

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)

Version FTD minimale 7.0.3

Composants utilisés

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

- CdFMC
- 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.

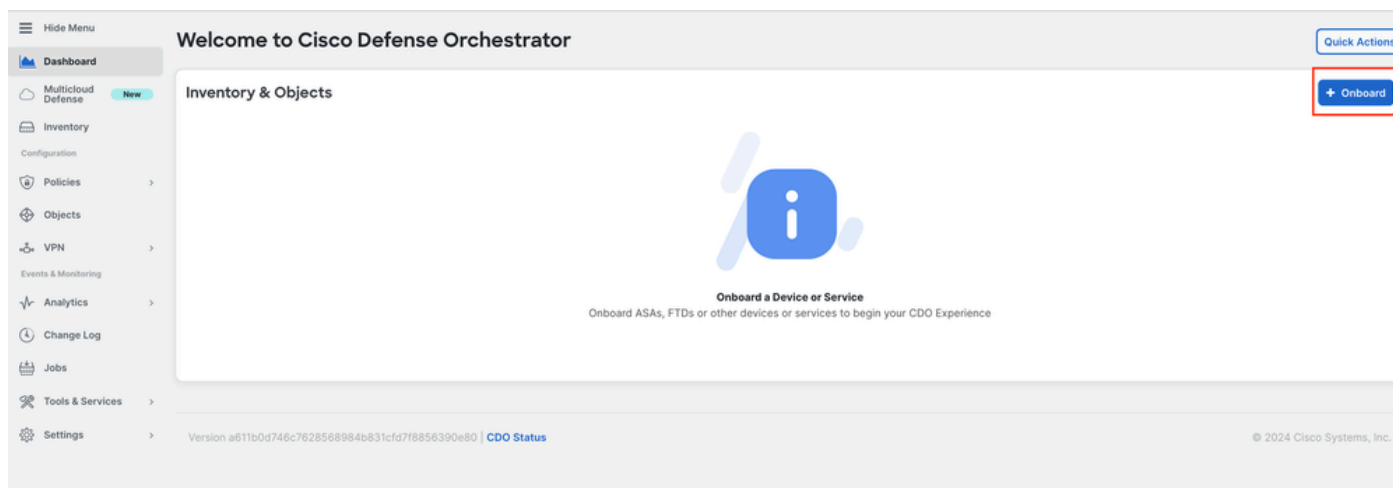
Ce produit est conçu pour la migration des centres de gestion de pare-feu sécurisés sur site vers la version SaaS du centre de gestion de pare-feu sécurisé.

Configurer

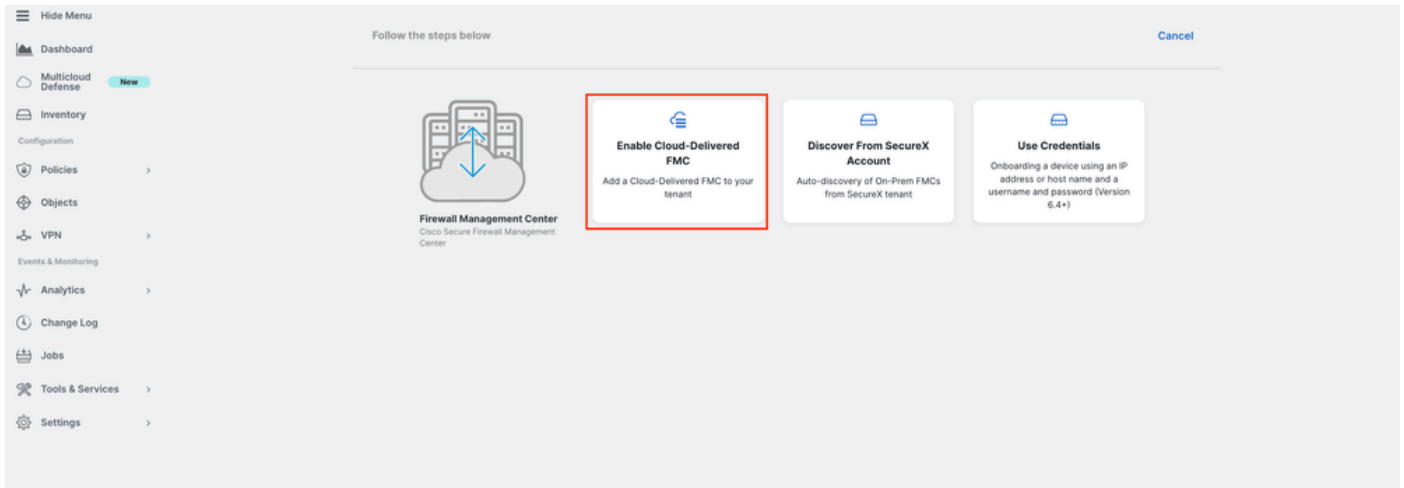
Déployez un centre de gestion Firepower fourni dans le cloud sur CDO.

