

將FTD從一個FMC遷移到另一個FMC

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本文檔介紹如何在Firepower管理中心之間遷移Cisco Firepower威脅防禦(FTD)裝置。

必要條件

開始移轉程式之前，請確定您已具備下列先決條件：

- 訪問源和目標FMC。
- FMC和FTD的管理認證。
- 備份當前FMC配置。
- 確定FTD裝置執行的軟體版本與目的地FMC相容。
- 確保目標FMC的版本與源FMC的版本相同。

需求

- 兩個FMC必須運行相容的軟體版本。
- FTD裝置與兩個FMC之間的網路連線。
- 目的地FMC上有足夠的儲存空間和資源，足以容納FTD裝置。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

Cisco Firepower威脅防禦虛擬(FTDv)版本7.2.5

Firepower管理中心虛擬(FMCv)版本7.2.5

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

將FTD裝置從一個FMC遷移至另一個FMC涉及數個步驟，包括從來源FMC取消註冊裝置、準備目的地FMC以及重新註冊裝置。此過程可確保正確傳輸和應用所有策略和配置。

設定

組態

1. 登入源FMC。



Secure Firewall Management Center

Username

Password

Log In

2. 導航到裝置>裝置管理，選擇要遷移的裝置。



View By:

All (1) ● Error (0) ● Warning (0) ● Offline (0) ● Normal (1) ● Deployment Pending (0) ● Upgrade (0) ● Snort 3 (1)

[Collapse All](#)

| <input type="checkbox"/> | Name | Model | Version | Chassis |
|--------------------------|---|-----------------|---------|---------|
| <input type="checkbox"/> | ▼ Ungrouped (1) | | | |
| <input type="checkbox"/> | ● 192.168.15.31 Snort 3 192.168.15.31 - Routed | FTDv for VMware | 7.2.5 | N/A |

3. 在「裝置」區段中，瀏覽至裝置，然後按一下「匯出」以匯出您的裝置設定。

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

General



Name: FTD1
Transfer Packets: Yes
Mode: Routed
Compliance Mode: None
TLS Crypto Acceleration: Disabled

Device Configuration:

4. 導出配置後，必須下載該配置。

Device Configuration Download

Backup taken on **14-Oct-2024 07:05 PM** is available.

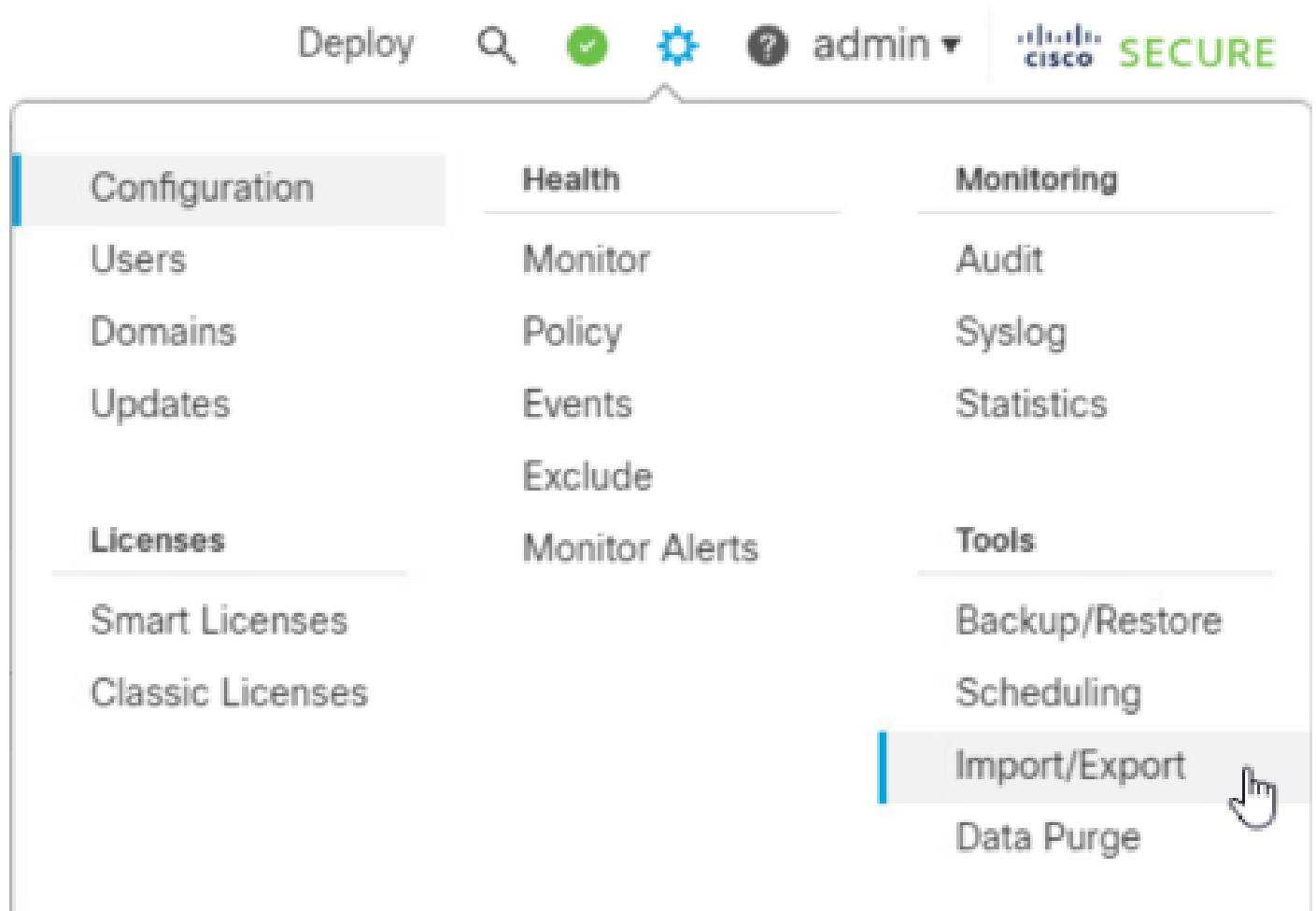
[Click here to download the package](#)

