Implemente un FMC distribuido en la nube (cdFMC) en Cisco Defense Orchestrator (CDO)

Contenido

Introducción

Este documento describe el proceso de implementación e incorporación de FMC en nube en la plataforma CDO.

Prerequisites

Requirements

Cisco recomienda conocer estos temas:

- FirePOWER Management Center (cdFMC) proporcionado en la nube
- Cisco Defense Orchestrator (CDO)
- Firepower Threat Defence Virtual (FTDv)

FTD versión mínima 7.0.3

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- cdFMC
- FTDv 7.2.0

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Cisco Defense Orchestrator (CDO) es la plataforma para el centro de gestión de firewall (cdFMC) suministrado en la nube. El centro de gestión de firewalls en la nube es un producto de software como servicio (SaaS) que gestiona los dispositivos de defensa frente a amenazas de firewall seguro. Ofrece muchas de las mismas funciones que un firewall seguro in situ Secure Firewall Threat Defence. Tiene el mismo aspecto y comportamiento que un Secure Firewall Management Center in situ y utiliza la misma interfaz de programación de aplicaciones (API) de FMC.

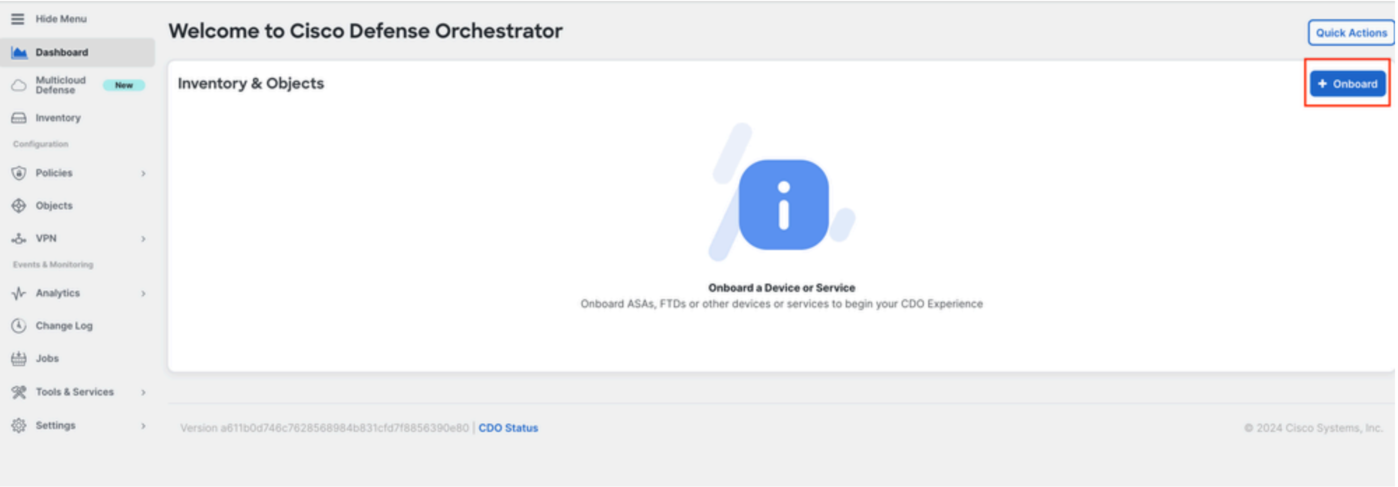
Este producto está diseñado para la migración de los Secure Firewall Management Centers in situ a la versión SaaS de Secure Firewall Management Center.

Configurar

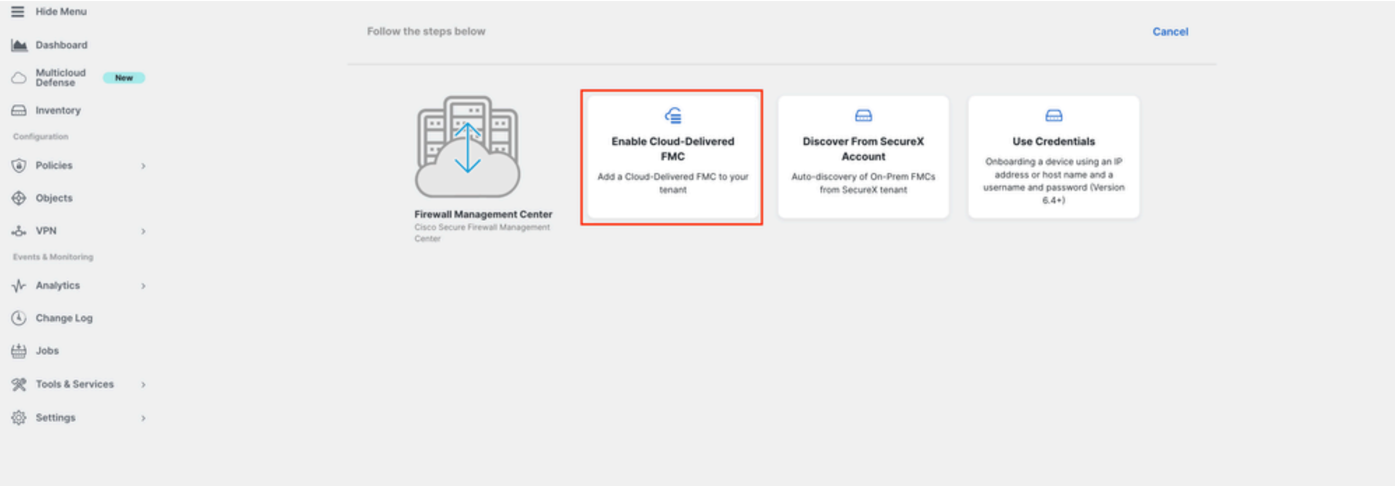
Implemente un FirePOWER Management Center en la nube en CDO.

Estas imágenes muestran el proceso de configuración inicial necesario para implementar un FMC en CDO proporcionado desde la nube.

En el menú CDO, vaya a **Tools & Services** > **Firewall Management Center** > **Onboard**.


Hide Menu
Dashboard
Multicloud Defense
New
Inventory
Configuration
Policies
Objects
VPN
Events & Monitoring
Analytics
Change Log
Jobs
Tools & Services
Settings
Welcome to Cisco Defense Orchestrator
Quick Actions
Inventory & Objects
+ Onboard
Onboard a Device or Service
Onboard ASAs, FTDs or other devices or services to begin your CDO Experience
Version a611b0d746c7628568984b831cfd7f8856390e80 | CDO Status
© 2024 Cisco Systems, Inc.

Seleccionar Enable Cloud-Delivered FMC.