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

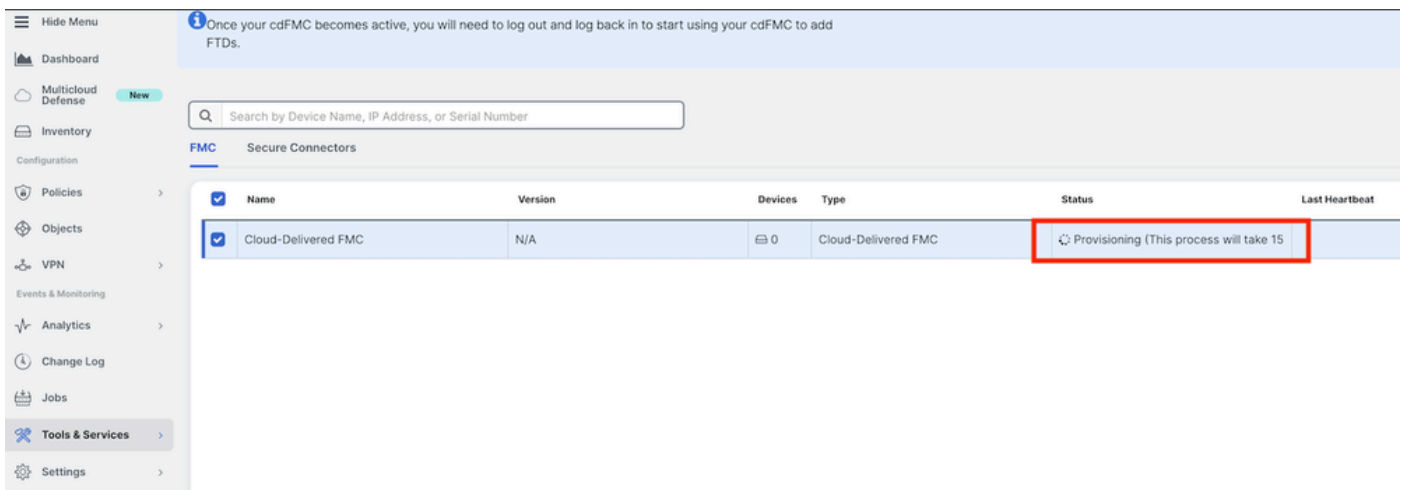
Dans le menu CDO, accédez à **Tools & Services > Firewall Management Center > Onboard**.



