

Implante um FMC fornecido em nuvem (cdFMC) no Cisco Defense Orchestrator (CDO)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Implante um Firepower Management Center fornecido em nuvem no CDO.](#)

[Integrar um FTD em um FMC oferecido em nuvem](#)

[Informações Relacionadas](#)

Introduction

Este documento descreve o processo de implantação e integração do FMC fornecido em nuvem na plataforma CDO.

Prerequisites

Requirements

A Cisco recomenda o conhecimento destes tópicos:

- Firepower Management Center fornecido em nuvem (cdFMC)
- Cisco Defense Orchestrator (CDO)
- Defesa contra ameaças do Firepower Virtual (FTDv)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- 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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

O Cisco Defense Orchestrator (CDO) é a plataforma para o Firewall Management Center (cdFMC) fornecido em nuvem. O Firewall Management Center fornecido em nuvem é um produto

de software como serviço (SaaS) que gerencia dispositivos Secure Firewall Threat Defense. Ele oferece muitas das mesmas funções que um Secure Firewall Secure Firewall Secure Firewall Threat Defense local. Ele tem a mesma aparência e comportamento de um Secure Firewall Management Center local e usa a mesma API (Application Programming Interface, interface de programação de aplicativos) do FMC.

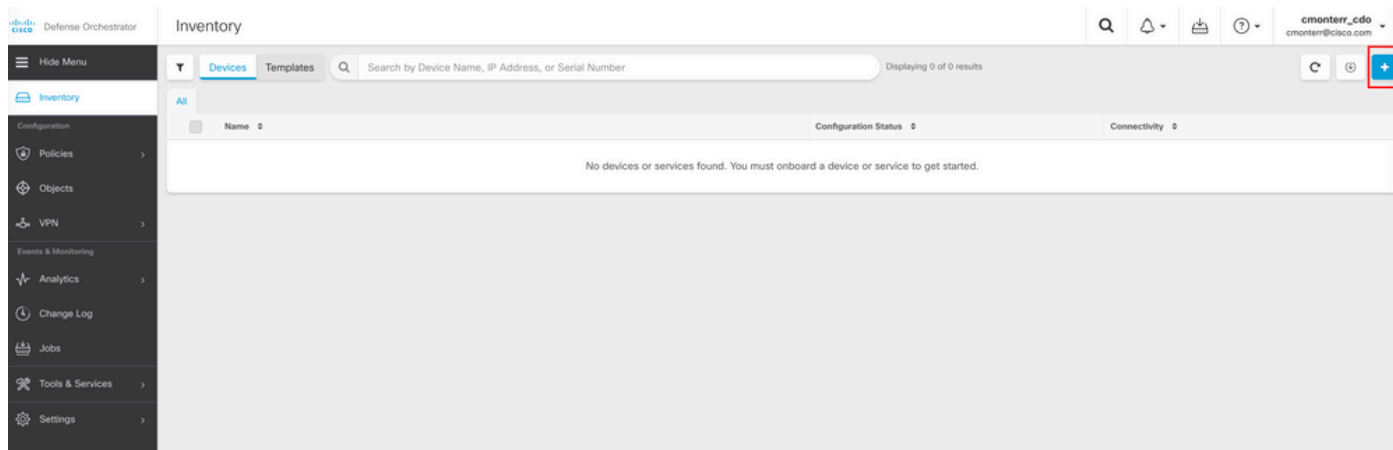
Este produto foi projetado para migração dos Secure Firewall Management Centers locais para a versão Secure Firewall Management Center SaaS.

