

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

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Déployez un centre de gestion Firepower fourni dans le cloud sur CDO.](#)

[Intégration d'un FTD sur un FMC fourni dans le cloud](#)

[Informations connexes](#)

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.

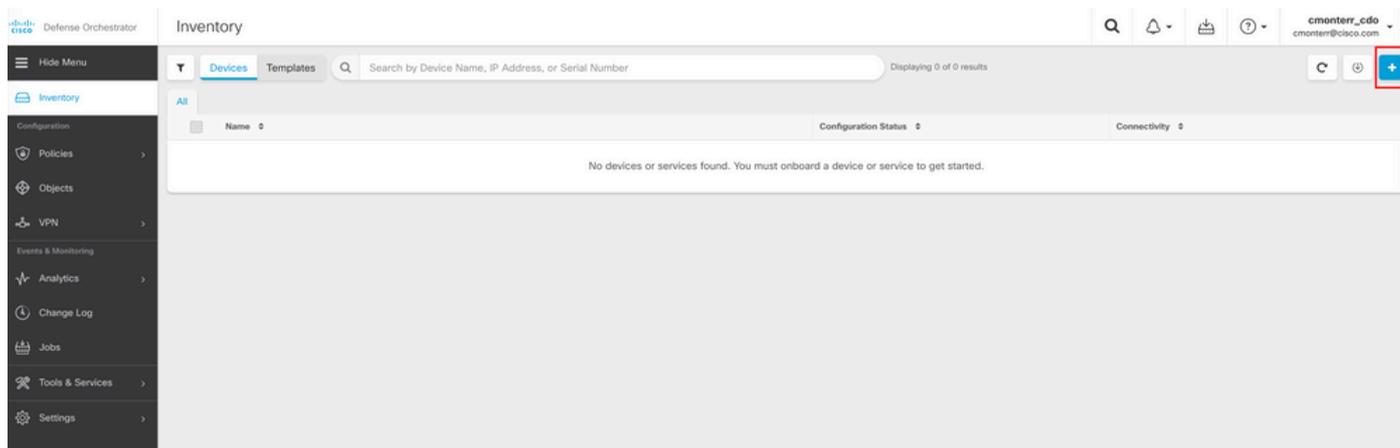
Ce produit est conçu pour la migration des centres de gestion de pare-feu sécurisés sur site vers la version SaaS du centre de gestion de pare-feu sécurisé.

Configurer

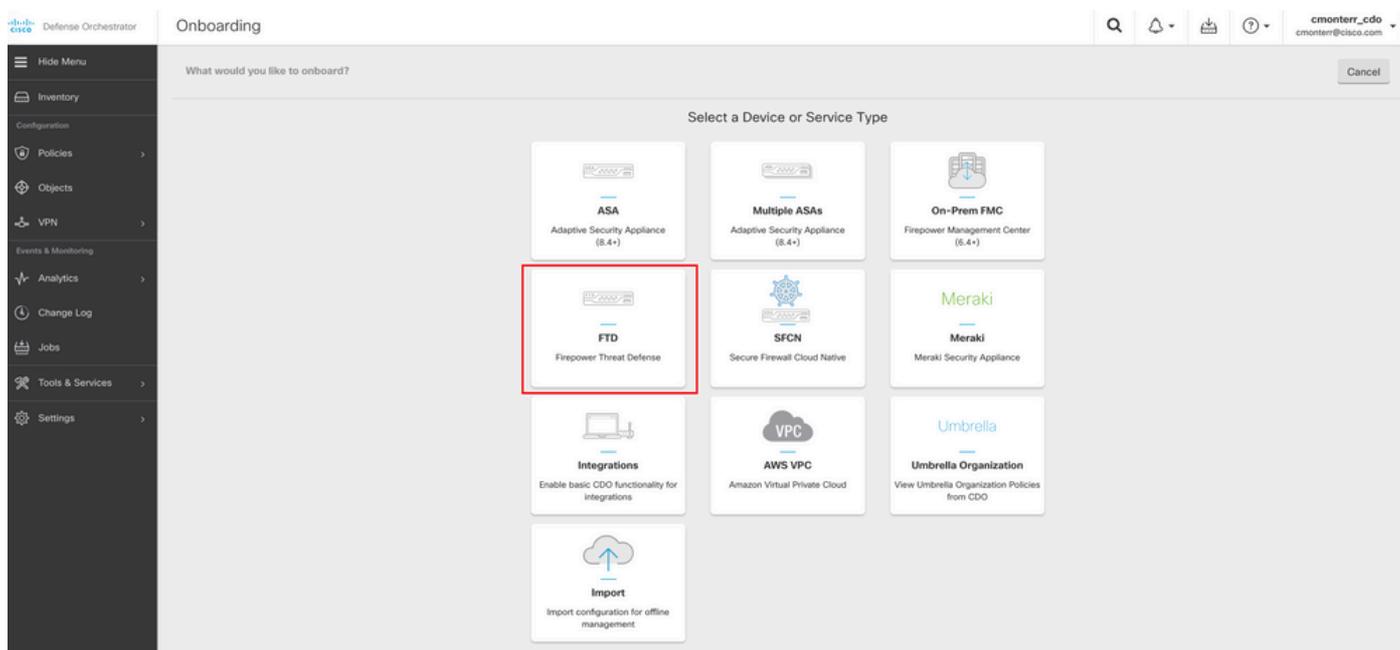
Déployez un centre de gestion Firepower fourni dans le cloud sur CDO.