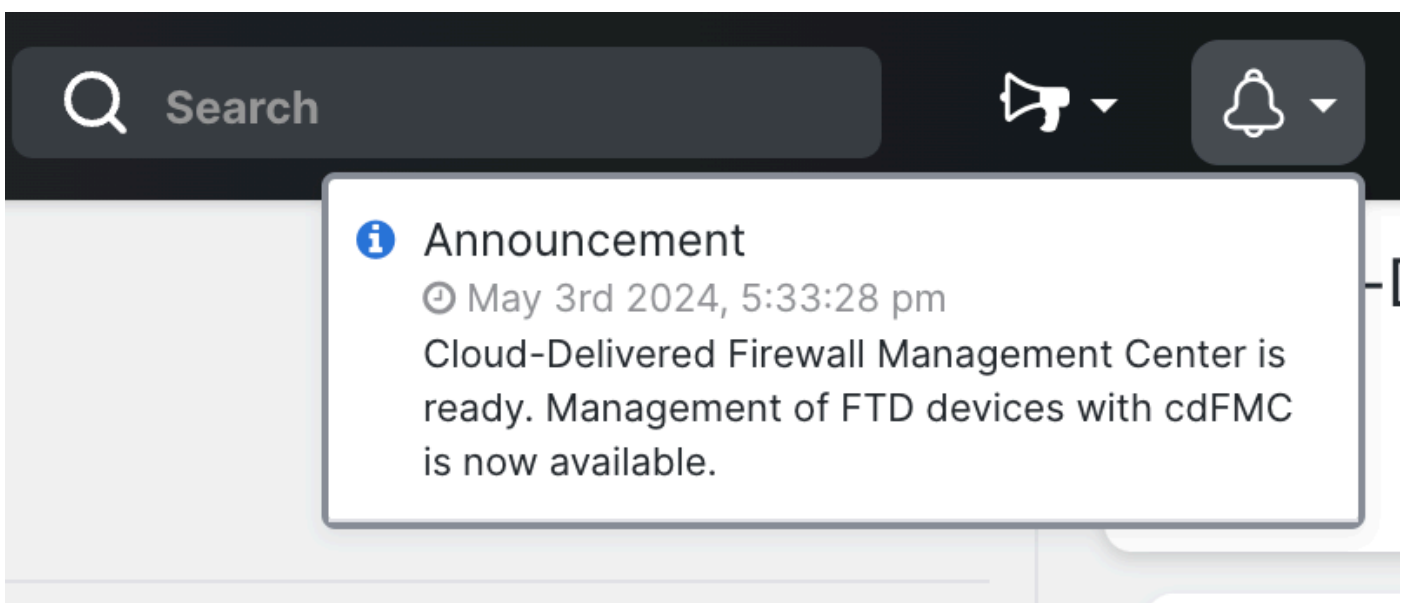
Sélectionner Enable Cloud-Delivered FMC.



CDO met en service une instance de Firewall Management Center dans le cloud en arrière-plan ; cela prend généralement 15 à 30 minutes. Vous pouvez suivre la progression du provisionnement dans la colonne État de Cloud-Delivered FMC.



Une fois la mise en service terminée, l'état passe à Actif. En outre, vous recevez une notification « Firewall Management Center is Ready » dans le panneau de notifications CDO.



The screenshot shows the Cisco Defense Orchestrator interface. The main content area displays a table of Secure Connectors. The table has the following columns: Name, Version, Devices, Type, Status, and Last Heartbeat. One entry is visible: 'Cloud-Delivered FMC' with version '20240412', 0 devices, and a status of 'Active'. The 'Status' column is highlighted with a red box.

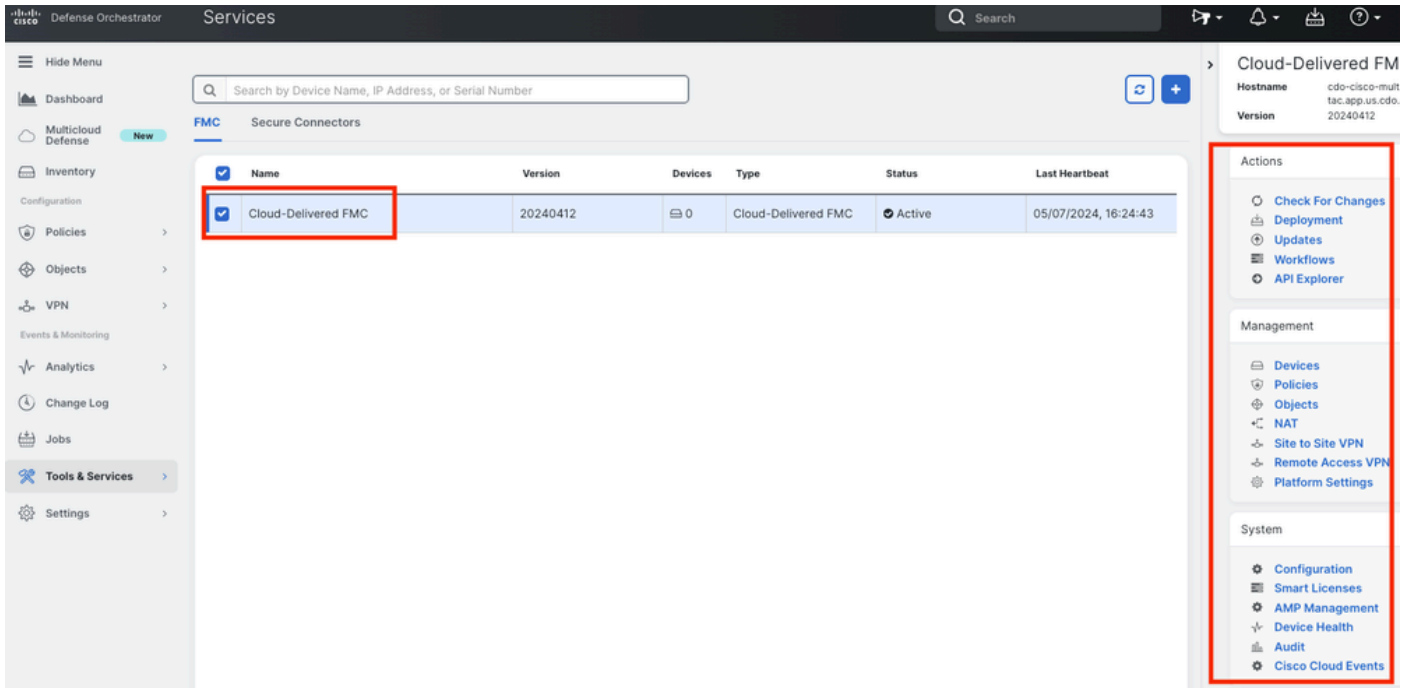
Name	Version	Devices	Type	Status	Last Heartbeat
Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	Active	05/07/2024, 16:24:43