Configurar

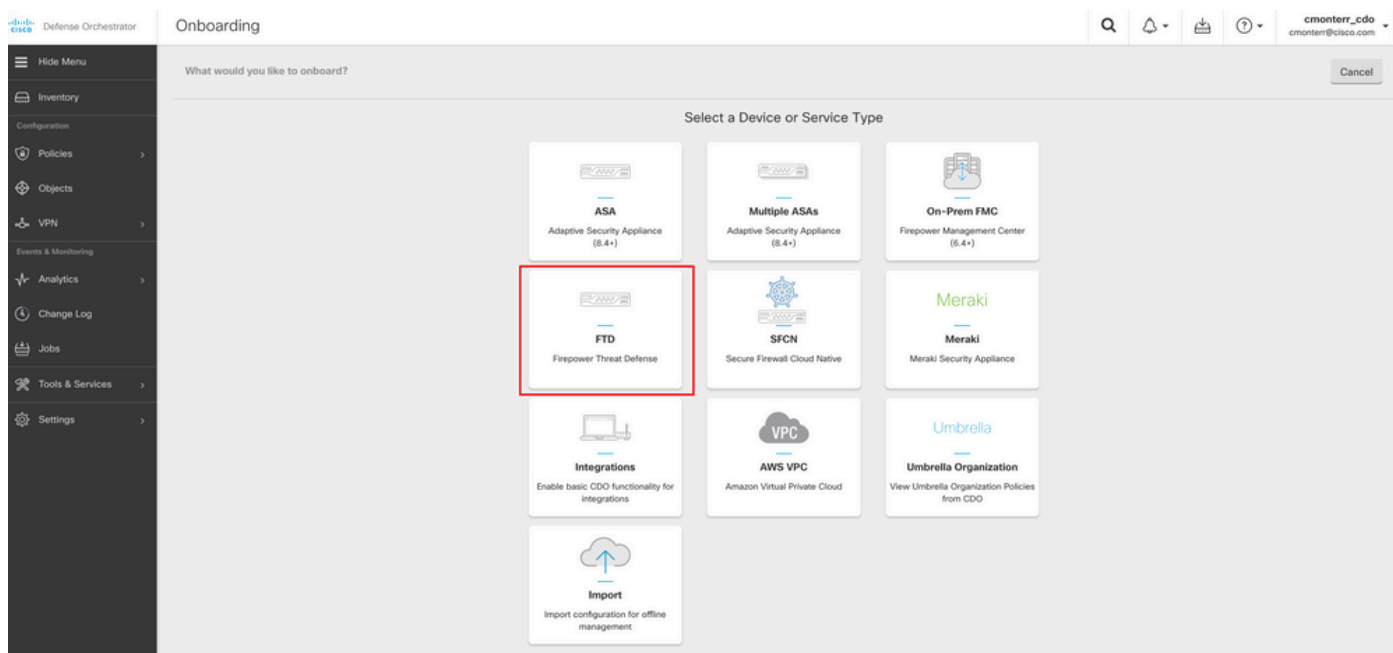
Implante um Firepower Management Center fornecido em nuvem no CDO.

Essas imagens mostram o processo de configuração inicial necessário para implantar um FMC fornecido em nuvem no CDO.

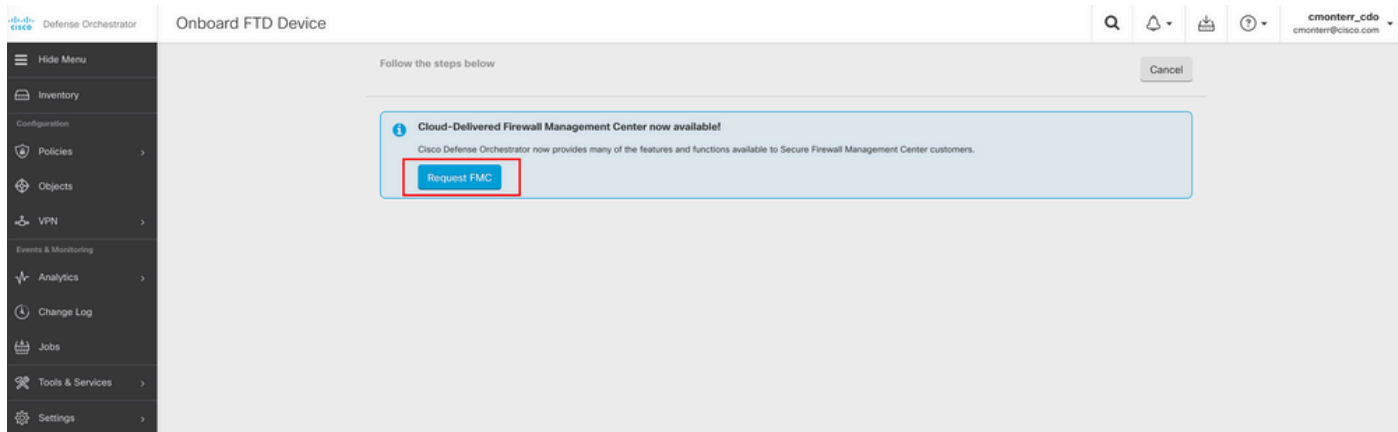
Primeiro, navegue até **Menu > Inventory** para adicionar um novo dispositivo.



