

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

本文檔介紹雲交付的FMC在CDO平台上的部署和板載流程。

必要條件

需求

思科建議瞭解以下主題：

- 雲端交付的Firepower管理中心(cdFMC)
- Cisco Defense Orchestrator(CDO)
- Firepower威脅防禦虛擬(FTDv)

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- cdFMC 7.2.0
- 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)是雲交付的防火牆管理中心(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本地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)。

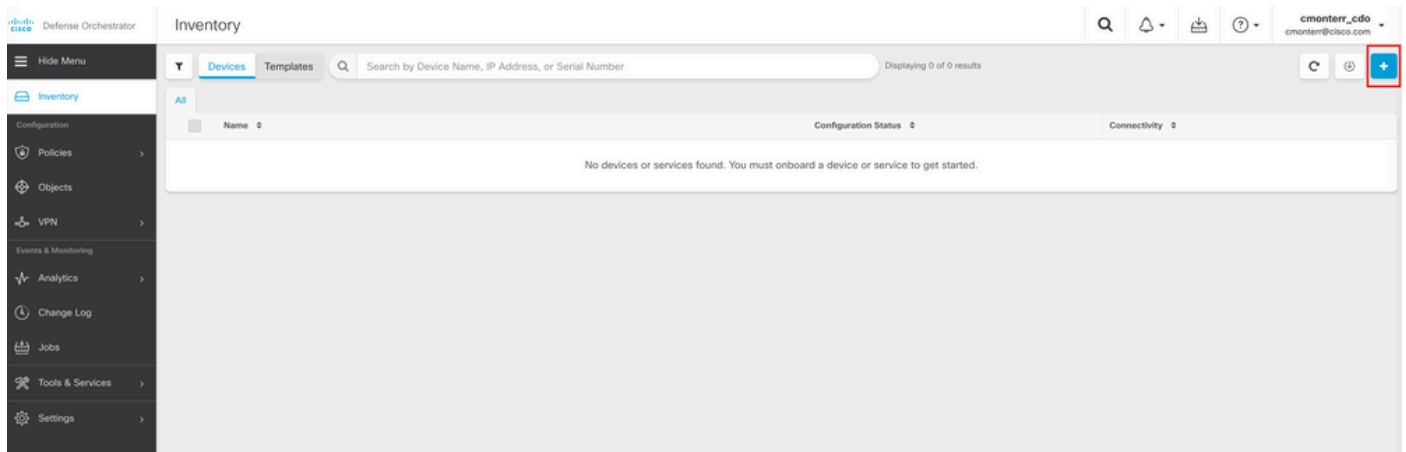
此產品旨在從內部部署的安全防火牆管理中心遷移到Secure Firewall Management Center SaaS版本。