Vous pouvez ensuite intégrer vos appareils de protection contre les menaces au centre de gestion des pare-feu fourni dans le cloud et les gérer.

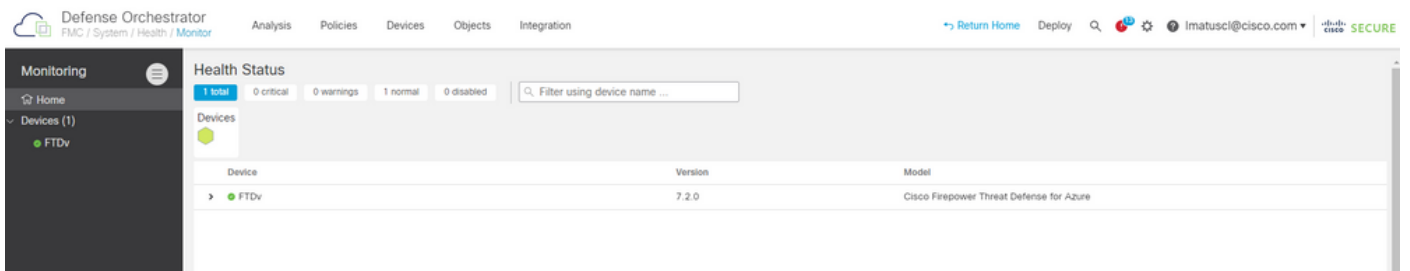
Accédez à **Menu > Tools & Services > Firewall Management Center**.

The screenshot shows the 'Tools & Services' menu. The menu items are: Tools & Services, Settings, Dynamic Attributes Connector, Secure Connectors, Firewall Management Center, Migrations, and Migrate FTD to Cloud. The 'Firewall Management Center' option is highlighted.

Sélectionnez votre cdFMC pour afficher les informations de cdFMC et, 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).

Tout d'abord, sélectionnez **Onboard an FTD** sur la page d'accueil de CDO.

Defense Orchestrator

Hide Menu

Inventory

Configuration

Policies

Objects

VPN

Events & Monitoring

Analytics

Change Log

Jobs

Tools & Services

Settings

Cisco Defense Orchestrator

No devices or services have been onboarded

[Click Here to Get Started](#)

FTD Management New

- Manage FTD Policies**
Create, edit, or manage FTD Policies
- Onboard an FTD**
Onboard an FTD Device
- Migrate FTD to Cloud**
Migrate FTD Manager from Firewall Management Center to Cloud-Delivered FMC via CDO
- Dynamic Attributes Connector**
Configure Dynamic Attributes

Take a tour of Cisco Defense Orchestrator

- Onboarding Devices and Services**
Get started by onboarding all your devices to CDO.
- Object Management and Issue Detection**
CDO provides easy object management and analytics.
- ASA Image Upgrades**
ASA and ASDM upgrades made simple.
- ASA Command Line Interface**
For expert users, CDO provides a command line interface for ASA devices.
- VPN Management**
Visualize VPN configurations across all your devices to detect and resolve issues.
- Change Log and Change Requests**
CDO provides easy logging of changes made across your devices.
- Read More**
Visit our documentation for a full view of what CDO offers.