Selecionar Firepower Threat Defense (FTD).

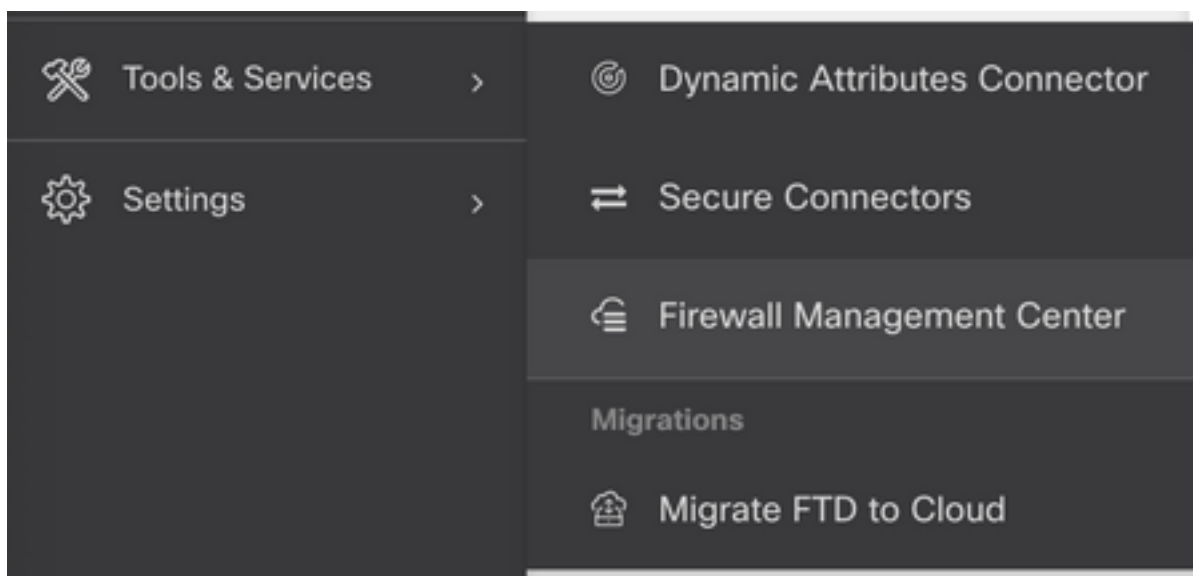


Selecionar **Request FMC** para solicitar o Firepower Management Center fornecido pela nuvem.

