

在思科防御协调器(CDO)中部署云交付的FMC (cdFMC)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[配置](#)

[在CDO上部署云交付的Firepower管理中心。](#)

[在云交付的FMC上注册FTD](#)

[相关信息](#)

简介

本文档介绍云交付FMC在CDO平台上的部署和入网流程。

先决条件

要求

建议掌握下列主题的相关知识：

- 云交付的Firepower管理中心(cdFMC)
- 思科防御协调器(CDO)
- Firepower威胁防御虚拟(FTDv)

最低FTD版本7.0.3

使用的组件

本文档中的信息基于以下软件和硬件版本：

- cdFMC
- FTDv 7.2.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

Cisco Defense Orchestrator (CDO)是云交付的防火墙管理中心(cdFMC)的平台。云交付的防火墙管理中心是一种软件即服务(SaaS)产品，用于管理安全防火墙威胁防御设备。它提供的许多功能与本地安全防火墙安全防火墙威胁防御功能相同。它具有与本地安全防火墙管理中心相同的外观和行为，并使用相同的FMC应用编程接口(API)。

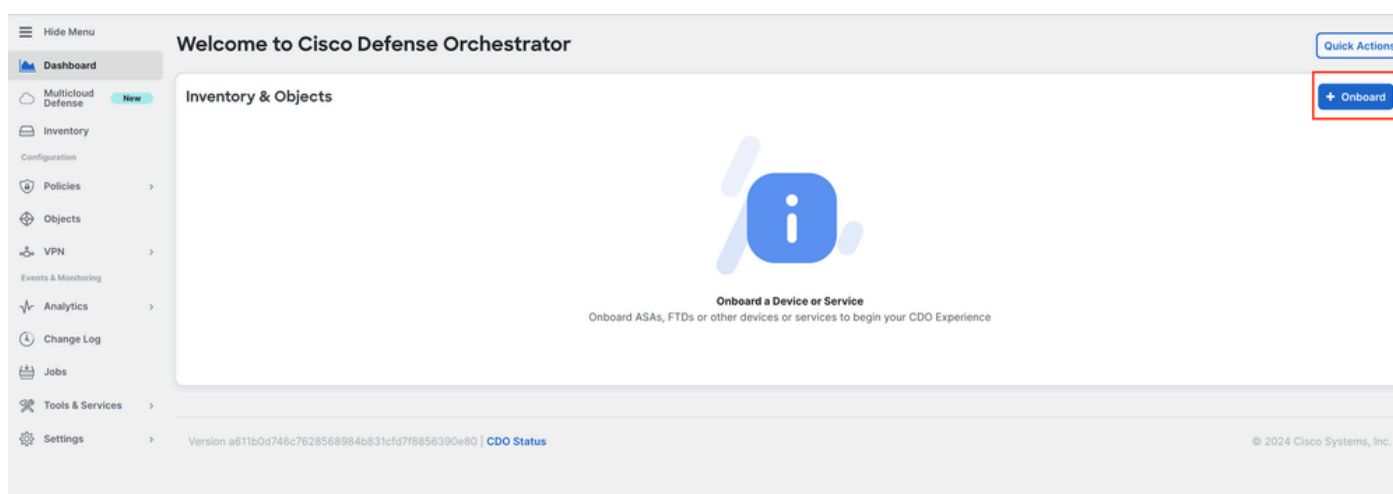
此产品旨在从本地安全防火墙管理中心迁移到安全防火墙管理中心SaaS版本。

配置

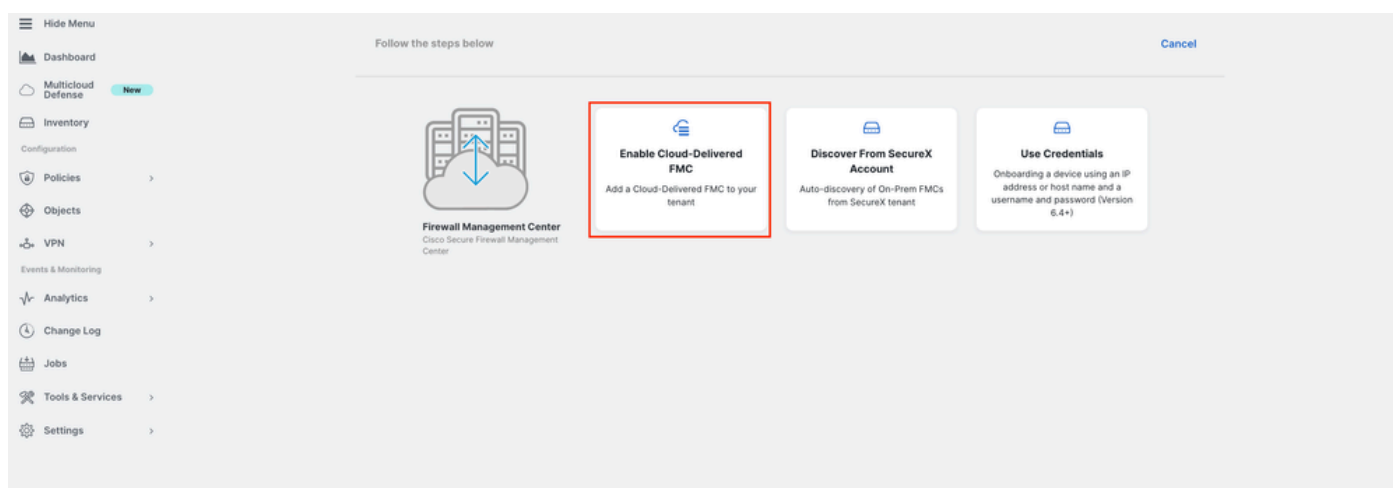
在CDO上部署云交付的Firepower管理中心。

这些图片显示了在CDO上部署云交付的FMC所需的初始设置流程。

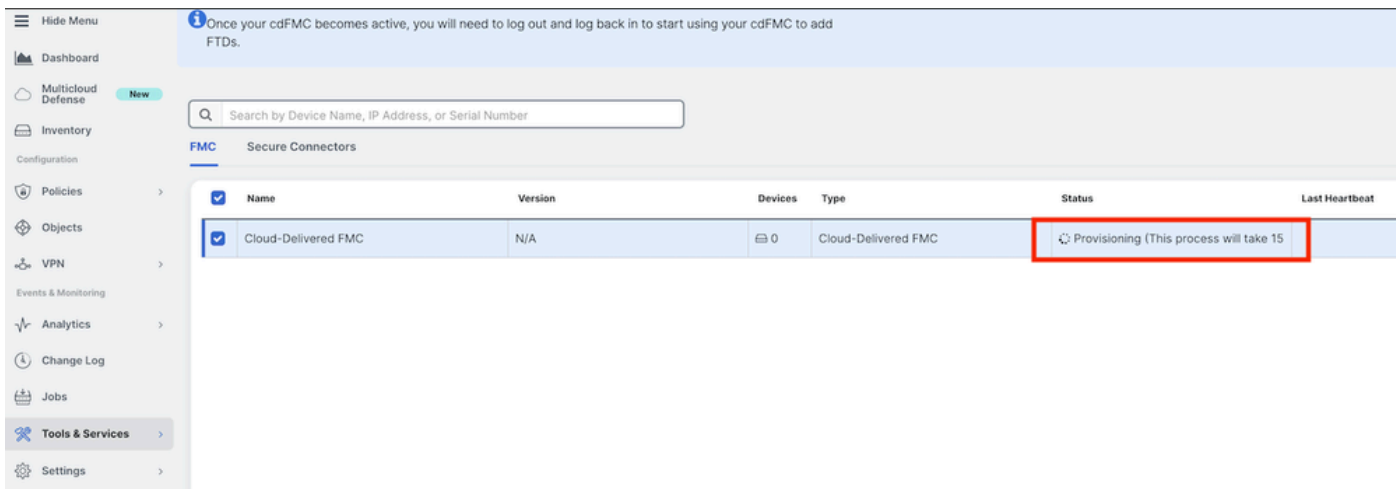
从CDO菜单导航至 **Tools & Services > Firewall Management Center > Onboard**。



