

在Cisco Defense Orchestrator (CDO)中部署雲交付的FMC (cdFMC)

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[在CDO上部署雲交付的Firepower管理中心。](#)

[在雲交付的FMC上安裝FTD](#)

[相關資訊](#)

簡介

本文檔介紹CDO平台上雲交付FMC的部署和板載過程。

必要條件

需求

思科建議瞭解以下主題：

- 雲端提供的Firepower管理中心(cdFMC)
- Cisco Defense Orchestrator (CDO)
- Firepower威脅防禦虛擬(FTDv)

最低FTD版本7.0.3

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- cdFMC
- FTDv 7.2.0

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

Cisco Defense Orchestrator (CDO)是雲交付防火牆管理中心(cdFMC)的平台。雲交付的防火牆管理中心是一種軟體即服務(SaaS)產品，用於管理安全防火牆威脅防禦裝置。它提供的許多功能與內部安全防火牆安全防火牆威脅防禦功能相同。其外觀和行為與本地安全防火牆管理中心相同，並使用相同的FMC應用程式設計介面(API)。

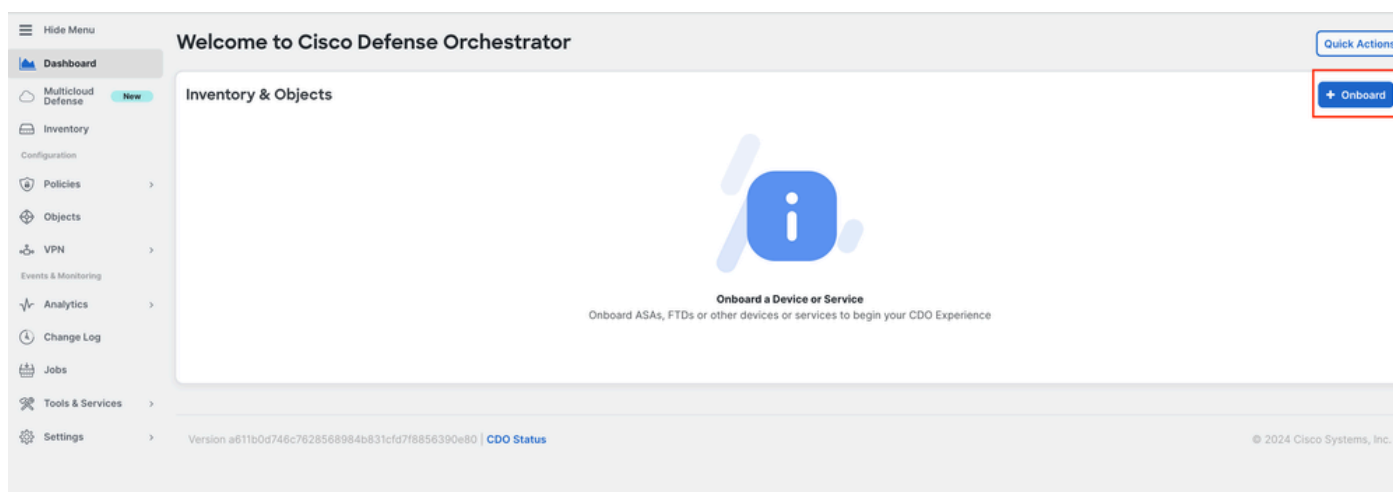