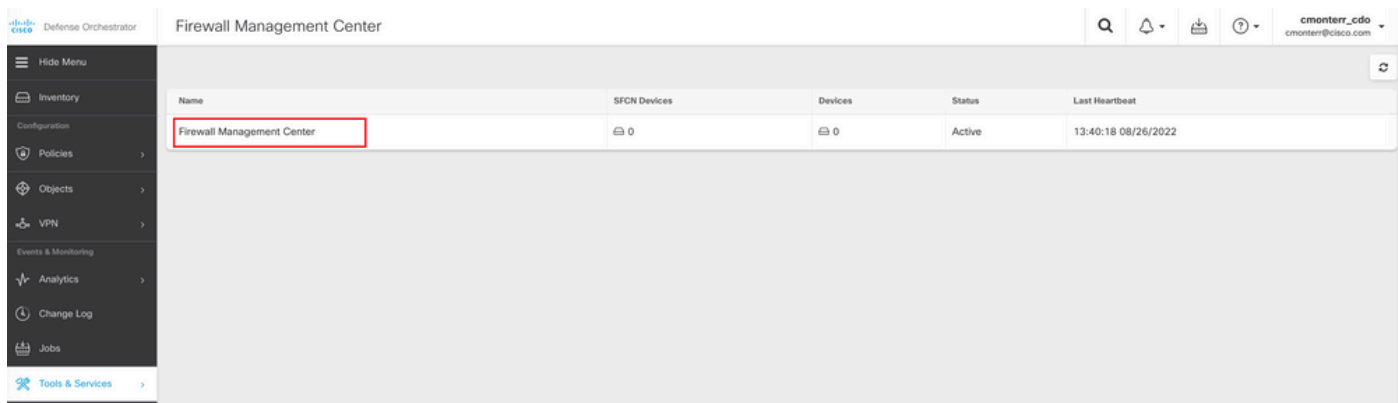


Observação: a opção "Solicitar FMC" será apresentada somente se você não tiver nenhum cdFMC no espaço.

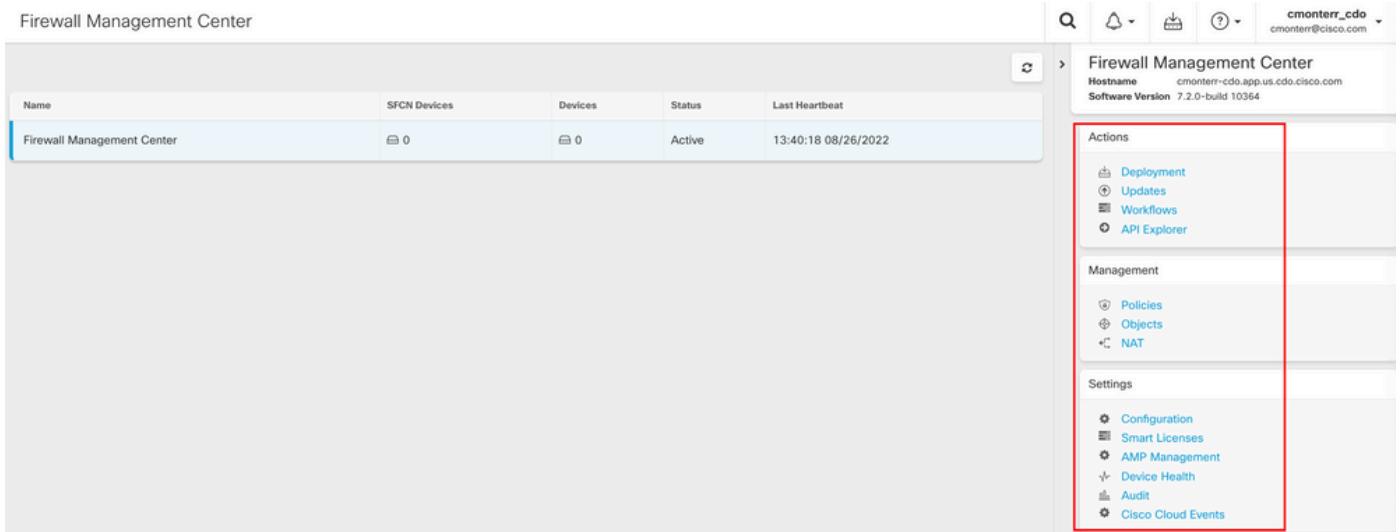
Navegue até Menu > Tools & Services > Firewall Management Center quando o cdFMC estiver pronto para uso.