設定

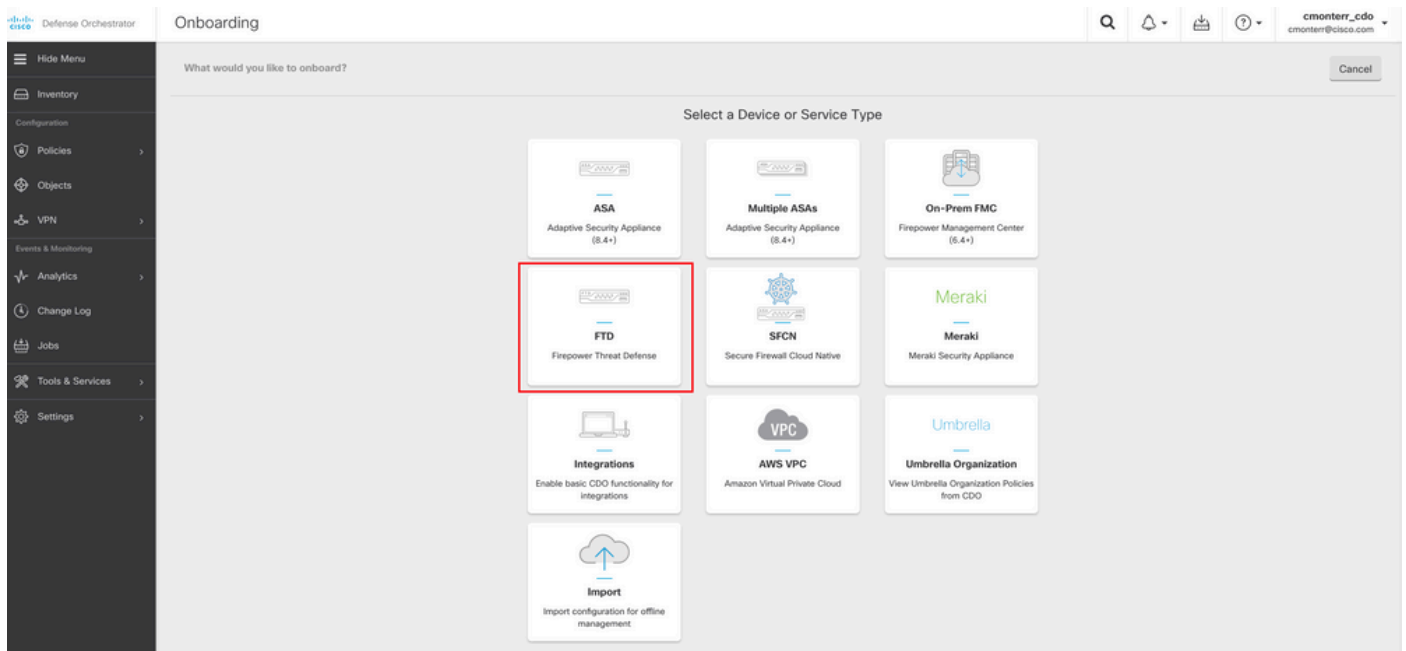
在CDO上部署雲交付的Firepower管理中心。

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。

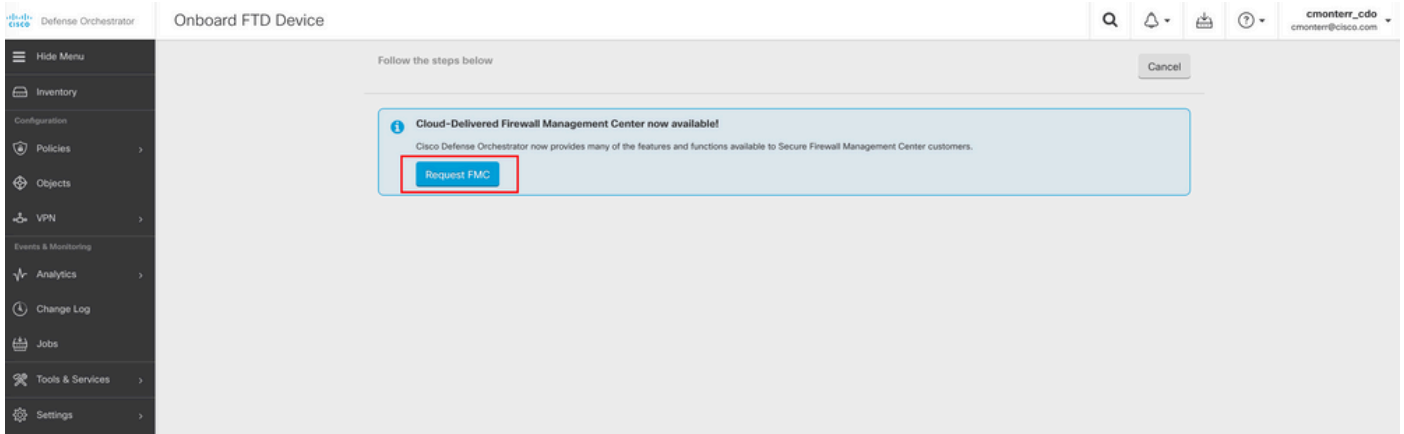
首先，導航至 **Menu > Inventory** 以便新增新裝置。



選擇 **Firepower Threat Defense (FTD)**.

