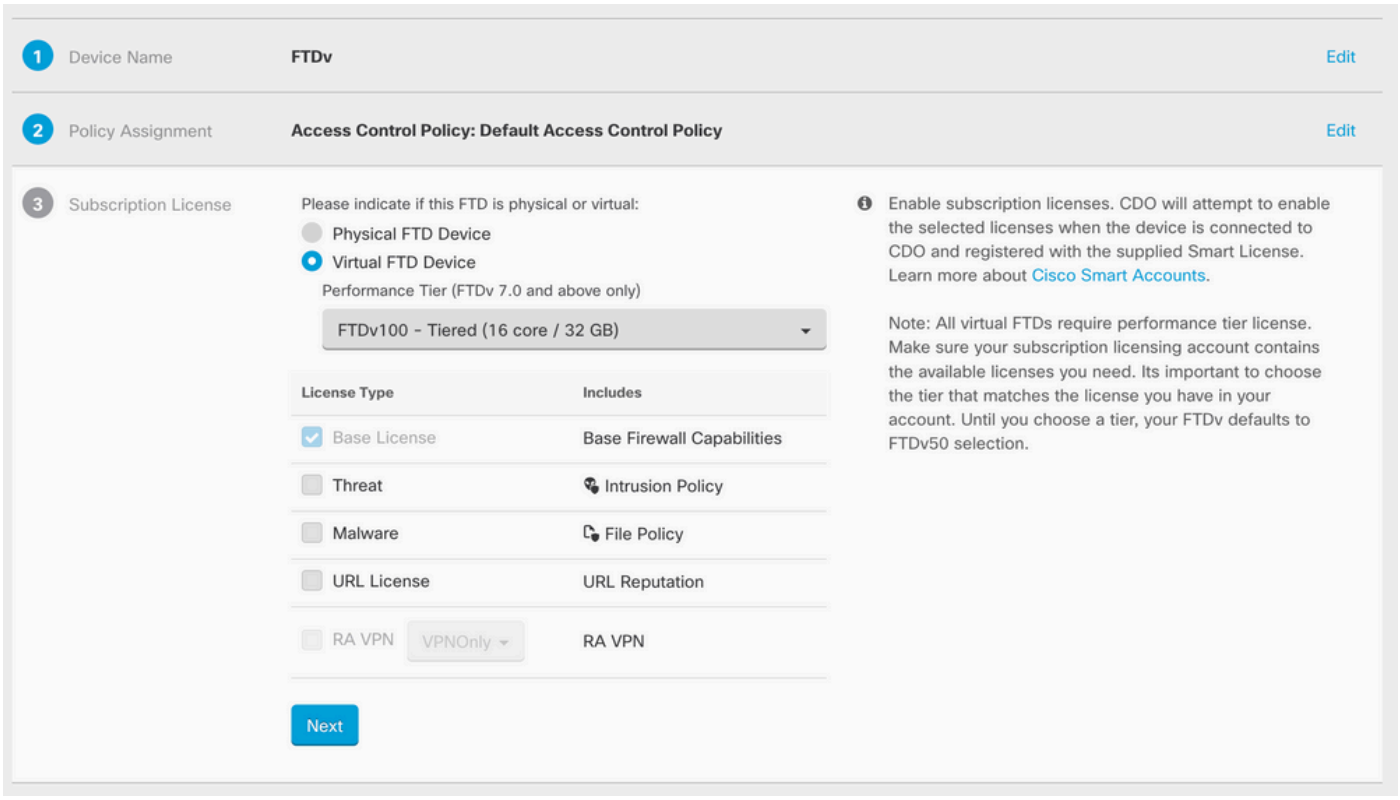
Sélectionnez d'abord **Onboard an FTD** sur la page d'accueil de CDO.