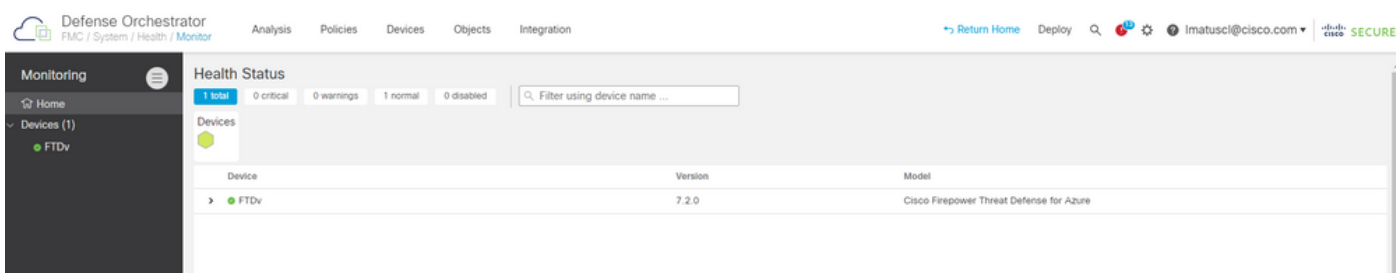
Selecione o cdFMC desejado para exibir as informações do cdFMC.



Para acessar a interface gráfica do usuário (GUI) do cdFMC, selecione qualquer uma das opções disponíveis no lado direito.



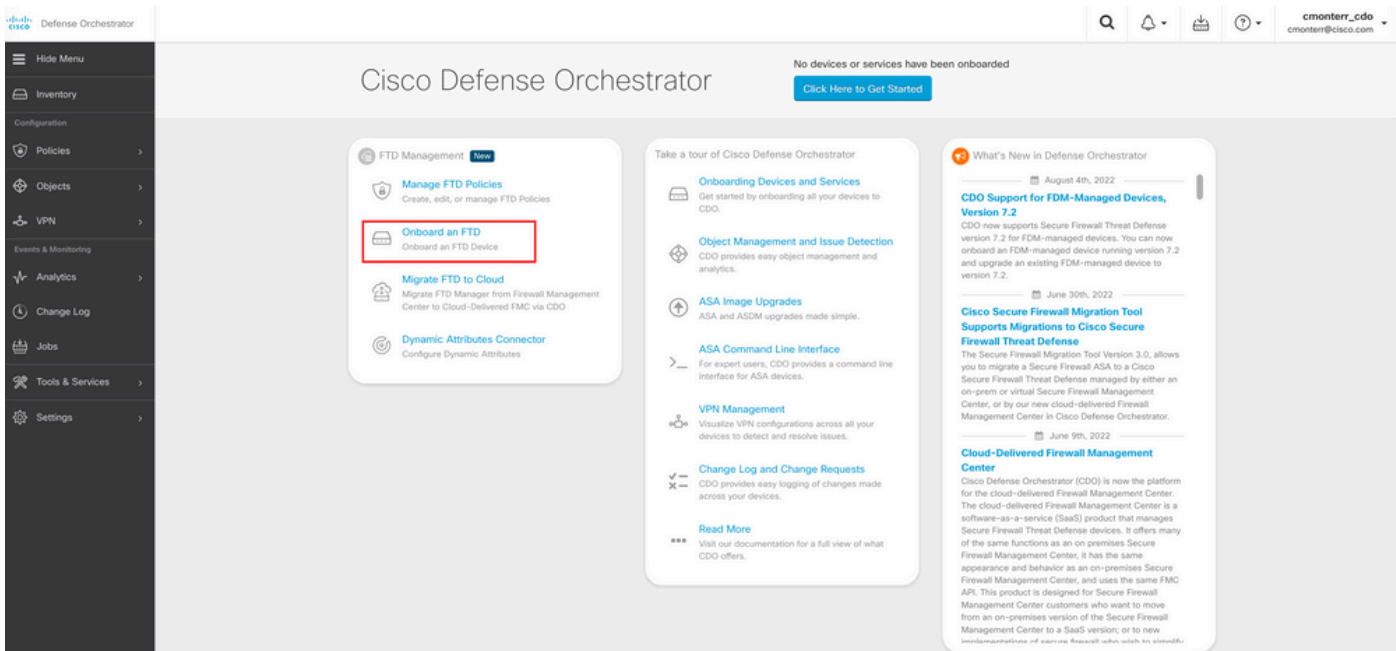
Agora você pode ver a GUI do cdFMC.