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

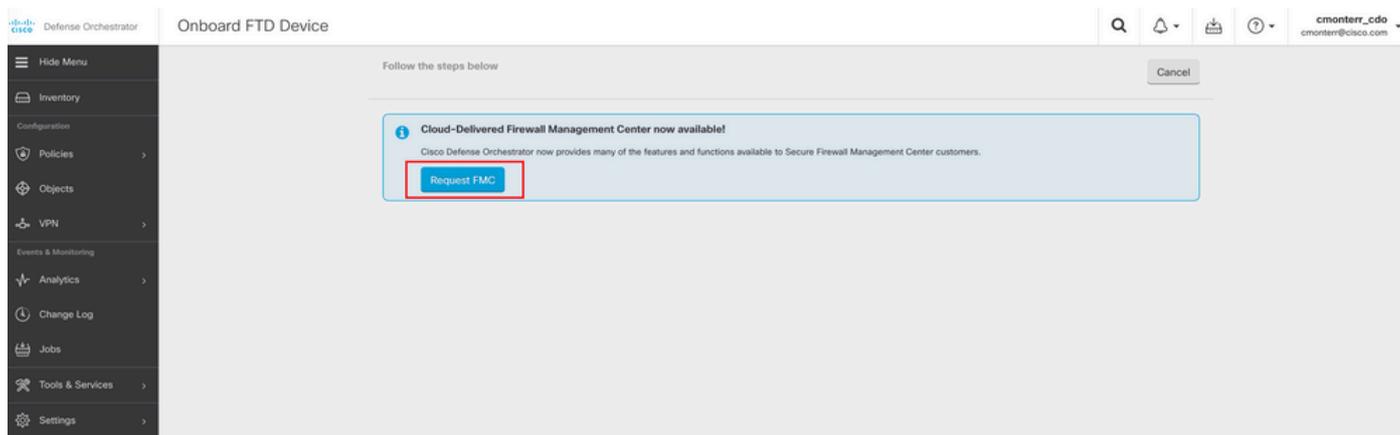
Tout d'abord, accédez à **Menu > Inventory** afin d'ajouter un nouveau périphérique.



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

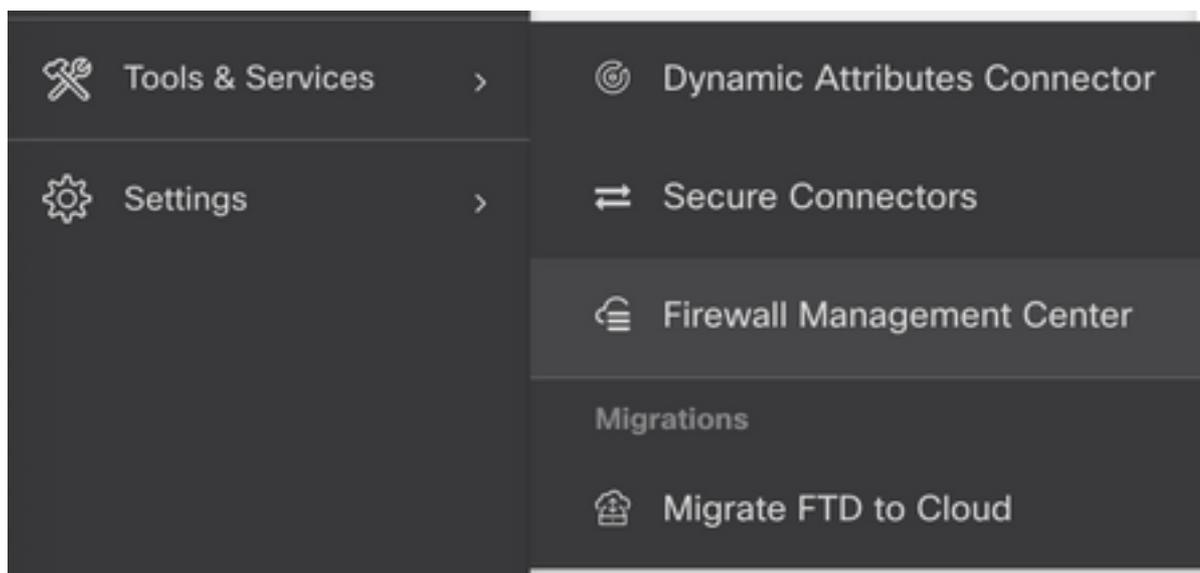


Sélectionner **Request FMC** afin de demander le centre de gestion Firepower fourni dans le cloud.