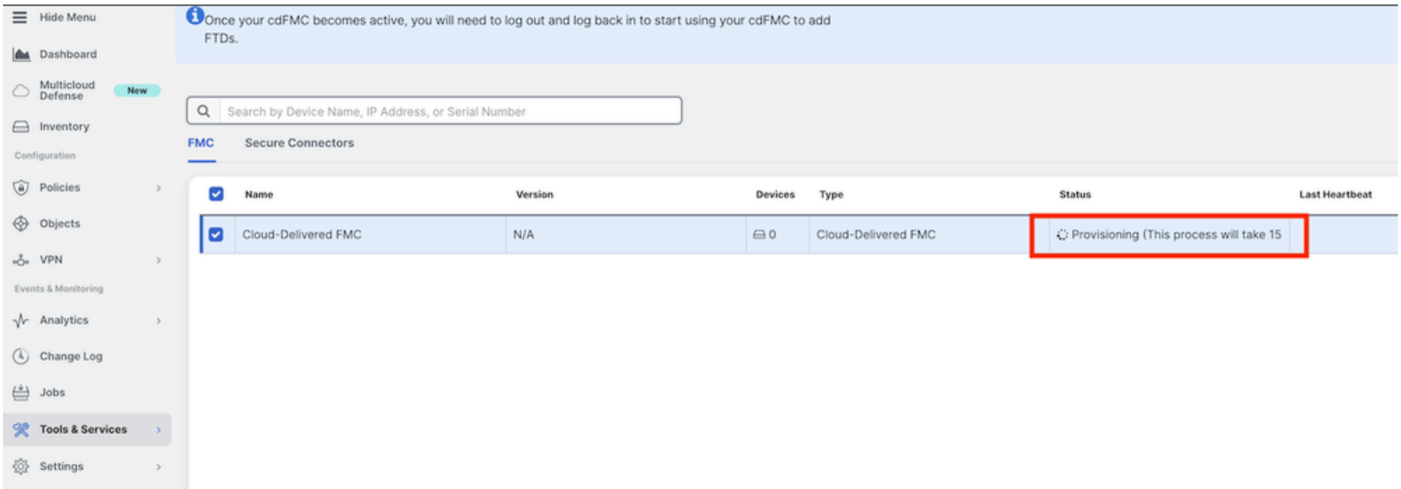


Enable Cloud-Delivered FMC
Add a Cloud-Delivered FMC to your tenant

Discover From SecureX Account
Auto-discovery of On-Prem FMCs from SecureX tenant

Use Credentials
Onboarding a device using an IP address or host name and a username and password (Version 6.4+)

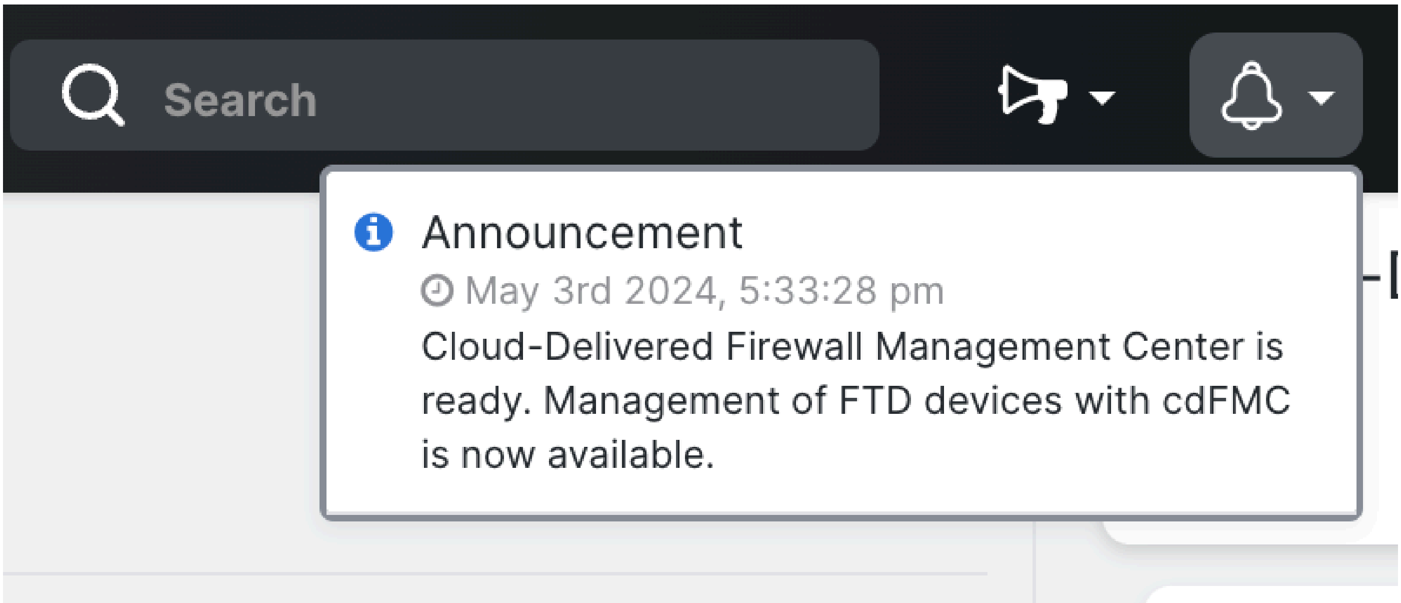
CDO proporciona una instancia de Firewall Management Center en la nube en segundo plano. Normalmente, se tardan entre 15 y 30 minutos en completar este proceso. Puede realizar un seguimiento del progreso del aprovisionamiento en la columna Status (Estado) de Cloud-Delivered FMC.