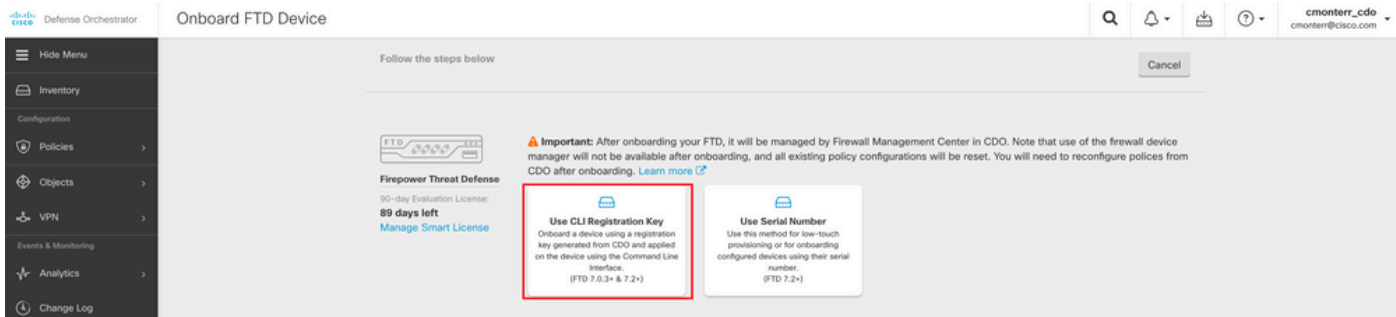
Integrar um FTD em um FMC oferecido em nuvem

Essas imagens mostram como integrar um FTD para ser registrado em um cdFMC com a chave de registro da Interface de Linha de Comando (CLI).

Primeiro, selecione **onboard an FTD** na página inicial do CDO.



Em seguida, selecione a opção **Use CLI Registration Key** opção.



Continue para inserir as informações de FTDv solicitadas e desejadas.

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](#)