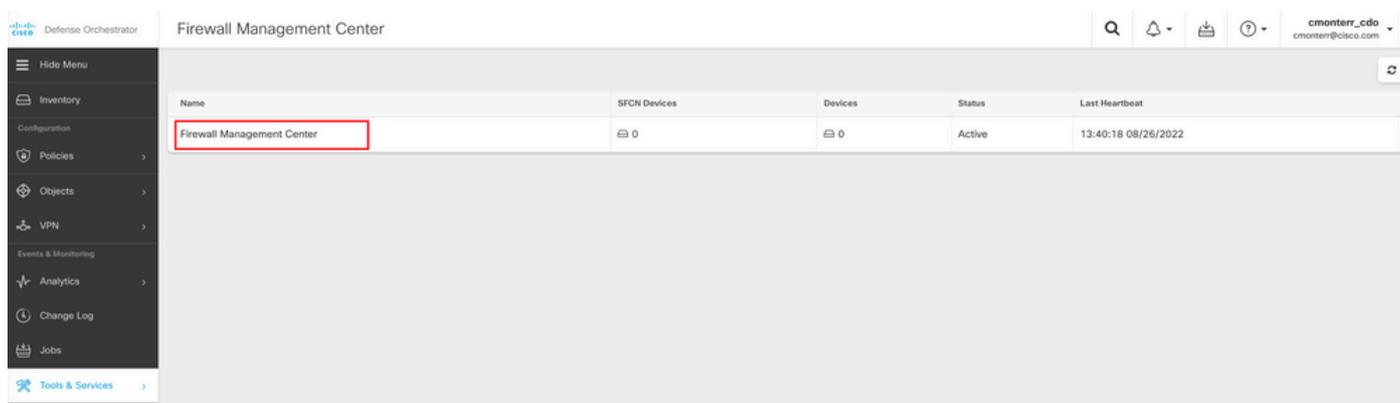


Remarque : l'option « Request FMC » (Demander FMC) n'est présentée que si vous n'avez aucun cdFMC dans le service partagé.

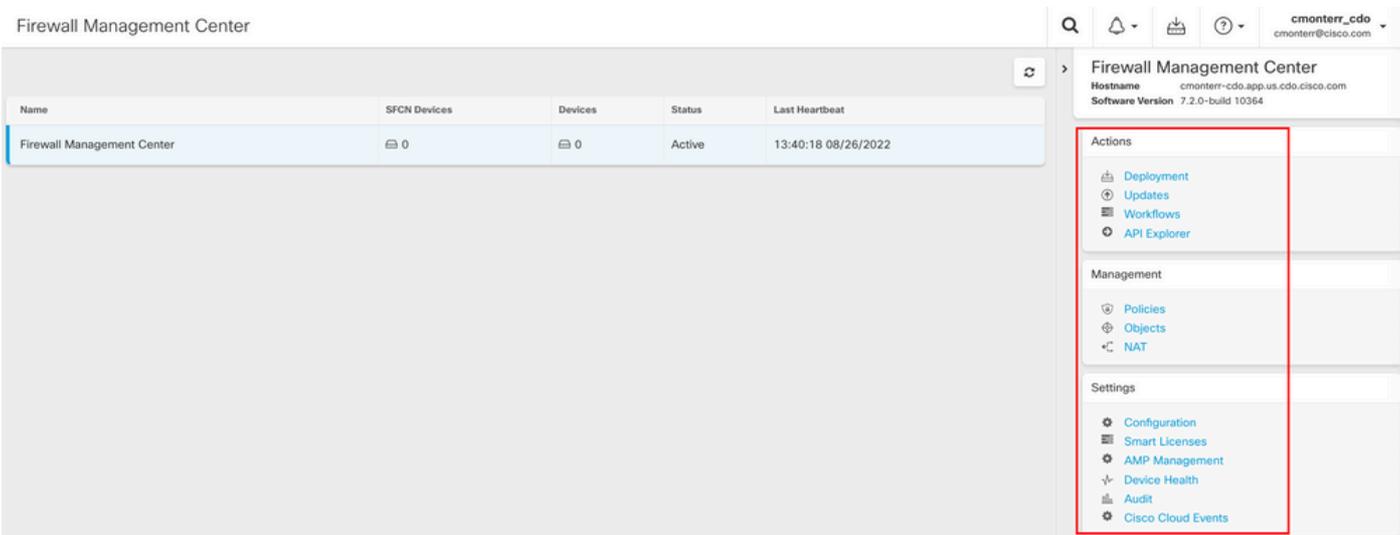
Naviguez jusqu'à **Menu > Tools & Services > Firewall Management Center** lorsque le cdFMC est prêt à être utilisé.