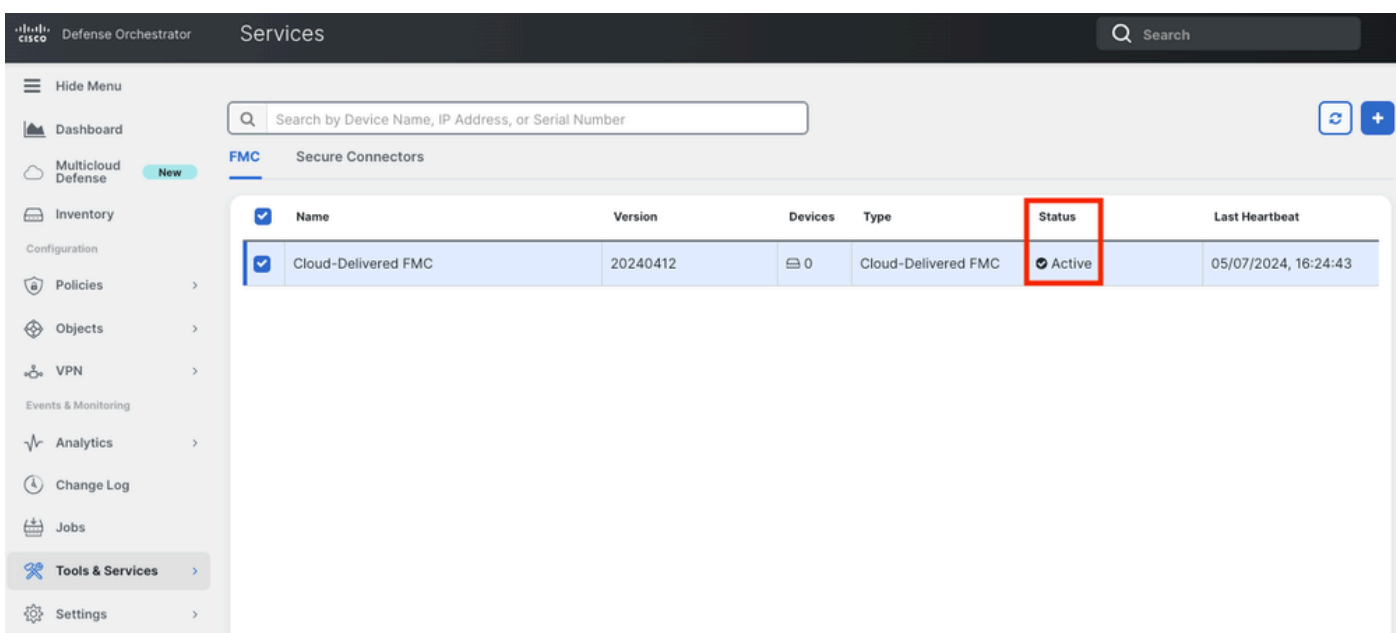
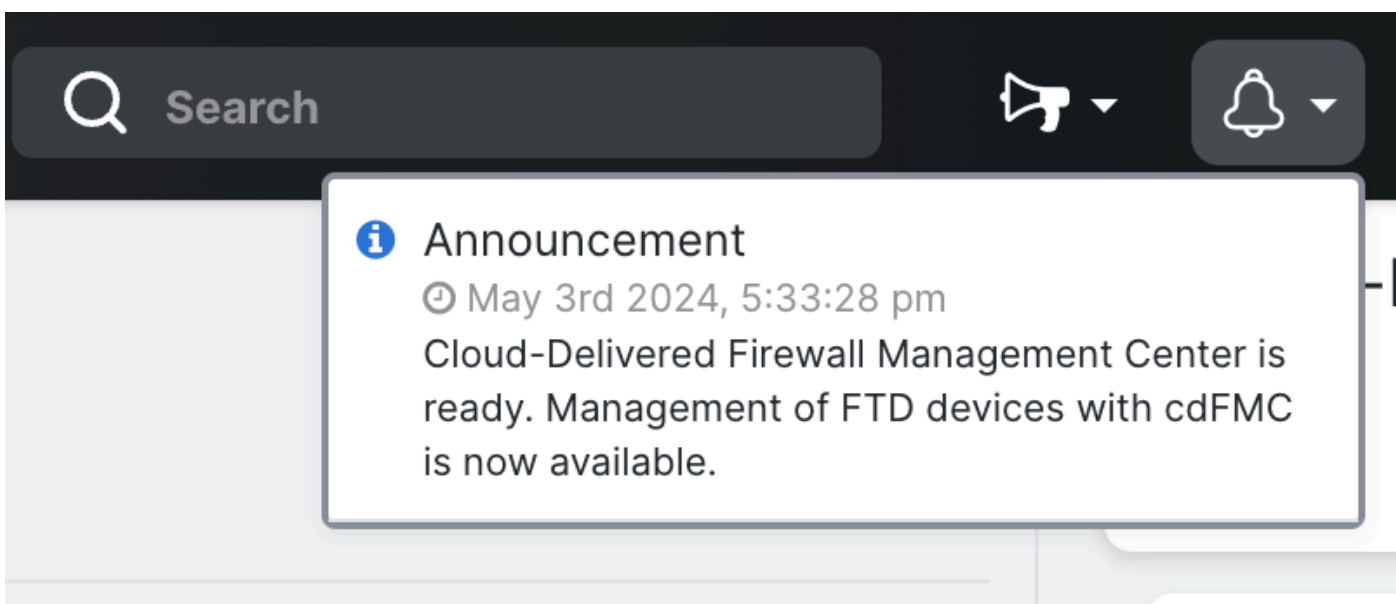
选择 **Enable Cloud-Delivered FMC**。