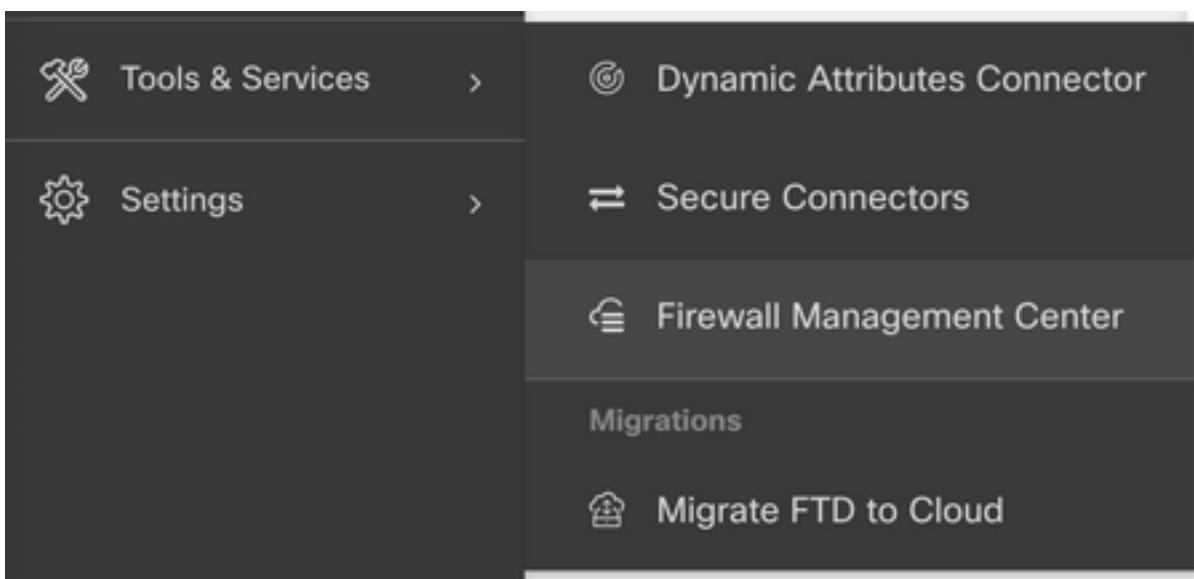


選擇 **Request FMC** 請求雲交付的Firepower管理中心。

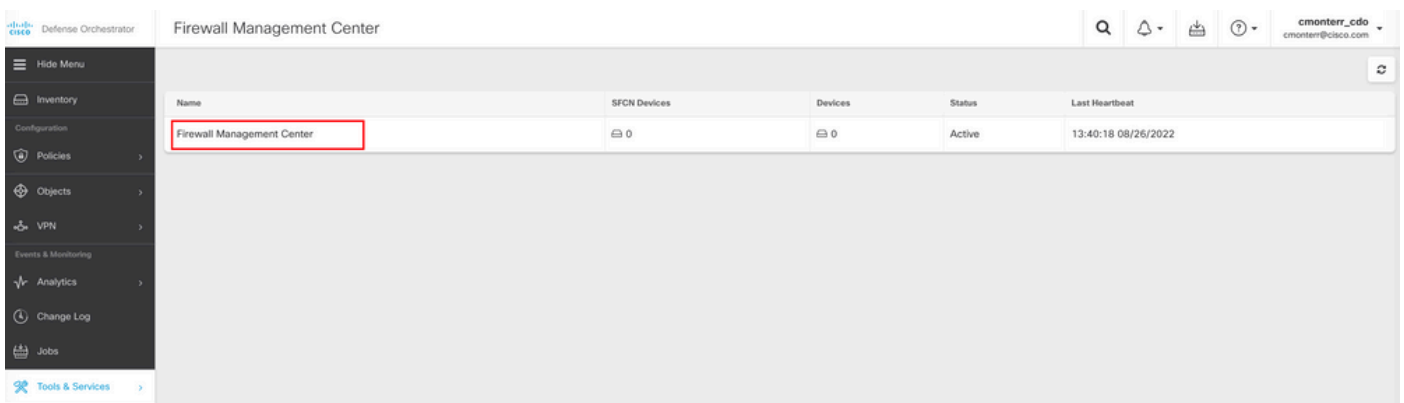