i 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 fim, o cdFMC cria um CLI keyChave CLI do 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
```

[Next](#)

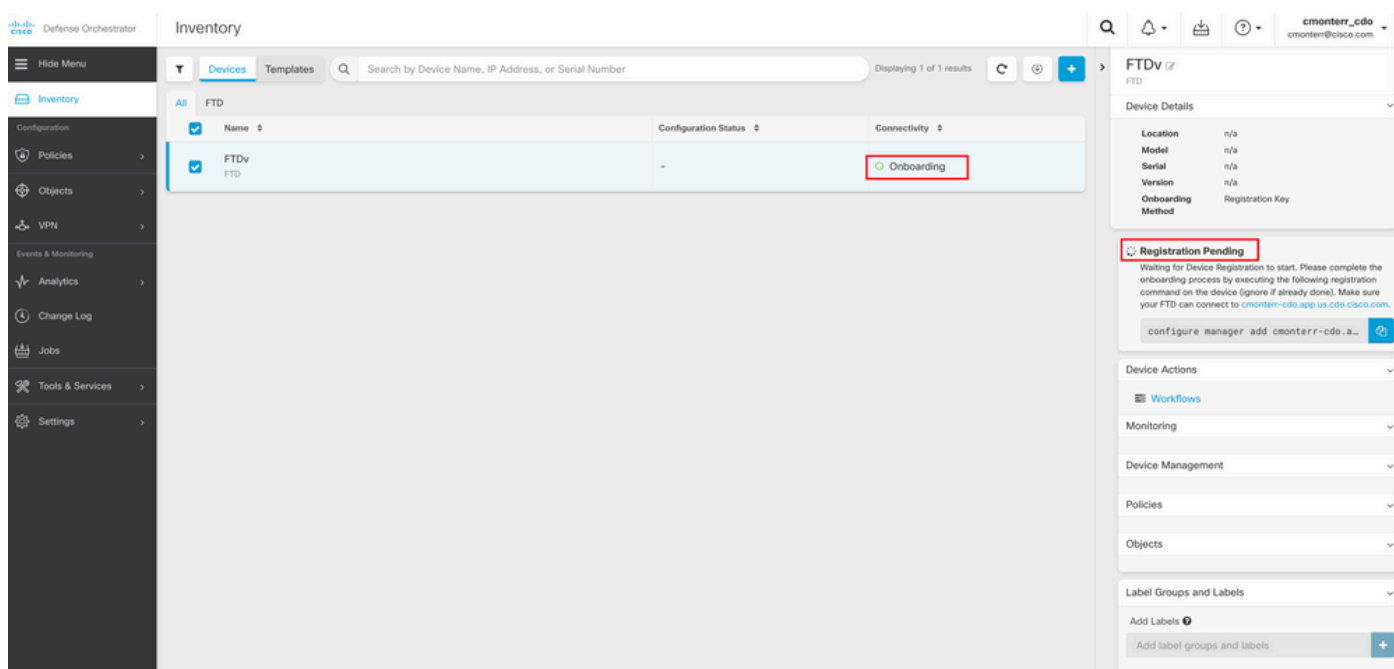
Copie o CLI key na CLI do dispositivo gerenciado.

```
> 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
```

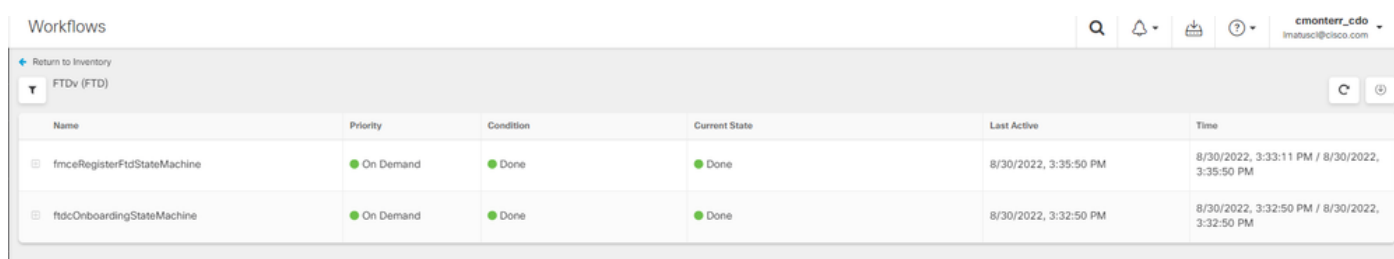
O cdFMC inicia uma tarefa de registro.



Observação: certifique-se de que o dispositivo FTD tenha comunicação nas portas 8305 (sftunnel) e 443 com o locatário CDO para concluir o processo de registro. Consulte todos os [requisitos de rede](#).

Observação: se você não conseguir se conectar ao host, poderá retificar a configuração DNS no FTD-CLI com este comando: `configure network dns <address>`.

Para monitorar o processo de registro, navegue até **Device Actions > Workflows..**



Expanda a **Active** para obter informações adicionais, essas imagens mostram como o FTDv foi registrado com êxito.

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

Por fim, navegue até **Device Management > Device Overview** para acessar o cdFMC e revisar o status de visão geral do 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>

Informações Relacionadas

- [Suporte Técnico e Documentação - Cisco Systems](#)
- [Gerencie dispositivos de defesa contra ameaças do Cisco Secure Firewall com o Centro de gerenciamento de firewall fornecido em nuvem](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.