CDO在后台预置云交付的防火墙管理中心实例；完成此过程通常需要15至30分钟。您可以在云交付FMC的Status (状态) 列中跟踪调配进度。

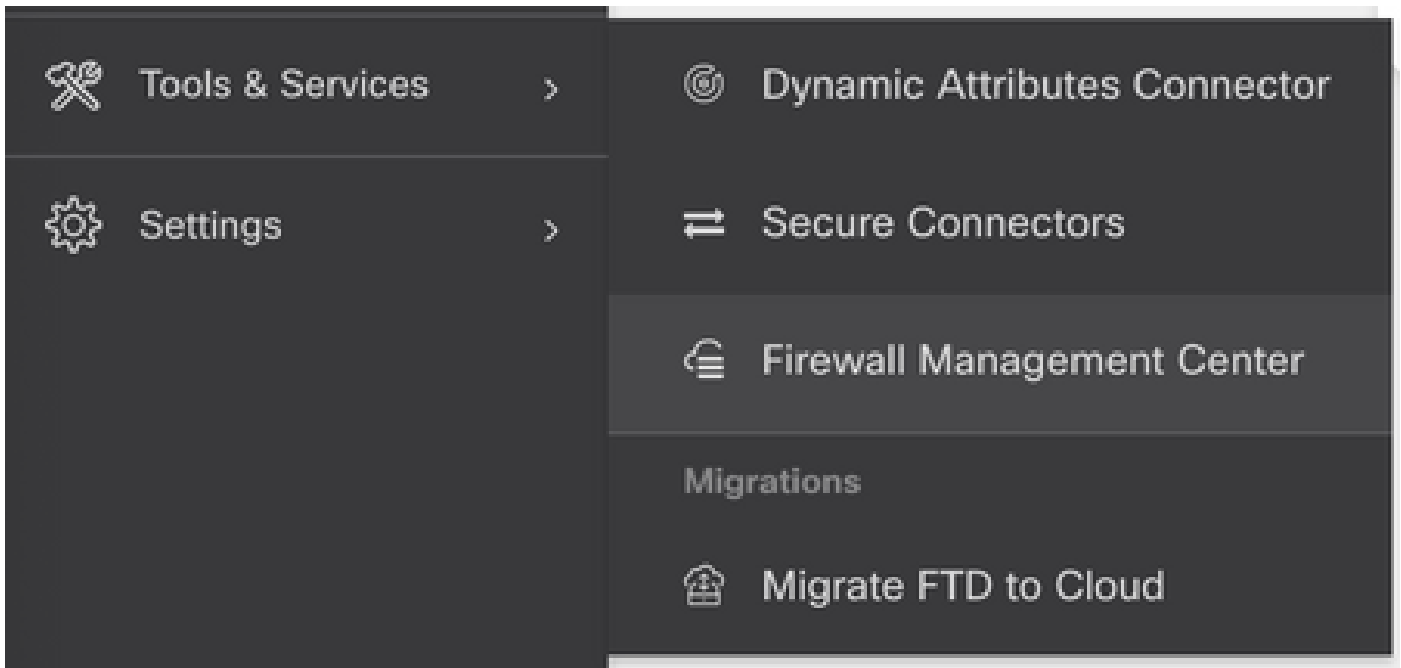


调配完成后，状态会变为“活动”。此外，您还会在CDO通知面板上收到云交付的防火墙管理中心就绪通知。