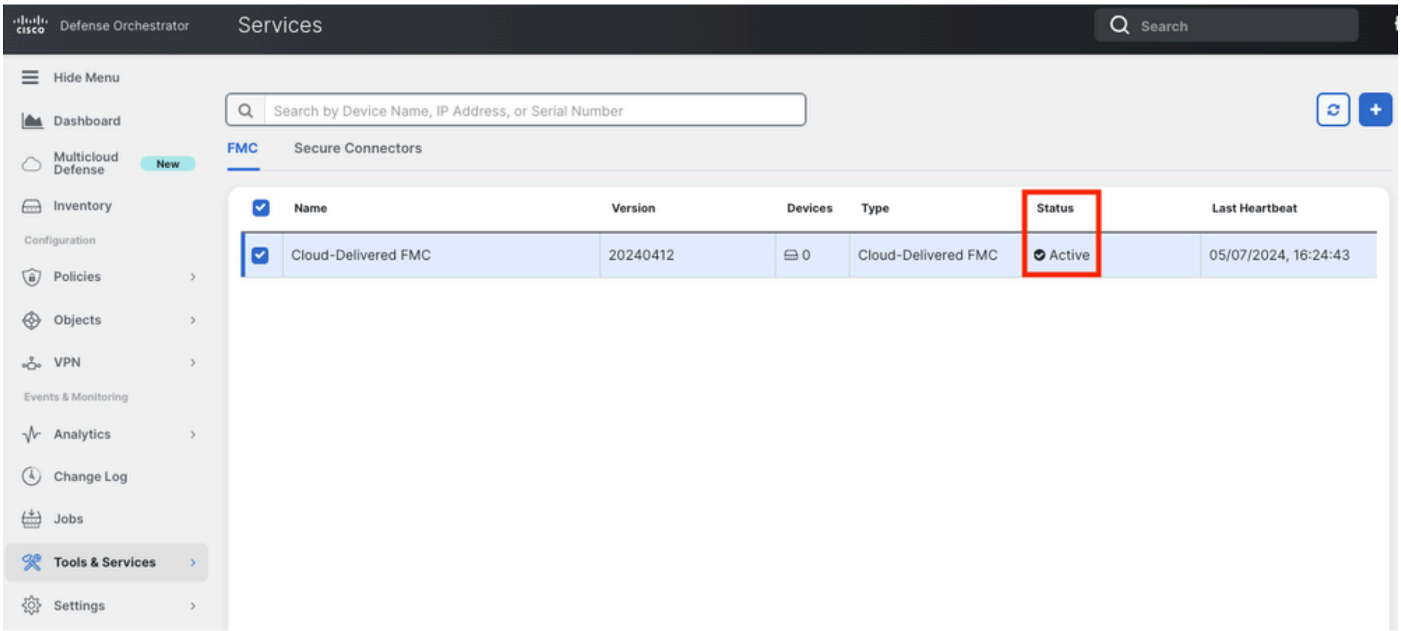
Once your cdFMC becomes active, you will need to log out and log back in to start using your cdFMC to add FTDs.

☑	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	N/A	0	Cloud-Delivered FMC	Provisioning (This process will take 15	

Una vez finalizado el aprovisionamiento, el estado cambia a Activo. Además, obtendrá una notificación Firewall Management Center is Ready (El centro de administración de firewalls está listo) en la nube en el panel de notificaciones de CDO.



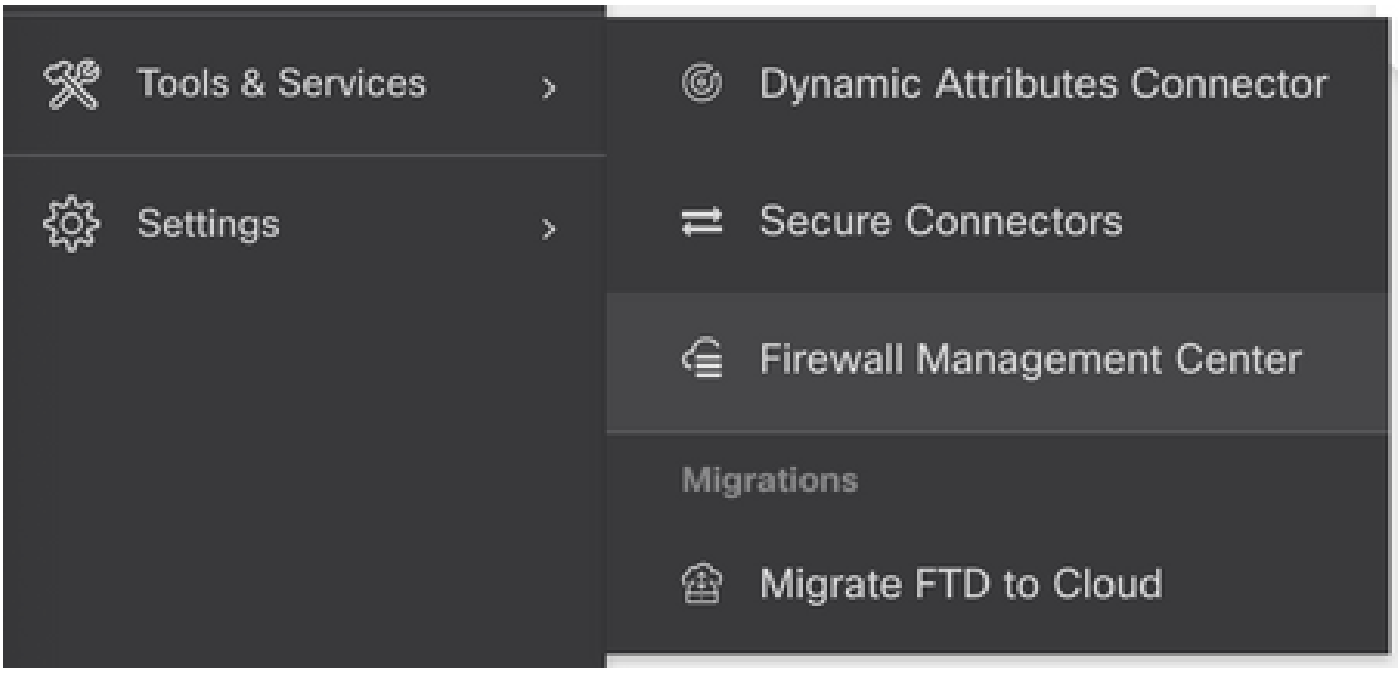
Announcement
May 3rd 2024, 5:33:28 pm
Cloud-Delivered Firewall Management Center is ready. Management of FTD devices with cdFMC is now available.