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.



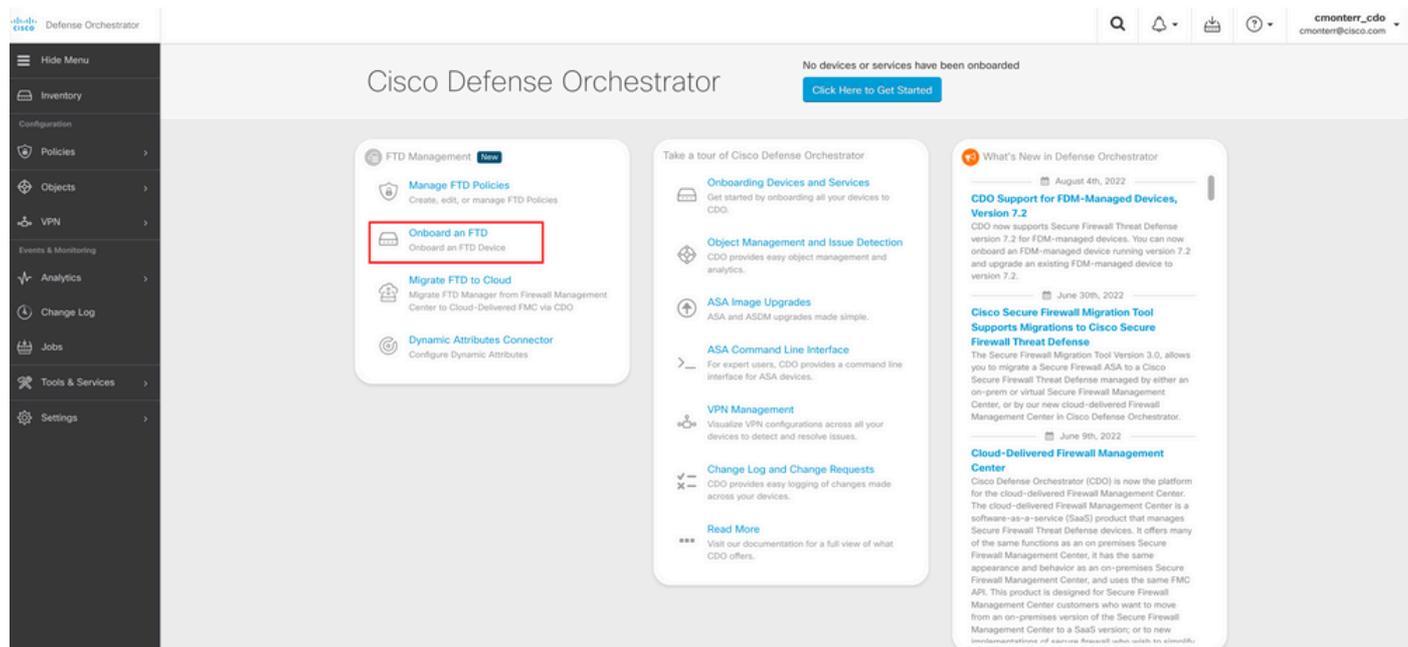
Vous pouvez maintenant voir l'interface graphique utilisateur de cdFMC.



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.

Onboard FTD Device

Follow the steps below

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+)

Saisissez les informations FTDv requises et souhaitées.

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.

Enfin, le cdFMC crée un CLI keyClé CLI de votre périphérique.

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](#)

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.

The screenshot shows the Cisco Defense Orchestrator (CDO) interface. The main view is the 'Inventory' page, which displays a table of devices. One device, 'FTDv', is highlighted with a red box around its 'Onboarding' status. The right-hand pane shows the 'Device Details' for 'FTDv', including a 'Registration Pending' status and instructions for completing the registration process.

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..**

The screenshot shows the 'Workflows' page in the CDO interface. It displays a table of workflows related to the device registration process. The table has columns for Name, Priority, Condition, Current State, Last Active, and Time.

Name	Priority	Condition	Current State	Last Active	Time
fmcRegisterFtdStateMachine	On Demand	Done	Done	8/30/2022, 3:35:50 PM	8/30/2022, 3:33:11 PM / 8/30/2022, 3:35:50 PM
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

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

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

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

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>

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.