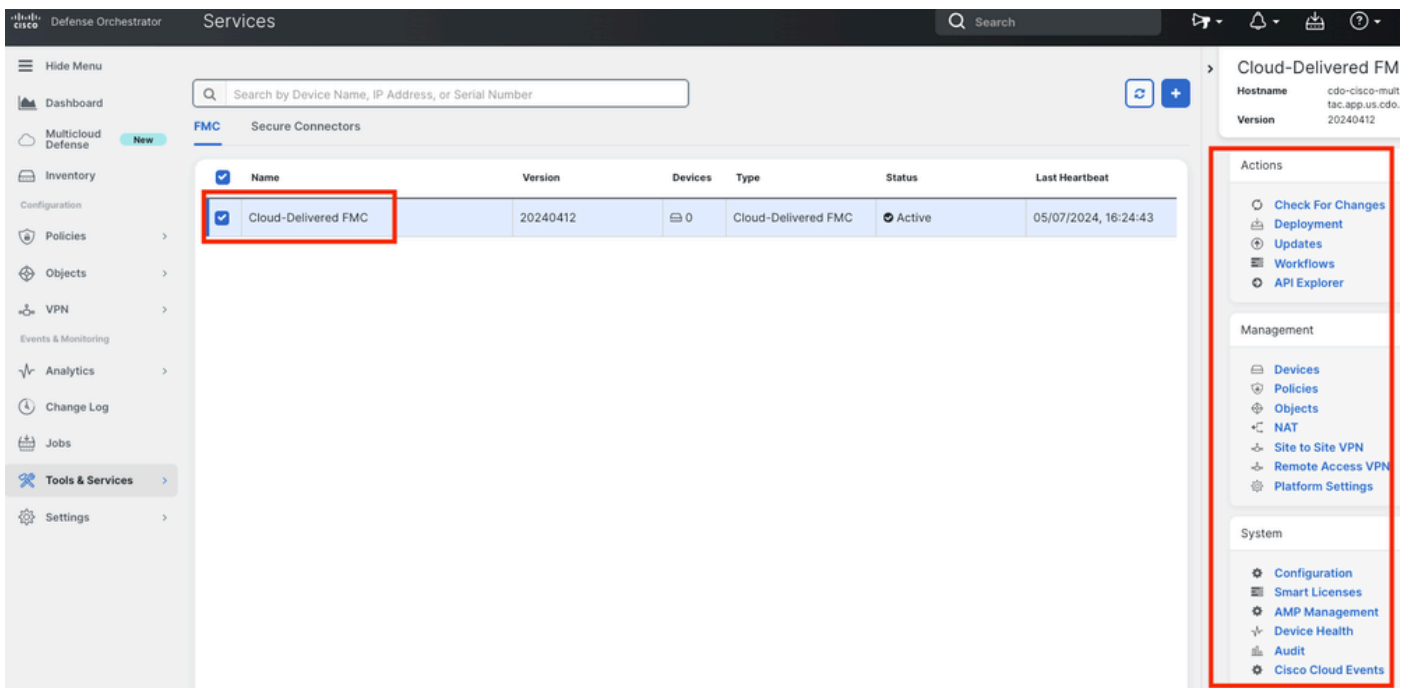


然后，您可以将威胁防御设备安装到云交付的防火墙管理中心并对其进行管理。

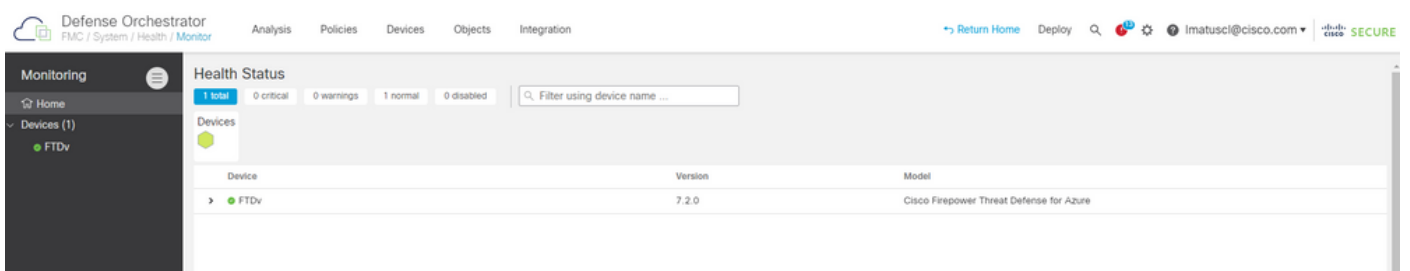
导航到Menu > Tools & Services > Firewall Management Center。