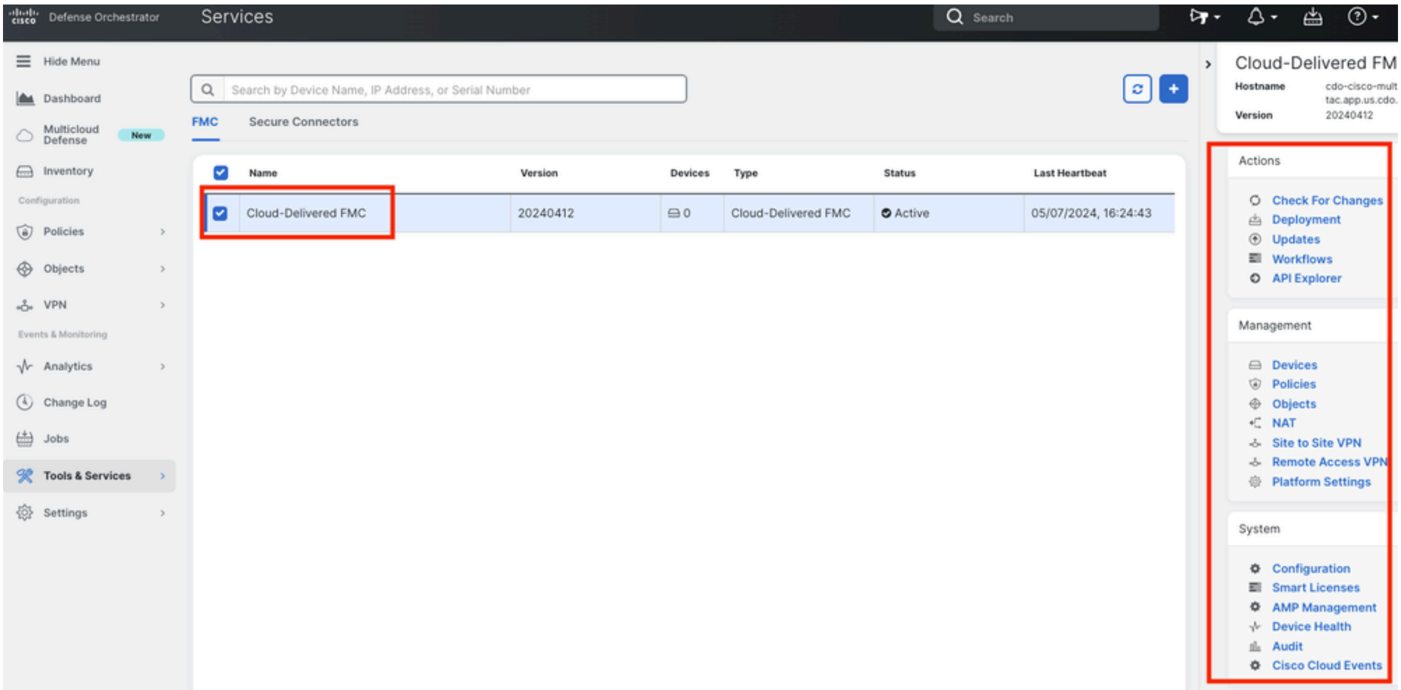
Name	Version	Devices	Type	Status	Last Heartbeat
Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	Active	05/07/2024, 16:24:43

A continuación, puede incorporar sus dispositivos de defensa frente a amenazas al centro de gestión de firewalls en la nube y gestionarlos.

Desplácese hasta **Menu** > **Tools & Services** > **Firewall Management Center**.



Seleccione su cdFMC para mostrar la información de cdFMC y, para acceder a la interfaz gráfica de usuario (GUI) del cdFMC, seleccione cualquiera de las opciones disponibles en el lado derecho.



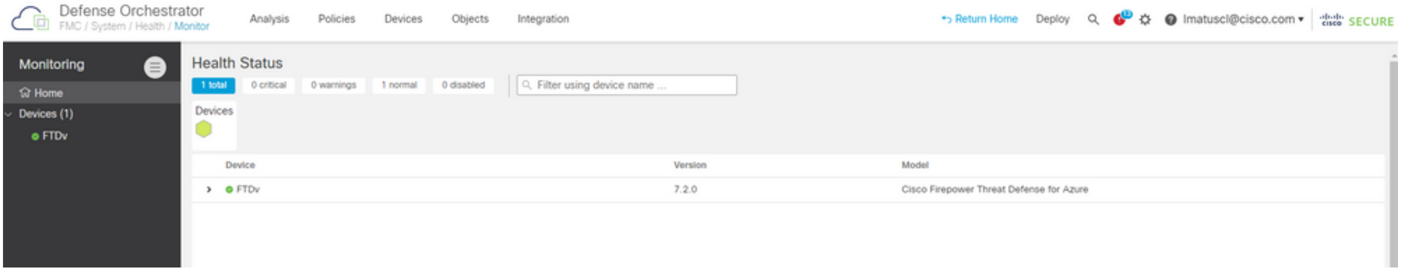
☑	Name	Version	Devices	Type	Status	Last Heartbeat
☑	Cloud-Delivered FMC	20240412	0	Cloud-Delivered FMC	Active	05/07/2024, 16:24:43

Cloud-Delivered FM

Hostname cdo-cisco-mult tac.app.us.cdo.

Version 20240412

Ahora puede ver la GUI de cdFMC.

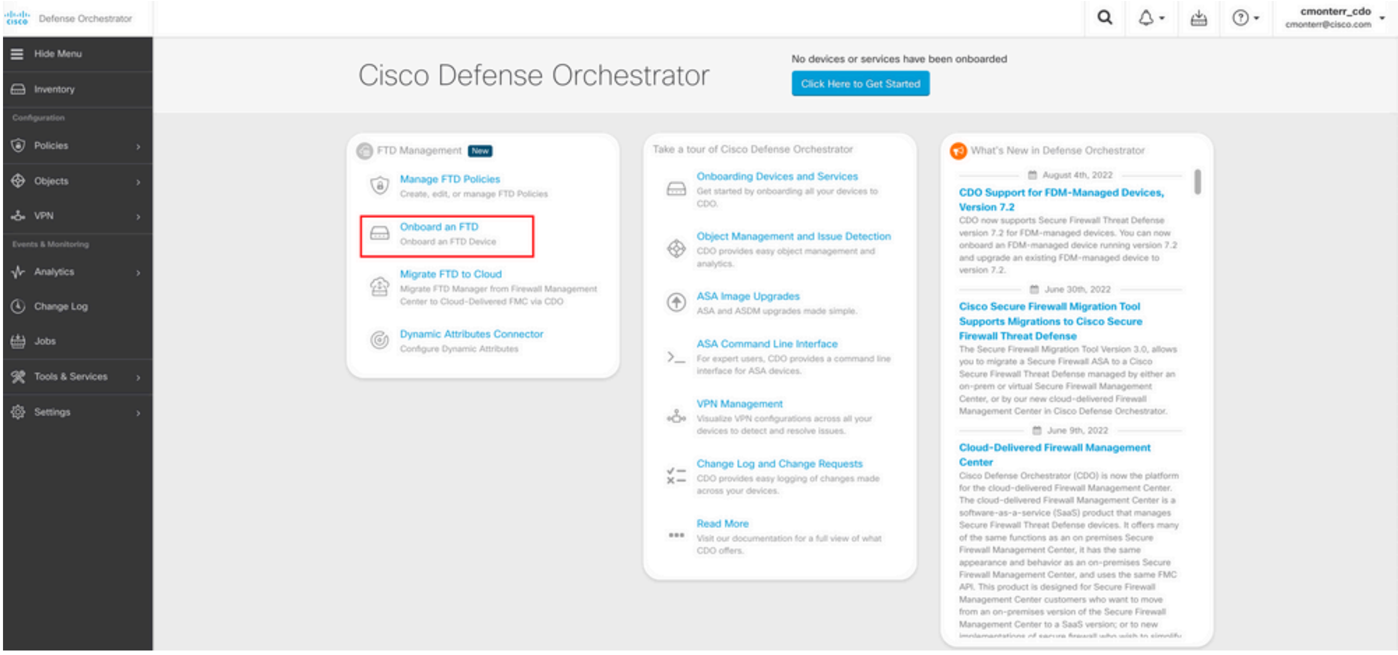


Device	Version	Model
FTDv	7.2.0	Cisco Firepower Threat Defense for Azure

Incorporación de un FTD en un FMC proporcionado en la nube

Estas imágenes muestran cómo incorporar un FTD para registrarse en un cdFMC con la clave de registro de la interfaz de línea de comandos (CLI).