What's New in Defense Orchestrator

- August 4th, 2022**
CDO Support for FDM-Managed Devices, Version 7.2
CDO now supports Secure Firewall Threat Defense version 7.2 for FDM-managed devices. You can now onboard an FDM-managed device running version 7.2 and upgrade an existing FDM-managed device to version 7.2.
- June 30th, 2022**
Cisco Secure Firewall Migration Tool Supports Migrations to Cisco Secure Firewall Threat Defense
The Secure Firewall Migration Tool Version 3.0, allows you to migrate a Secure Firewall ASA to a Cisco Secure Firewall Threat Defense managed by either an on-prem or virtual Secure Firewall Management Center, or by our new cloud-delivered Firewall Management Center in Cisco Defense Orchestrator.
- June 9th, 2022**
Cloud-Delivered Firewall Management Center
Cisco Defense Orchestrator (CDO) is now the platform for the cloud-delivered Firewall Management Center. The cloud-delivered Firewall Management Center is a software-as-a-service (SaaS) product that manages Secure Firewall Threat Defense devices. It offers many of the same functions as an on-premises Secure Firewall Management Center, it has the same appearance and behavior as an on-premises Secure Firewall Management Center, and uses the same FMC API. This product is designed for Secure Firewall Management Center customers who want to move from an on-premises version of the Secure Firewall Management Center to a SaaS version, or to new implementations of secure firewall with which to comply.

Sélectionnez ensuite l'Use CLI Registration Key option.

Defense Orchestrator

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+)

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](#)

! 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 une configuration spécifique **CLI Key** pour 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 'Inventory' page in Cisco Defense Orchestrator. A table lists one device: 'FTDv' with a status of 'Onboarding'. The 'Onboarding' button is highlighted with a red box. The right sidebar shows 'Registration Pending' status with instructions to complete the onboarding 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 Cisco Defense Orchestrator. A table lists two workflows for the 'FTDv (FTD)' device:

Name	Priority	Condition	Current State	Last Active	Time
fmceRegisterFtdStateMachine	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 l' **Active** état pour avoir des informations supplémentaires, ces images montrent comment le FTDv a été enregistré avec succès.

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		
DeviceStateMachineSetErrorAfterHook	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

All	Name	Configuration Status	Connectivity
<input checked="" type="checkbox"/>	FTDv FTD	○ Synced	● Online

FTDv
FTD

○ 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 à cdFMC et consultez l'état de la vue d'ensemble FTDv.

FTDv

Cisco Firepower Threat Defense for Azure

Device Routing Interfaces Inline Sets DHCP VTEP

General

Name: FTDv

Transfer Packets: No

Mode: Routed

Compliance Mode: None

TLS Crypto Acceleration: Disabled

Device Configuration: [Import](#) [Export](#) [Download](#)

License

Performance Tier : FTDv100 - Tiered (Core 16 / 32 GB)

Base: Yes

Export-Controlled Features: No

Malware: No

Threat: No

URL Filtering: No

AnyConnect Apex: No

AnyConnect Plus: No

AnyConnect VPN Only: No

System

Model: Cisco Firepower Threat Defense for Azure

Serial: 9AGTAFW24C6

Time: 2022-08-30 21:04:27

Time Zone: UTC (UTC+0:00)

Version: 7.2.0

Time Zone setting for Time based Rules: UTC (UTC+0:00)

Inspection Engine

Inspection Engine: Snort 3

[Revert to Snort 2](#)

Health

Status:

Policy: Initial_Health_Policy 2022-06-04 01:25:03

Excluded: None

Management

Host: NO-IP

Status:

Manager Access Interface: [Management Interface](#)

Informations connexes

- [Assistance et documentation techniques - 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.