选择cdFMC以显示cdFMC信息，为了访问cdFMC的图形用户界面(GUI)，请选择右侧可用的任何选项。



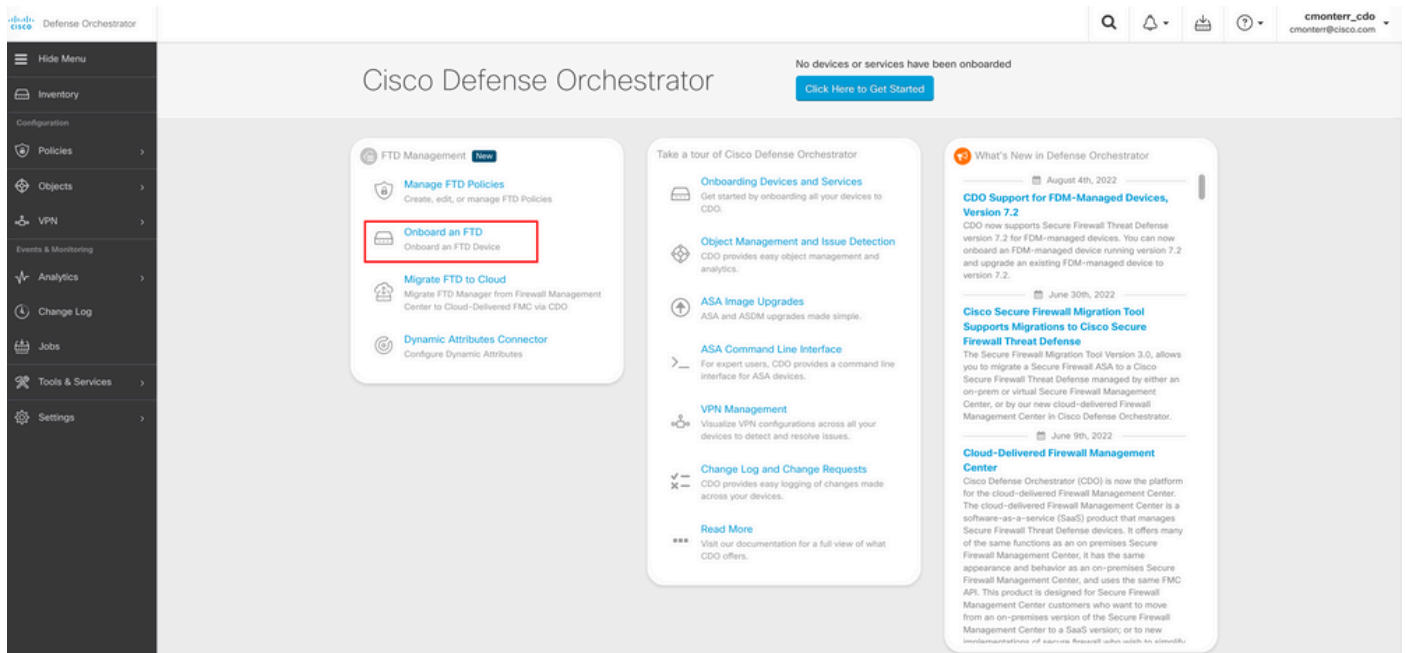
现在您可以看到cdFMC GUI。



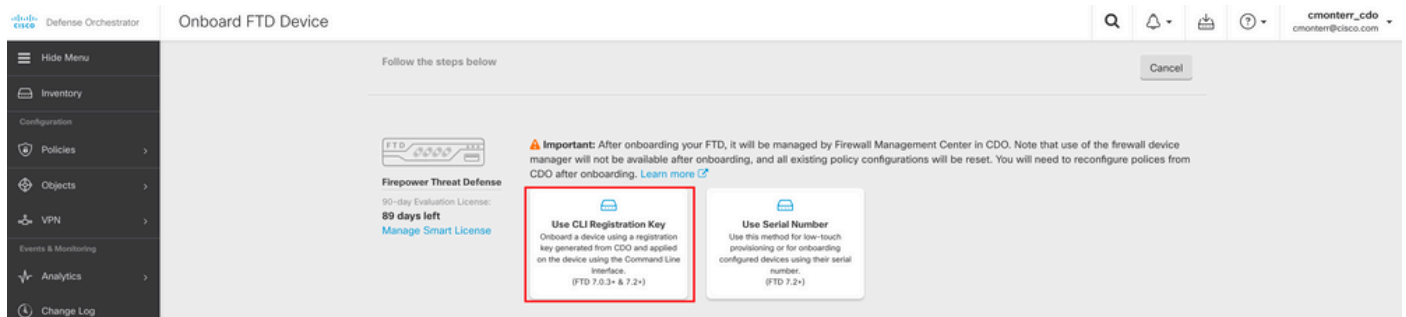
在云交付的FMC上注册FTD

这些映像显示了如何使用Command Line Interface (CLI)注册密钥注册FTD，以便在cdFMC上注册。

首先，在CDO主页上选择 **Onboard an FTD**。



然后，选择**Use CLI Registration Key** 选项。



继续输入请求和所需的FTDv信息。

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.

最后，cdFMC会为您的设备创建特 CLI Key定的。

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

将 CLI Key 复制到受管设备的CLI中。

```
> 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
```

cdFMC启动注册任务。

The screenshot shows the 'Inventory' page in Cisco Defense Orchestrator. A table lists one device, 'FTDv', with a status of 'Onboarding'. The right-hand sidebar displays 'Device Details' and a 'Registration Pending' section with instructions: '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.' A button labeled 'configure manager add cmonterr-cdo.a...' is visible.

注意：确保您的FTD设备能够通过端口8305 (sftunnel)和443与CDO租户通信，以便完成注册过程。查看完整的[网络要求](#)。

注意：如果无法连接到主机，则可以使用以下命令纠正FTD-CLI中的DNS配置：`configure network dns <address>`。

要监控注册过程，请导航到Device Actions > Workflows。

The screenshot shows the 'Workflows' page. A table lists two 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

展开状 Active 态以获得其他信息，这些图片显示了FTDv是如何成功注册的。

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		
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

最后，导航到Device Management > Device Overview 以访问cdFMC并查看FTDv概述状态。

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: 9AGTAFW2406 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

相关信息

- [技术支持和文档 - Cisco Systems](#)
- [通过云交付的防火墙管理中心管理思科安全防火墙威胁防御设备](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。