En primer lugar, seleccione **Onboard an FTD** en la página de inicio de CDO.



Cisco Defense Orchestrator

No devices or services have been onboarded

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

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.

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.

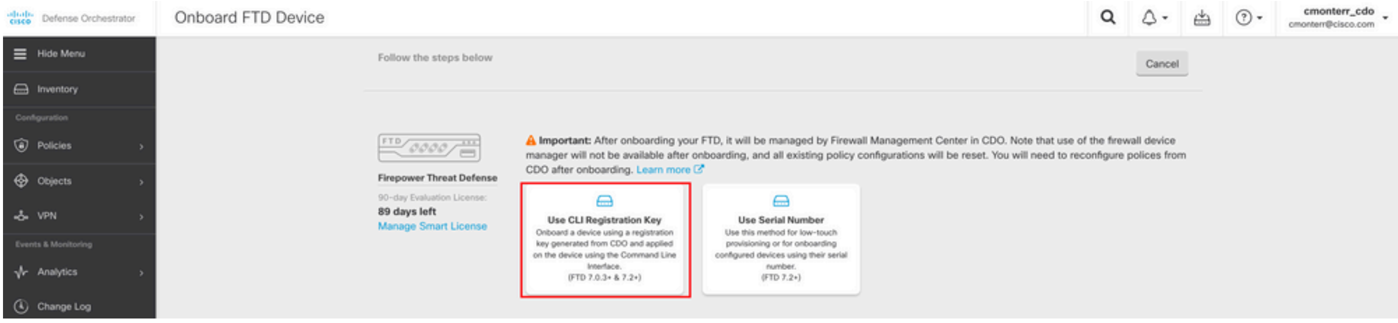
June 30th, 2022

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 who wish to simplify

A continuación, seleccione la **Use CLI Registration Key** opción.



Onboard FTD Device

Follow the steps below

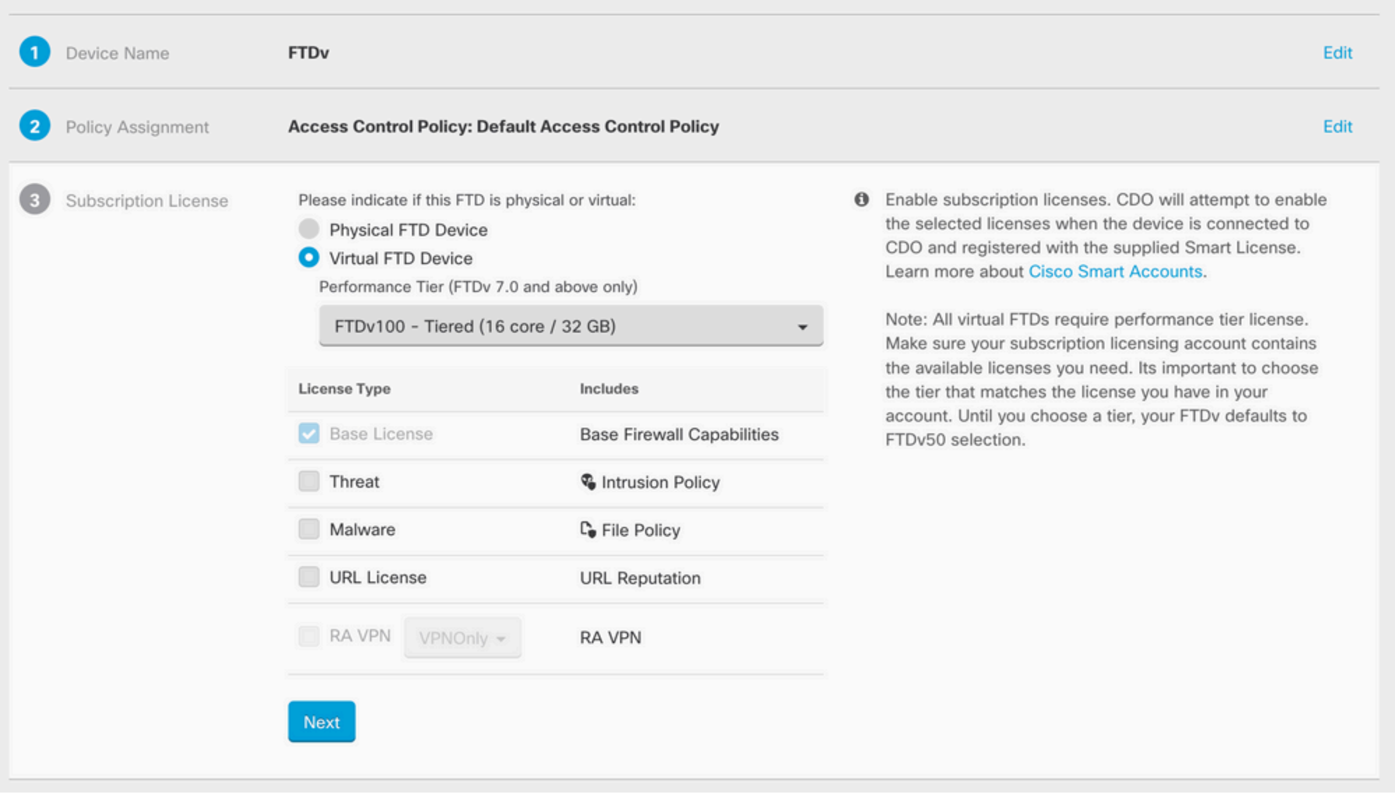
Firepower Threat Defense
90-day Evaluation License:
89 days left
Manage Smart License

⚠ **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 polices 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+)

Continúe introduciendo la información de FTDv solicitada y deseada.