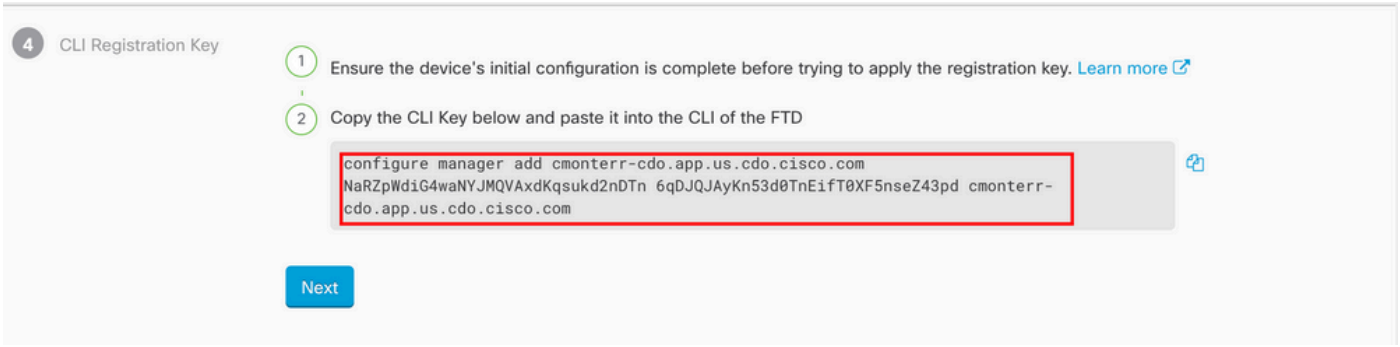
Sélectionnez ensuite l'option **Use CLI Registration Key** de l'assistant.



Saisissez les informations FTDv requises et souhaitées.



Enfin, le cdFMC crée un **CLI Key**Clé CLI de votre périphérique.



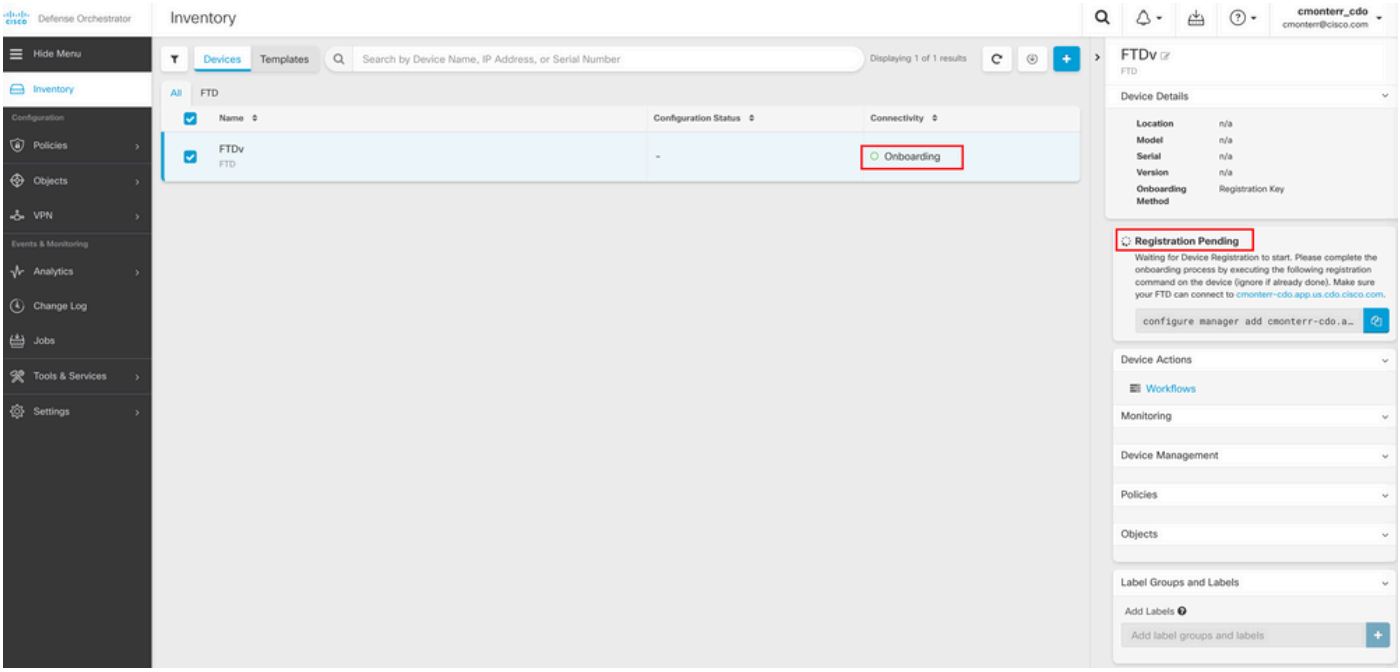
Copiez le **CLI Key** dans l'interface de ligne de commande de votre périphérique géré.

```
> 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
```