註：只有在租戶中沒有任何cdFMC時，才會顯示「請求FMC」選項。

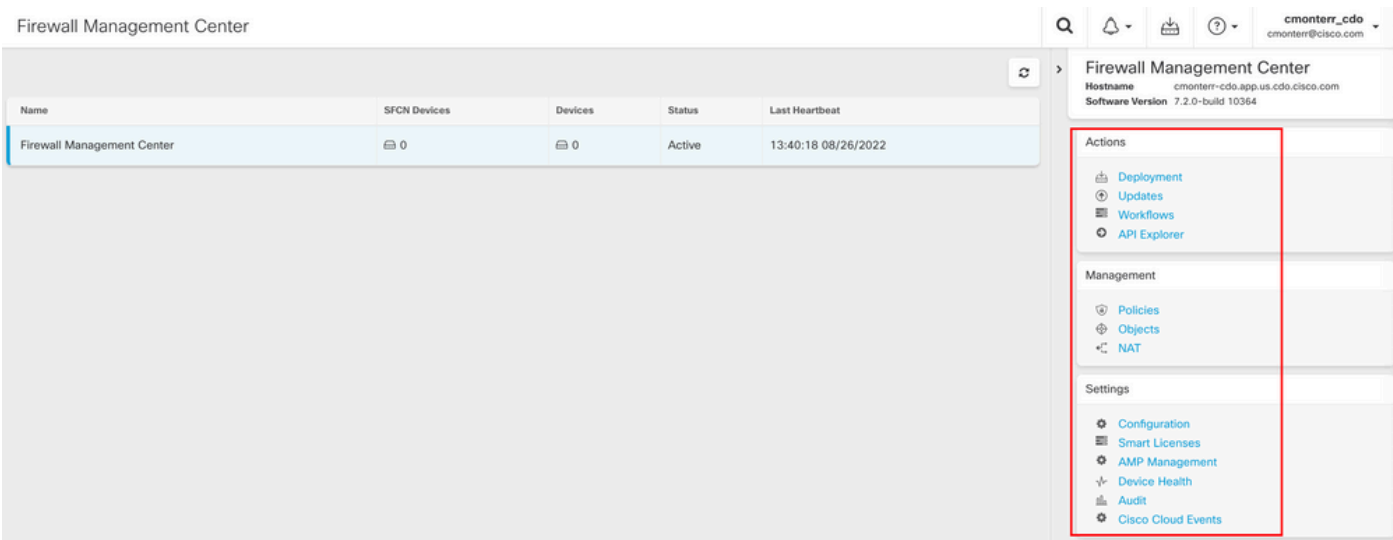
導航至 Menu > Tools & Services > Firewall Management Center cdFMC準備好使用時。