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)

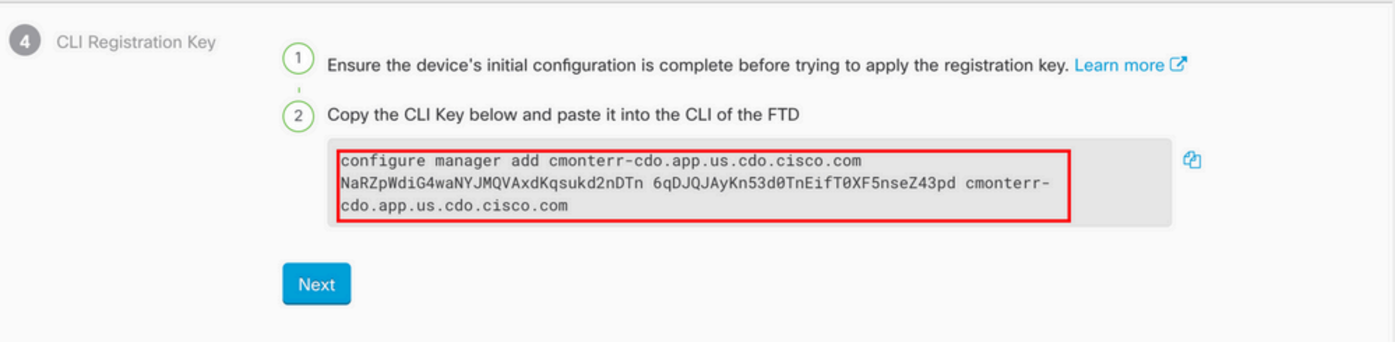
FTDv100 - Tiered (16 core / 32 GB)

License Type	Includes
☑ Base License	Base Firewall Capabilities
□ Threat	Intrusion Policy
□ Malware	File Policy
□ URL License	URL Reputation
□ RA VPN VPNOnly	RA VPN

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.

Por último, el cdFMC crea una interfaz específica **CLI Key**para su dispositivo.



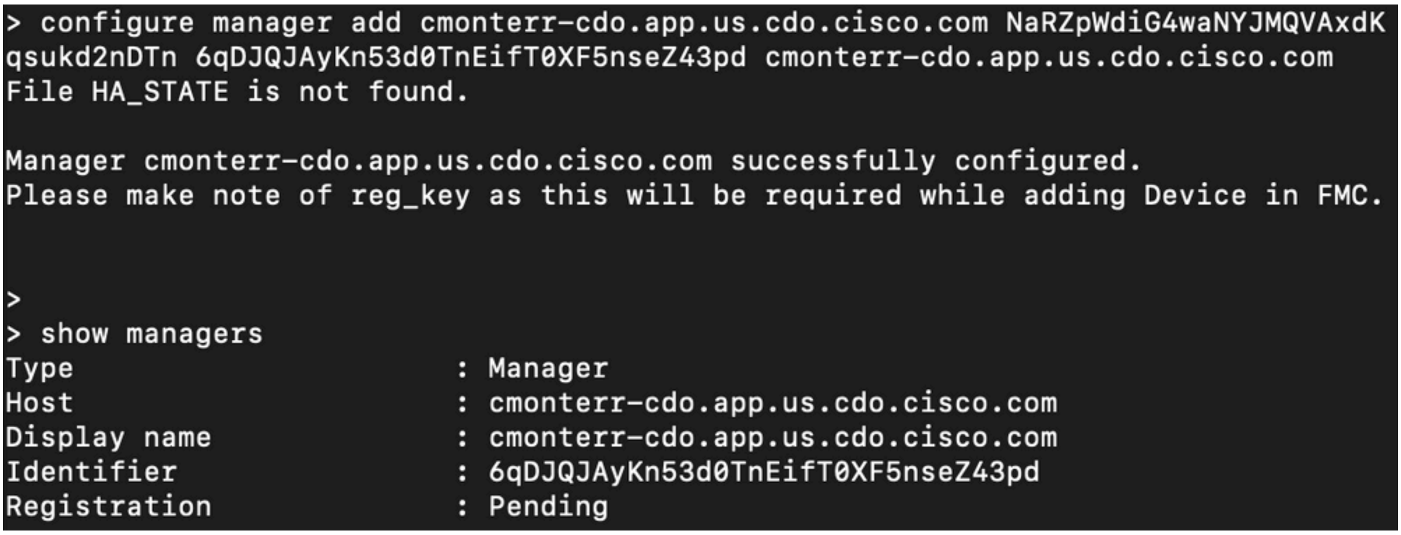
4 CLI Registration Key

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
```

Copie el **CLI Key** en la CLI del dispositivo administrado.

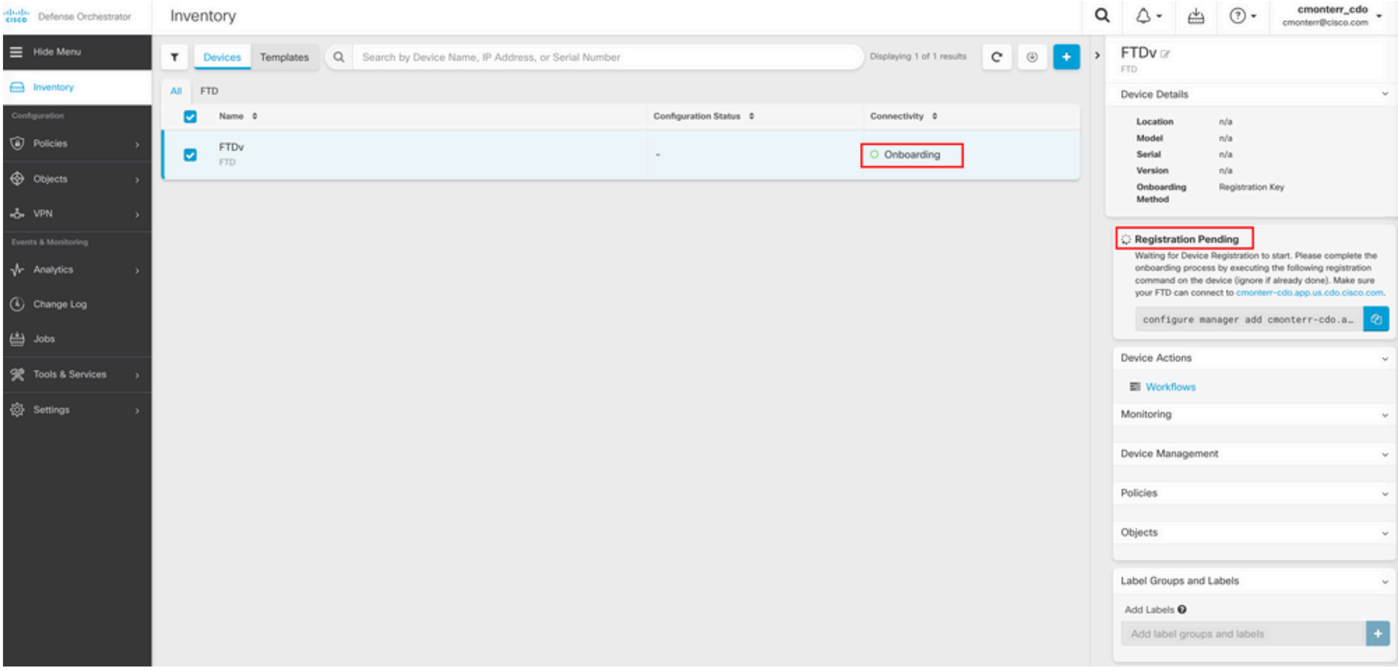


```
> configure manager add cmonterr-cdo.app.us.cdo.cisco.com NaRZpWdiG4waNYJMQVAxdK
qsukd2nDTn 6qDJQJAyKn53d0TnEifT0XF5nseZ43pd cmonterr-cdo.app.us.cdo.cisco.com
File HA_STATE is not found.