本產品旨在從內部部署的安全防火牆管理中心遷移到安全防火牆管理中心SaaS版本。

設定

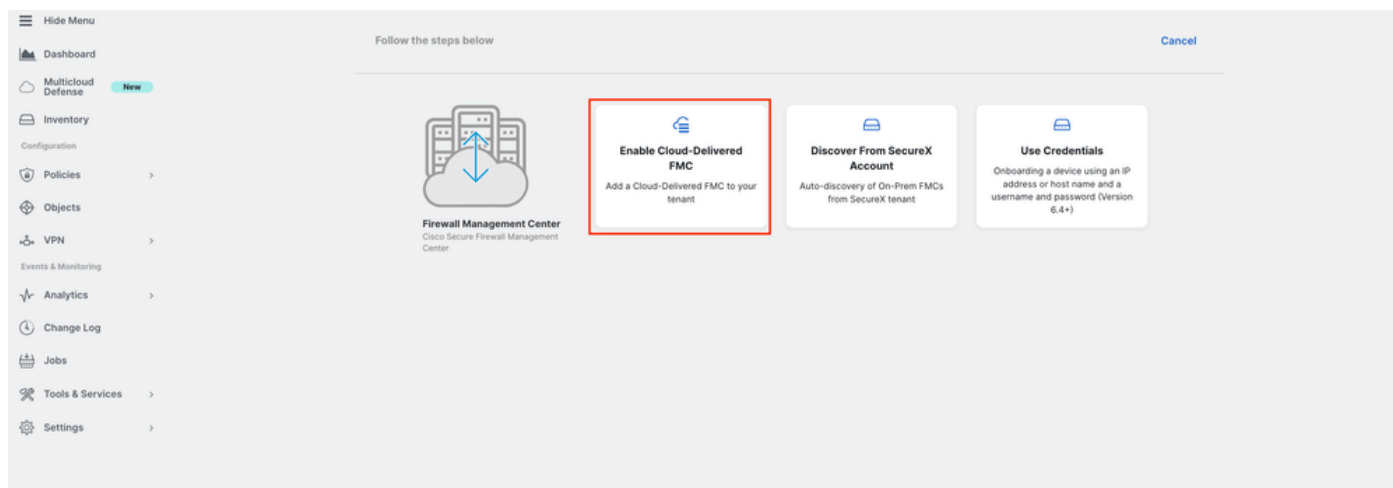
在CDO上部署雲交付的Firepower管理中心。

這些圖片顯示了在CDO上部署雲交付的FMC所需的初始設定過程。

從CDO功能表，瀏覽至 **Tools & Services > Firewall Management Center > Onboard**。

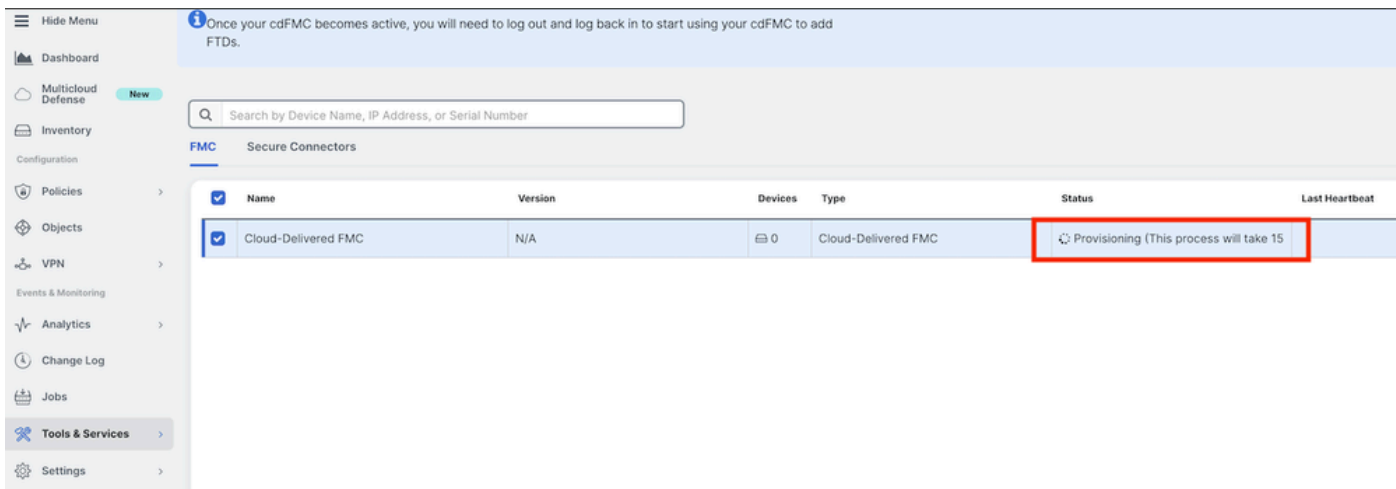


選取 **Enable Cloud-Delivered FMC**。

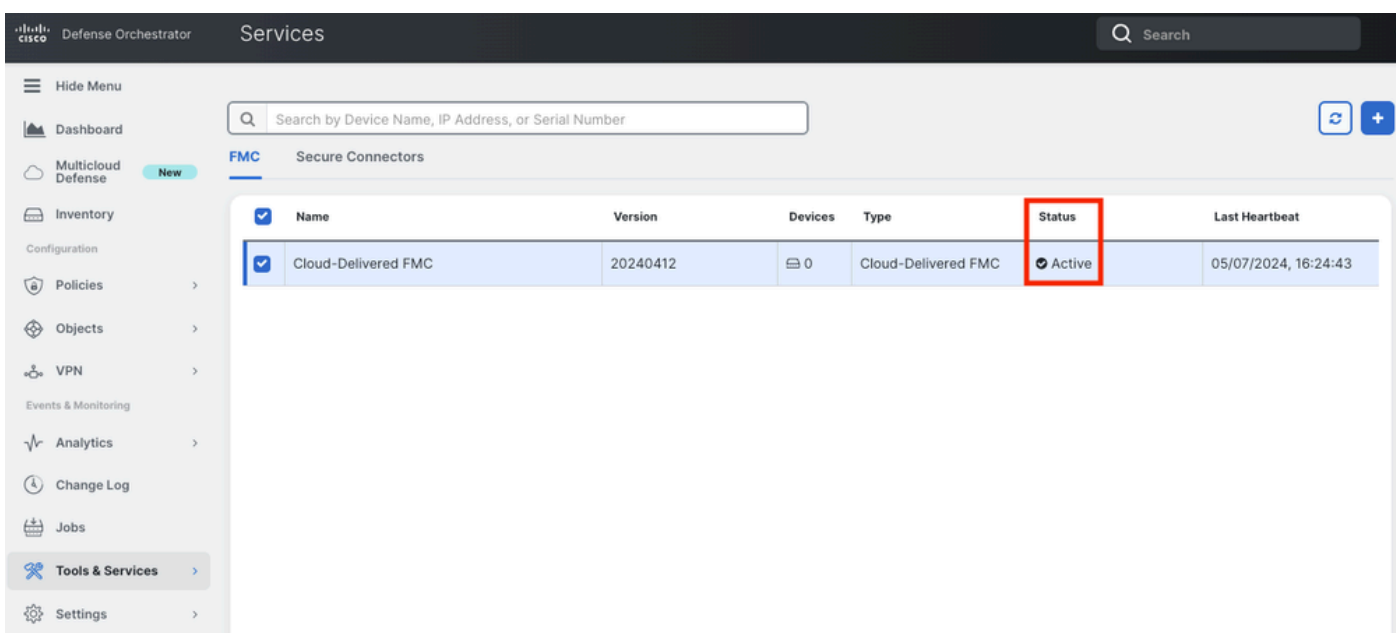