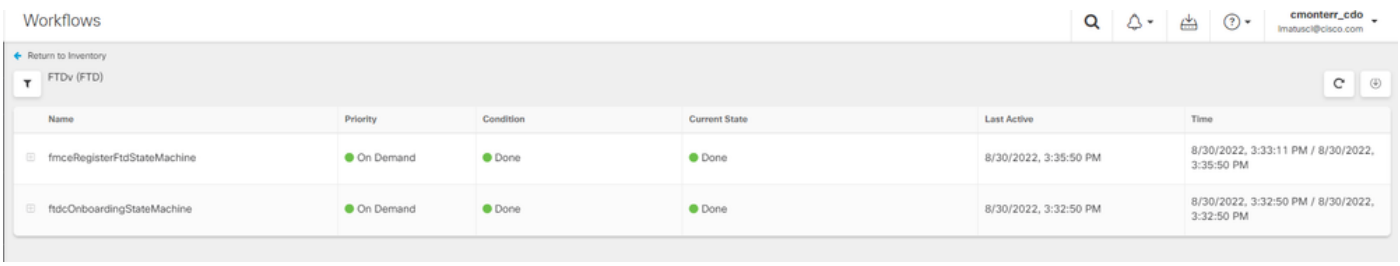
Le cdFMC lance une tâche d'enregistrement.



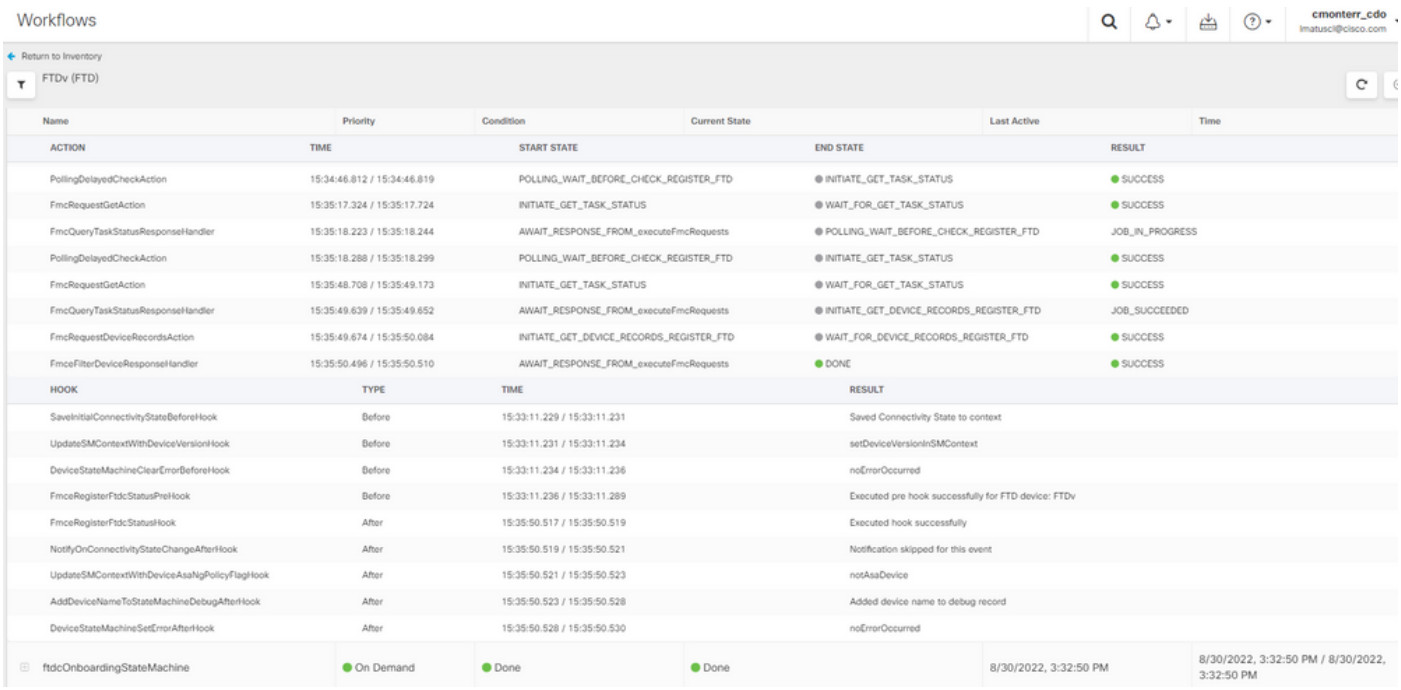
Remarque : assurez-vous que votre périphérique FTD communique avec le locataire CDO via les ports 8305 (sftunnel) et 443 afin de terminer le processus d'enregistrement. Consultez la configuration réseau requise complète.