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
```

El cdFMC inicia una tarea de registro.



Name	Configuration Status	Connectivity
FTDv FTD	-	○ Onboarding

FTDv
FTD

Device Details

Location	n/a
Model	n/a
Serial	n/a
Version	n/a
Onboarding Method	Registration Key

Registration Pending

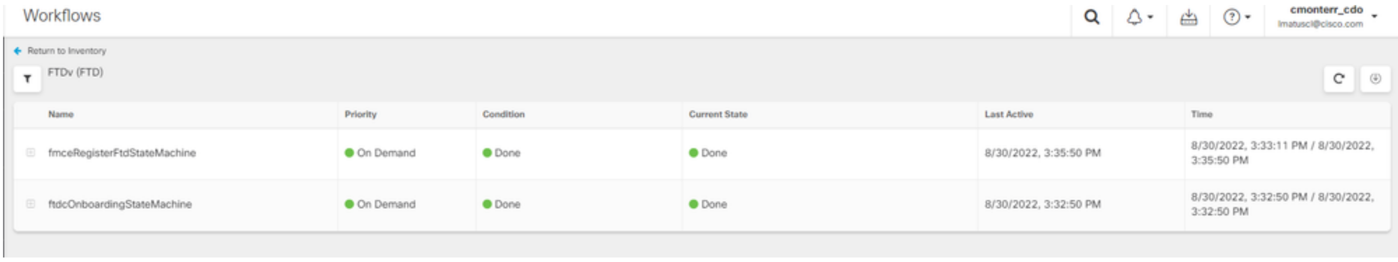
Waiting for Device Registration to start. Please complete the onboarding process by executing the following registration command on the device (ignore if already done). Make sure your FTD can connect to cmonterr-cdo.app.us.cdo.cisco.com.