CDO在後台提供雲交付的防火牆管理中心例項；完成此過程通常需要15到30分鐘。您可以在雲交付的FMC的Status列上跟蹤調配進度。

。

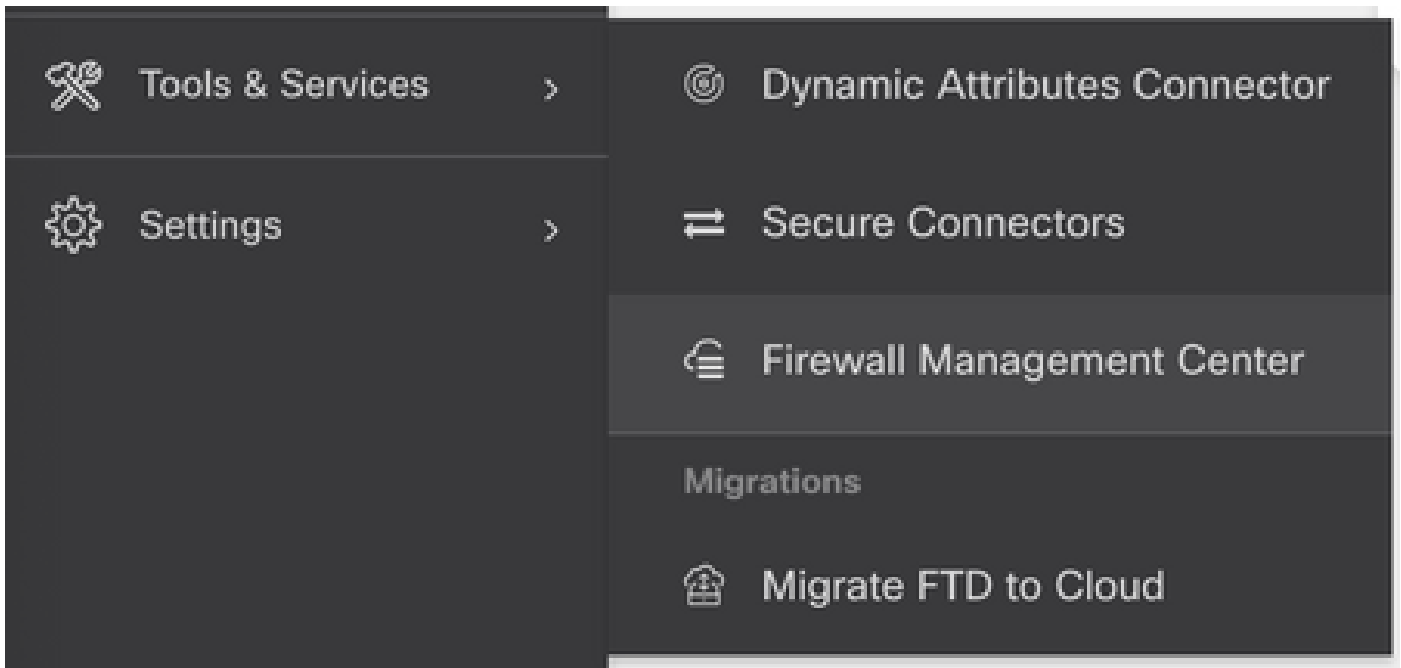


布建完成後，狀態會變更為「作用中」。此外，您還會在CDO通知面板上收到雲交付的防火牆管理中心就緒通知。

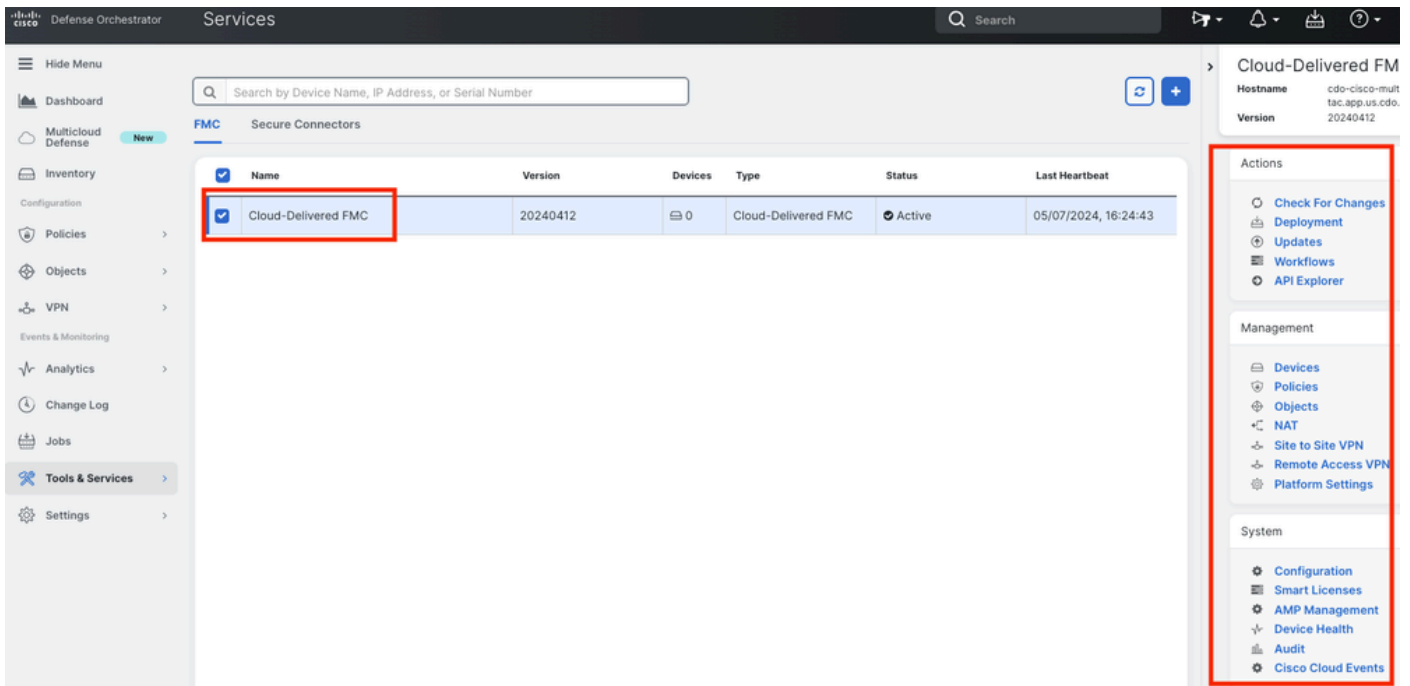


然後，您可以將威脅防禦裝置安裝到雲交付的防火牆管理中心並進行管理。

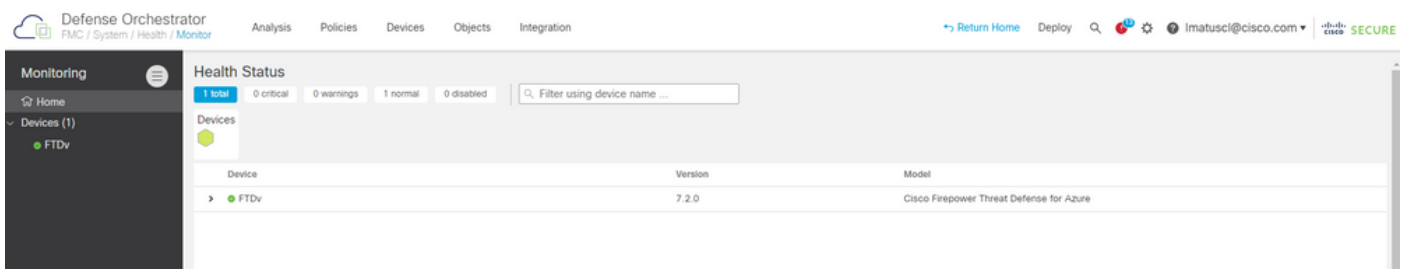
導航到Menu > Tools & Services > Firewall Management Center。