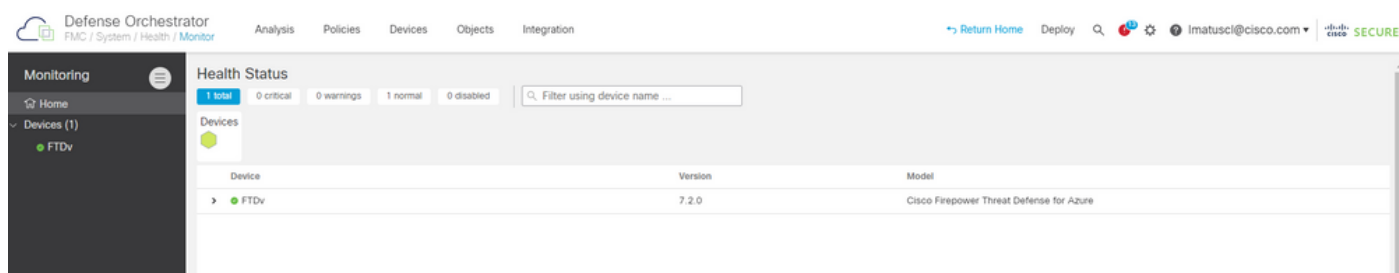
選擇所需的cdFMC以顯示cdFMC資訊。



要訪問cdFMC的圖形使用者介面(GUI)，請選擇右側的任何可用選項。



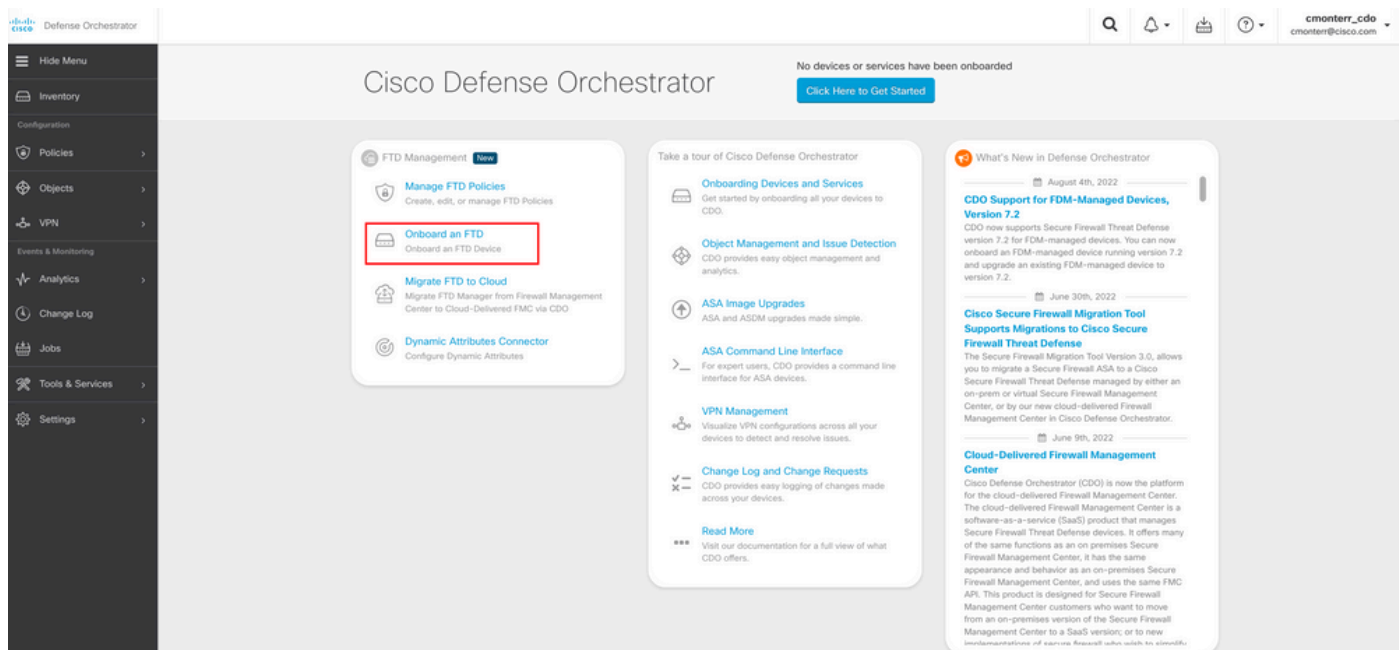
現在您可以看到cdFMC GUI。



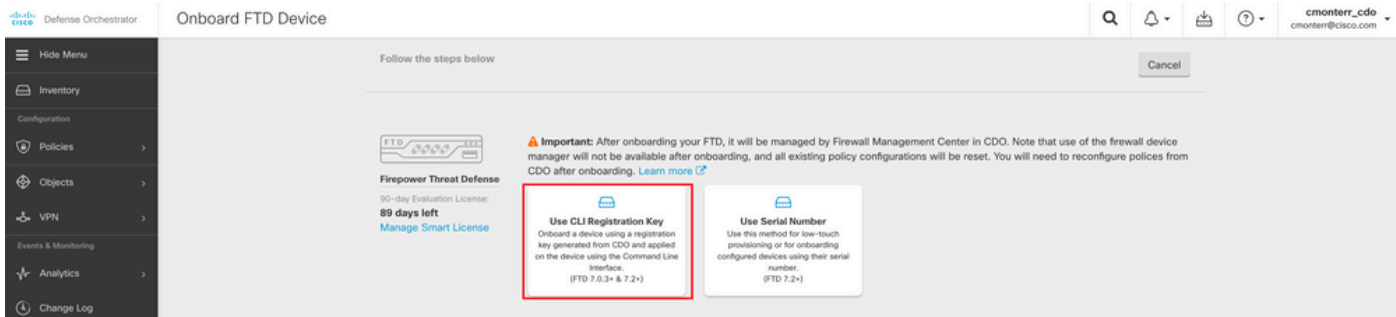
在雲交付的FMC上安裝FTD

以下映像顯示如何載入FTD以便使用指令行介面(CLI)註冊金鑰在cdFMC上註冊。

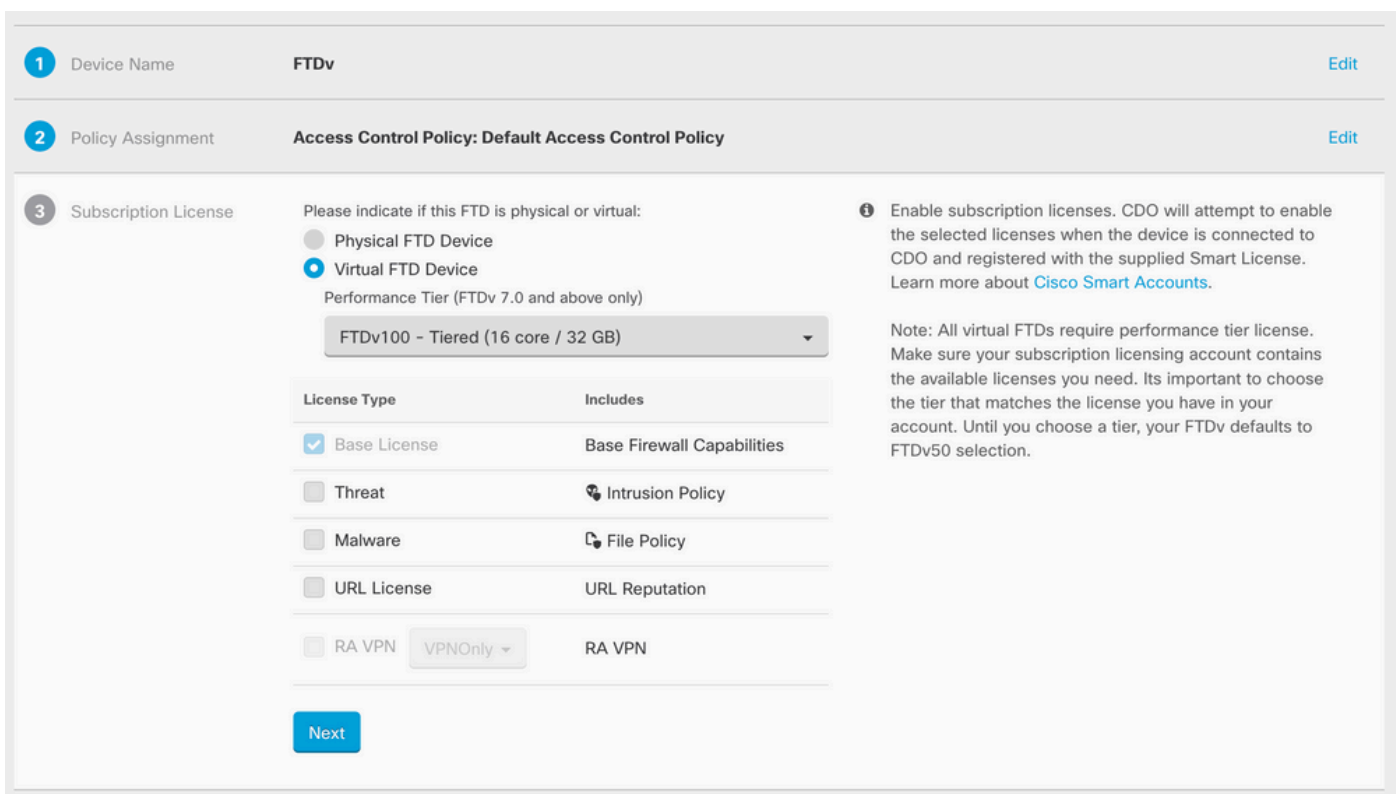
首先，選擇 **Onboard an FTD** 在CDO首頁上。



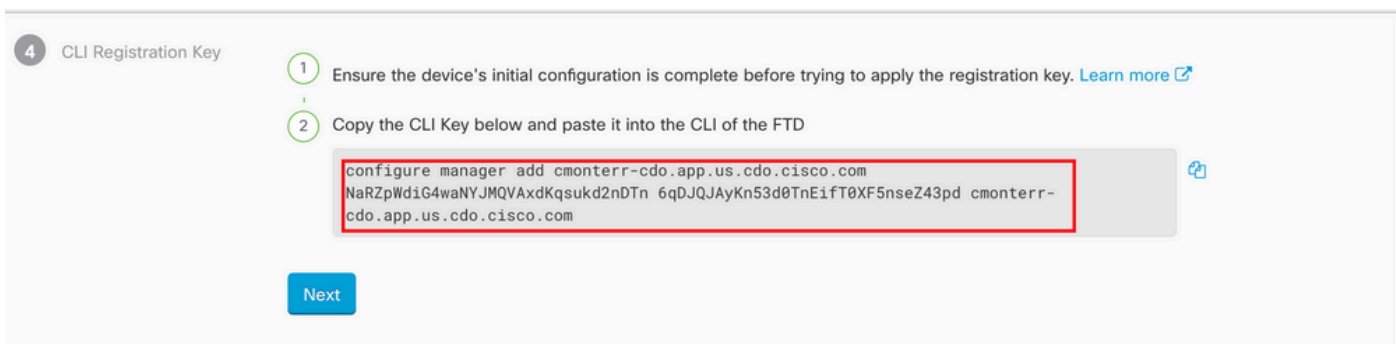
然後，選擇 **Use CLI Registration Key** 選項。



繼續輸入請求的和所需的FTDv資訊。