```
configure manager add cmonterr-cdo.a…
```

Nota: Asegúrese de que el dispositivo FTD tenga comunicación a través de los puertos 8305 (sftunnel) y 443 con el arrendatario CDO para completar el proceso de registro. Consulte todos los requisitos de red.

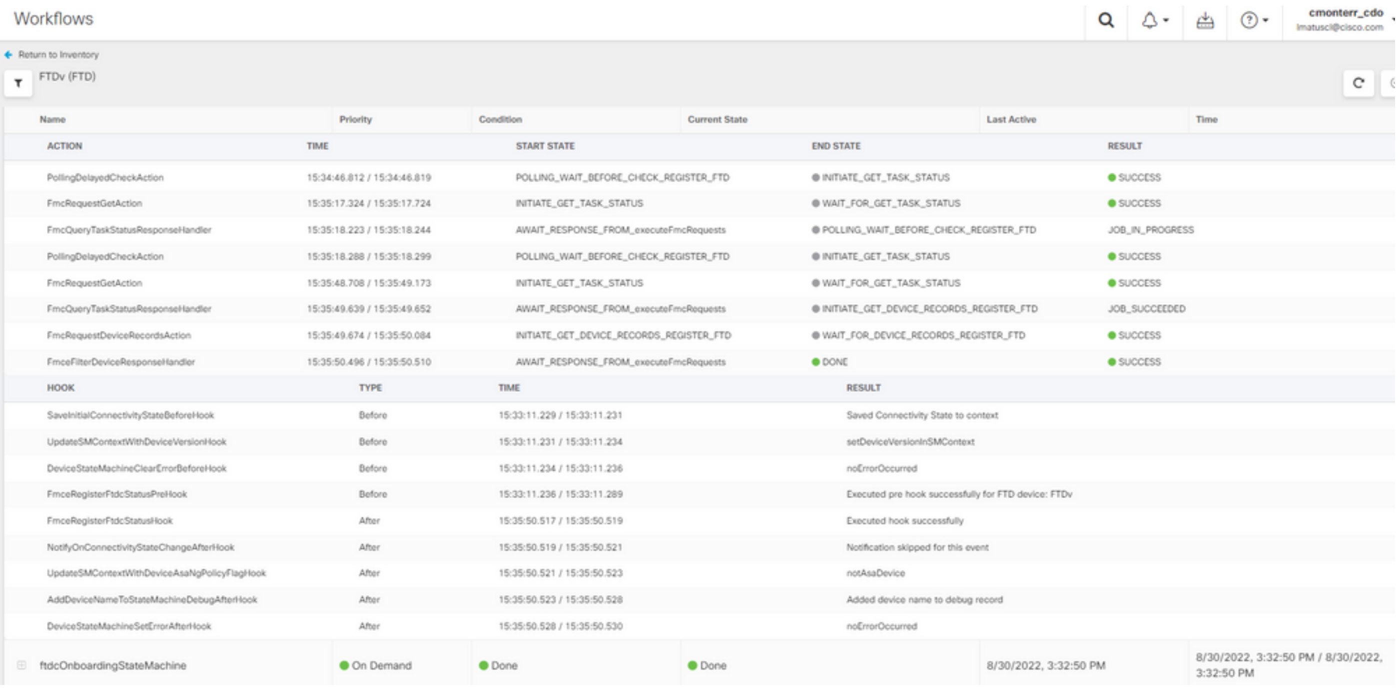
Nota: Si no puede conectarse al host, puede rectificar la configuración DNS en FTD-CLI con este comando: **configure network dns <address>**.

Para supervisar el proceso de registro, vaya a **Device Actions** > **Workflows.**.



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

Amplíe el **Active** estado para disponer de información adicional; estas imágenes muestran cómo se registró correctamente el FTDv.



Workflows

Return to Inventory

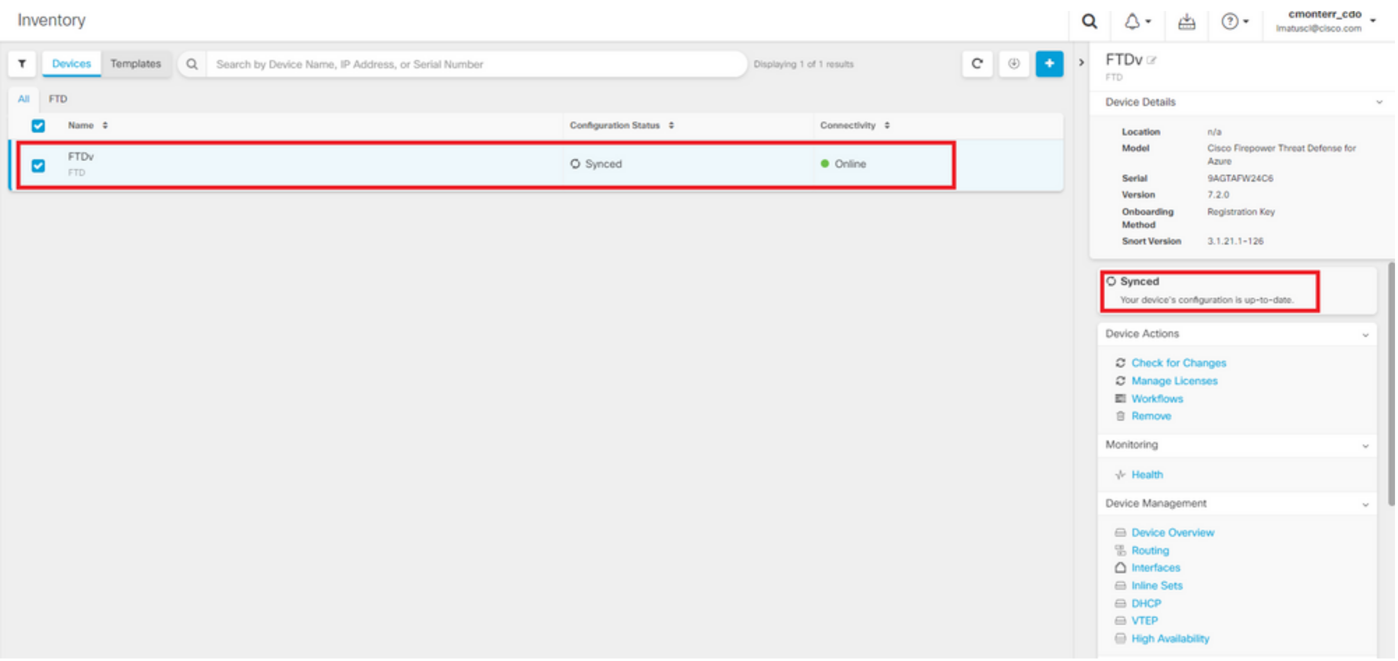
FTDv (FTD)

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
FmceFilterDeviceResponseHandler	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
FmceRegisterFtdcStatusPreHook	Before	15:33:11.236 / 15:33:11.289	Executed pre hook successfully for FTD device: FTDv
FmceRegisterFtdcStatusHook	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

Name	Priority	Condition	Current State	Last Active	Time
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
FTD
cmonterr_cdo
lmatuscl@cisco.com

Name	Configuration Status	Connectivity
☑ FTDv FTD	○ Synced	● Online

FTDv
FTD

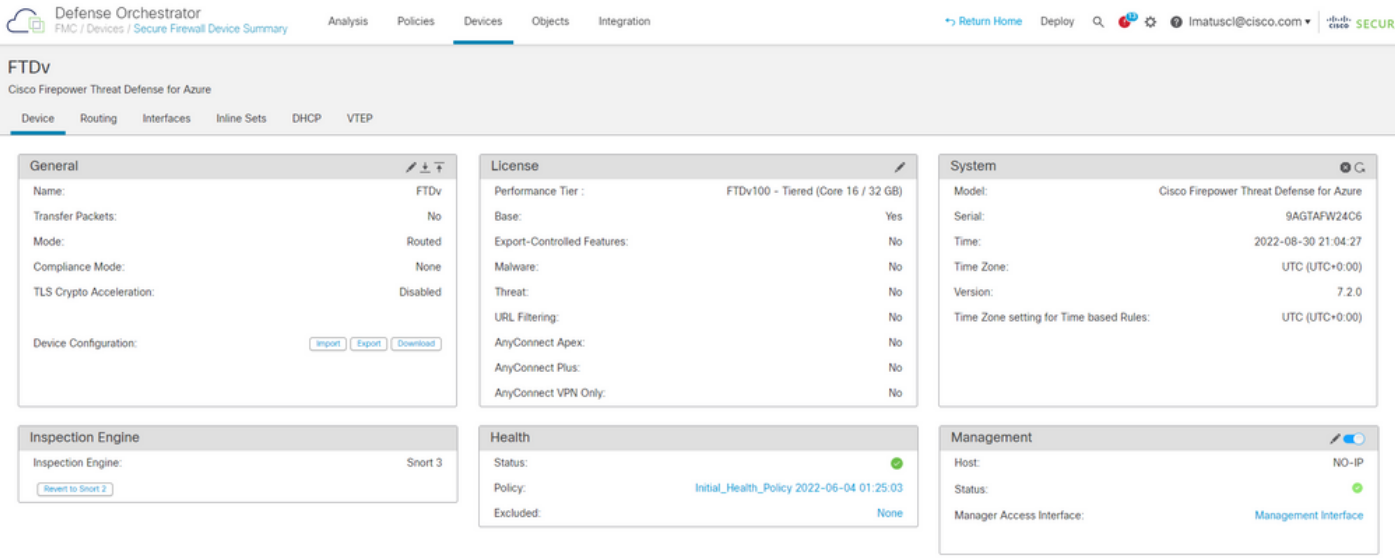
Device Details

Location	n/a
Model	Cisco Firepower Threat Defense for Azure
Serial	9AGTAFW24C6
Version	7.2.0
Onboarding Method	Registration Key
Snort Version	3.1.21.1-126

○ Synced

Your device's configuration is up-to-date.

Finalmente, navegue hasta **Device Management > Device Overview** para acceder al cdFMC y revisar el estado general del FTDv.



FTDv

Cisco Firepower Threat Defense for Azure

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

Health	
Status:	●
Policy:	Initial_Health_Policy 2022-06-04 01:25:03
Excluded:	None

Management	
Host:	NO-IP
Status:	●
Manager Access Interface:	Management Interface

Información Relacionada

- **Soporte Técnico y Documentación - Cisco Systems**
- **Gestione los dispositivos Cisco Secure Firewall Threat Defence con el centro de gestión de firewalls en la nube**

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).