選擇cdFMC以顯示cdFMC資訊，並且要訪問cdFMC的圖形使用者介面(GUI)，請選擇右側可用的任何選項。



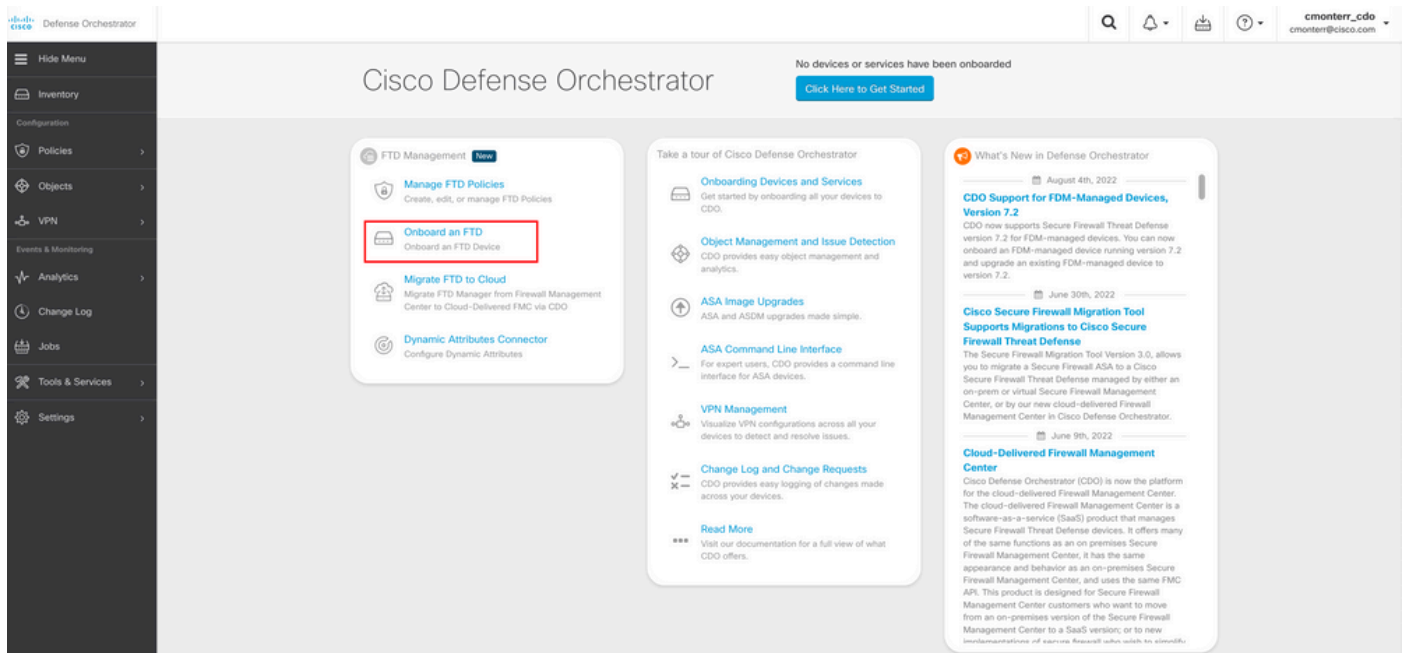
現在您可以看到cdFMC GUI。



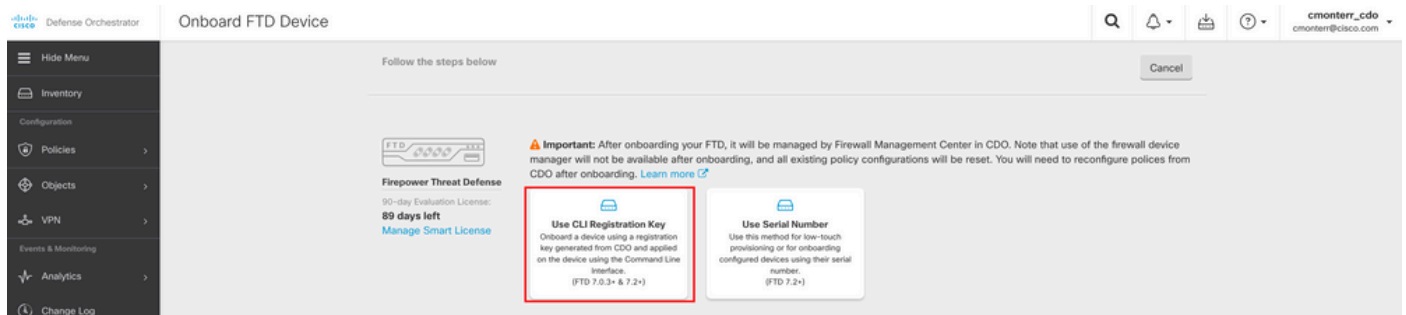
在雲交付的FMC上安裝FTD

以下影像顯示如何內建FTD，以便使用指令行介面(CLI)註冊金鑰在cdFMC上註冊。

首先，在CDO首頁上選擇 **Onboard an FTD** 該選項。



然後，選擇**Use CLI Registration Key** 選項。



繼續輸入請求和所需的FTDv資訊。

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.

最後，cdFMC會為您的裝置建 CLI Key立特定的。

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

將 CLI Key 複製到受管裝置的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會啟動註冊任務。

The screenshot shows the Cisco Defense Orchestrator (CDO) interface. In the 'Inventory' section, a table lists devices. One device, 'FTDv', is highlighted with a red box around the 'Onboarding' status in the 'Connectivity' column. To the right, the 'Device Details' for 'FTDv' are shown, with a red box around the 'Registration Pending' status and a message: '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.cisco.com.' Below this, there is a 'configure manager add cmonterr-cdo.a...' button.

注意：請確保FTD裝置透過埠8305 (sftunnel)和443與CDO租戶通訊，以便完成註冊過程。檢視完整的[網路要求](#)。

注意：如果您無法連線到主機，則可以使用以下命令修正FTD-CLI中的DNS組態：設定網路dns <位址>。

要監控註冊過程，請導航到Device Actions > Workflows。

The screenshot shows the 'Workflows' page in CDO. It displays a table with two workflows that have completed successfully. The table has columns for Name, Priority, Condition, Current State, Last Active, and Time.

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

展開 Active 狀態以取得其他資訊，這些圖片顯示FTDv已成功註冊的方式。

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 Displaying 1 of 1 results

All FTD

Name	Configuration Status	Connectivity
FTDv FTD	○ Synced	● Online

FTDv
FTD

Device Details

Location: n/a
Model: Cisco Firepower Threat Defense for Azure
Serial: 9AGTAPW24C6
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

最後，導航到Device Management > Device Overview 以訪問cdFMC並檢視FTDv概述狀態。

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

相關資訊

- [技術支援與文件 - Cisco Systems](#)
- [使用雲交付的防火牆管理中心管理思科安全防火牆威脅防禦裝置](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。