最後，cdFMC會建立一個特定的 CLI Key裝置的CLI金鑰。



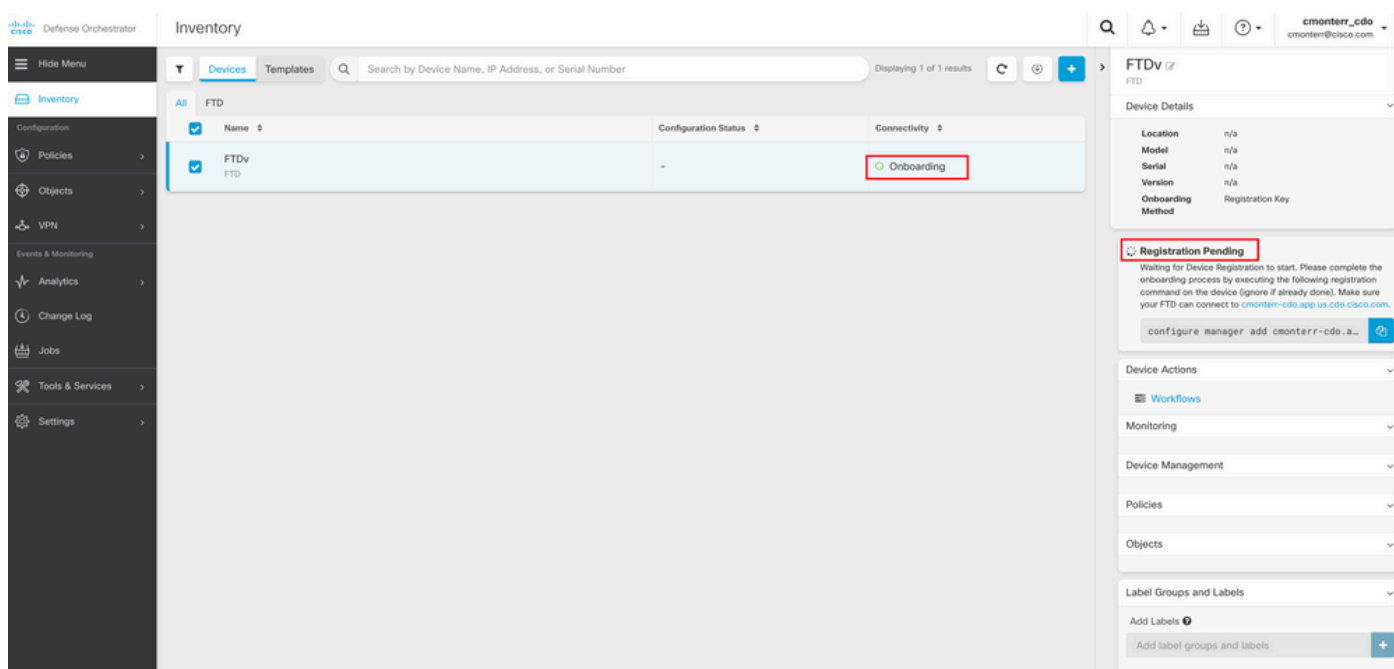
複製 CLI Key 進入受管裝置的CLI。

```
> 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
```

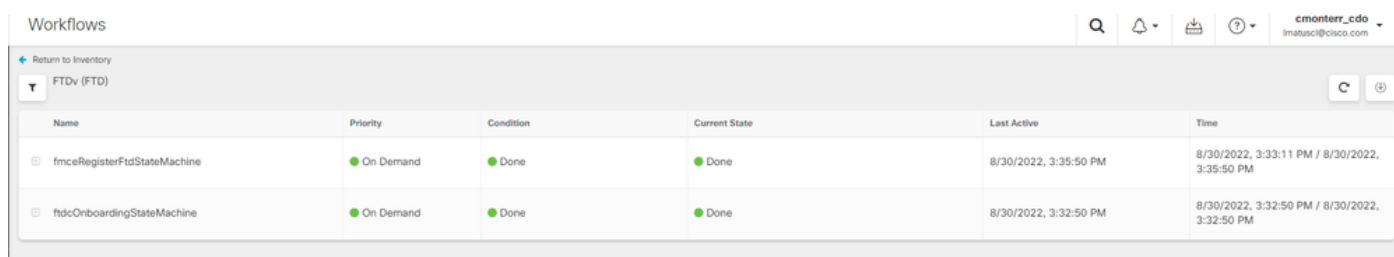
cdFMC啟動註冊任務。



註：確保FTD裝置透過連線埠8305(sftunnel)和443與CDO租戶通訊，以完成註冊程式。檢視完整的[網路要求](#)。

註：如果無法連線到主機，可以使用以下命令更正FTD-CLI中的DNS配置：**configure network dns <address>**。

要監控註冊流程，請導航至 **Device Actions > Workflows..**



展開 **Active** 如欲瞭解更多資訊，這些圖片顯示了FTDv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 | |
| 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 | | |
| 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 | Name | Configuration Status | Connectivity |
|-------------------------------------|-------------------------------------|-------------|----------------------|--------------|
| <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | FTDv FTD | Synced | Online |

FTDv

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.

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，導航至 Device Management > Device Overview 存取cdFMC和審閱FTDv概觀狀態。

Defense Orchestrator

FMC / Devices / Secure Firewall Device Summary

Analysis Policies **Devices** Objects Integration

Return Home Deploy

lmatusci@cisco.com

SECUR

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

相關資訊

- [技術支援與文件 - Cisco Systems](#)
- [通過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）。