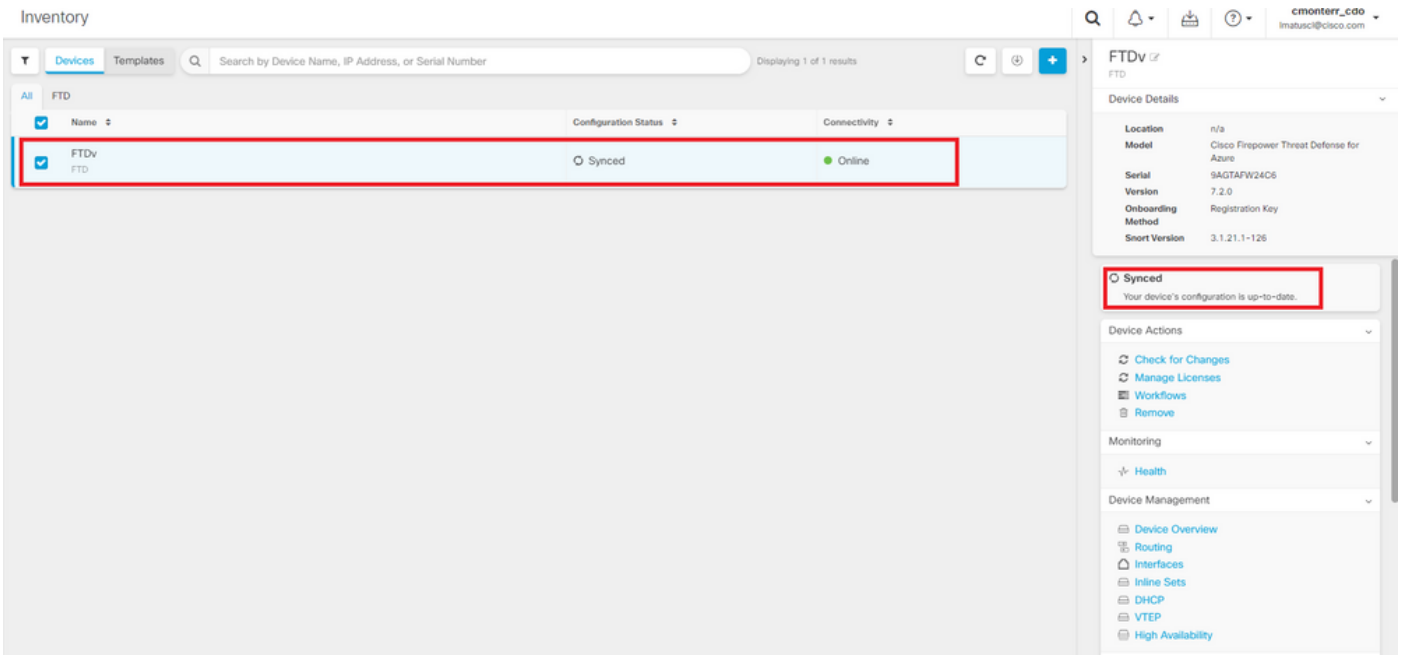
Remarque : si vous ne pouvez pas vous connecter à l'hôte, vous pouvez rectifier la configuration DNS dans l'interface de ligne de commande FTD à l'aide de la commande suivante : **configure network dns <address>**.

Pour surveiller le processus d'enregistrement, accédez à **Device Actions > Workflows.**.

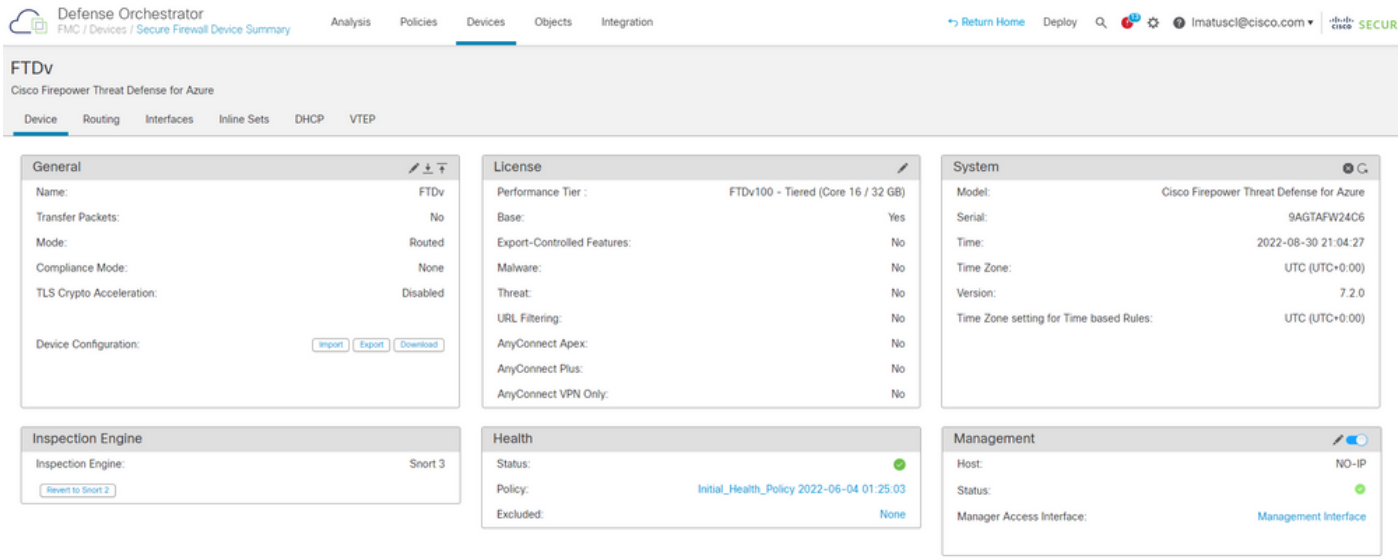


Développez le **Active** pour obtenir des informations supplémentaires, ces images montrent comment le FTDv a été enregistré avec succès.





Enfin, accédez à **Device Management > Device Overview** afin d'accéder au cdFMC et de consulter l'état de la présentation FTDv.



Informations connexes

- [Technical Support & Documentation - Cisco Systems]
- [Gestion des périphériques Cisco Secure Firewall Threat Defense grâce au centre de gestion des pare-feu fourni dans le cloud]

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.