OK

注意：下載的檔案必須包含.SFO副檔名，並且包含IP地址、安全區域、靜態路由等裝置配

置資訊以及其他裝置設定。

5. 您必須導出與裝置關聯的策略，導航到系統>工具>導入/導出，選擇您要導出的策略，然後按一下導出。



∨ Access Control Policy



test

Access Control Policy

> Contextual Cross-launch

> Custom Table View

> Custom Workflow

> Dashboard

> Health Policy

∨ NAT Threat Defense



NAT

NAT Threat Defense

∨ Platform Settings Threat Defense



test

Platform Settings Threat Defense

> Report Template

Export



注意：請確保已成功下載.SFO檔案。按一下「匯出」後，將自動完成下載。此檔案包含訪問控制策略、平台設定、NAT策略以及遷移所必需的其他策略，因為它們沒有與裝置配置一起導出，必須手動上傳到目標FMC。

6. 從FMC註銷FTD裝置，導航到裝置>裝置管理，點選右側的三個垂直點，然後選擇刪除。

The screenshot shows the FMC interface with the 'Devices' tab selected. The table below shows the device details:

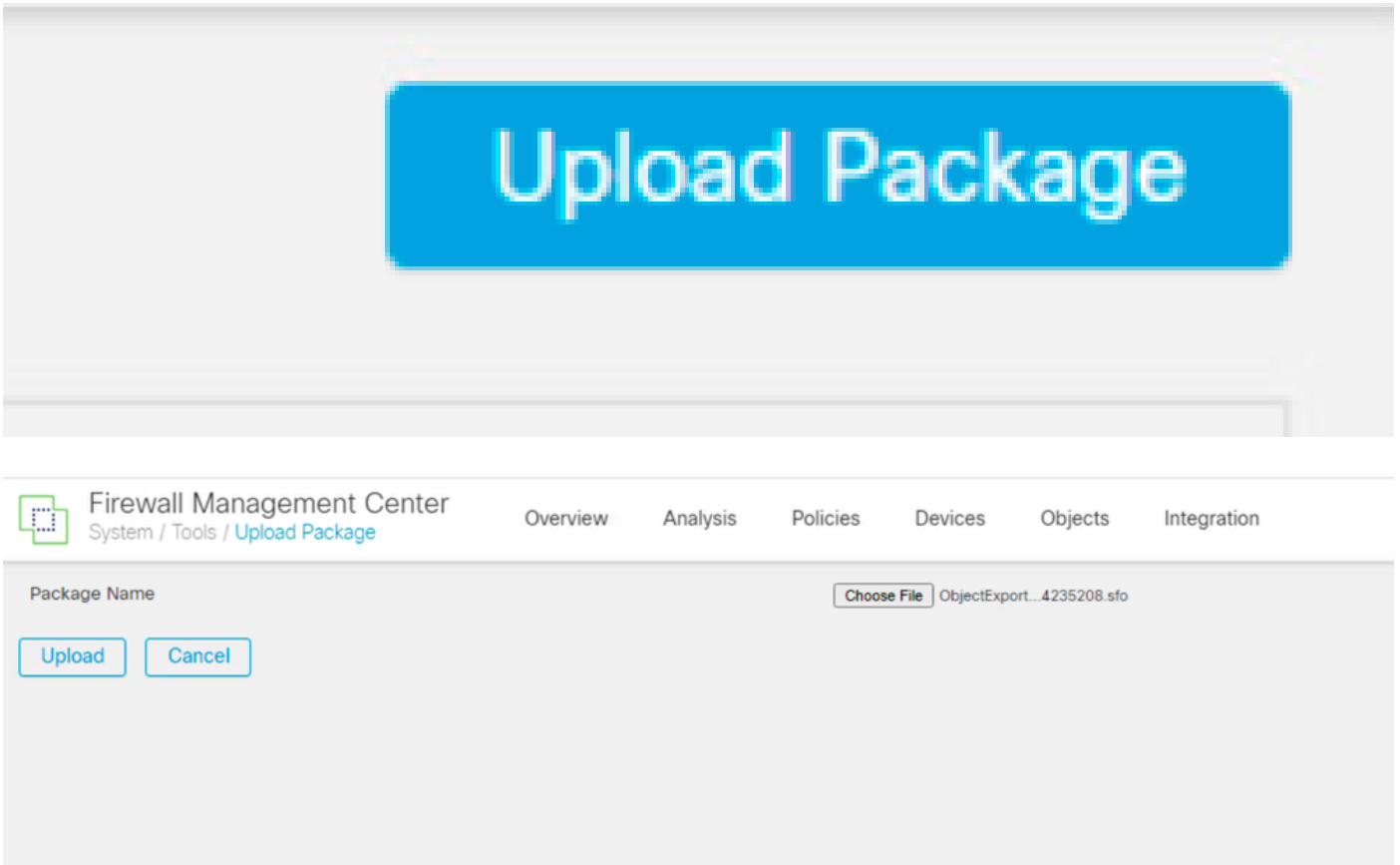
| Name | Model | Version | Chassis | Licenses | Access Control Policy | Auto RollBack |
|--|-----------------|---------|---------|--------------------------|-----------------------|---------------|
| FTD1 Snort 3 192.168.15.31 - Routed | FTDv for VMware | 7.2.5 | N/A | Base, Threat (2 more...) | test | |

The context menu for the selected device includes the following options:

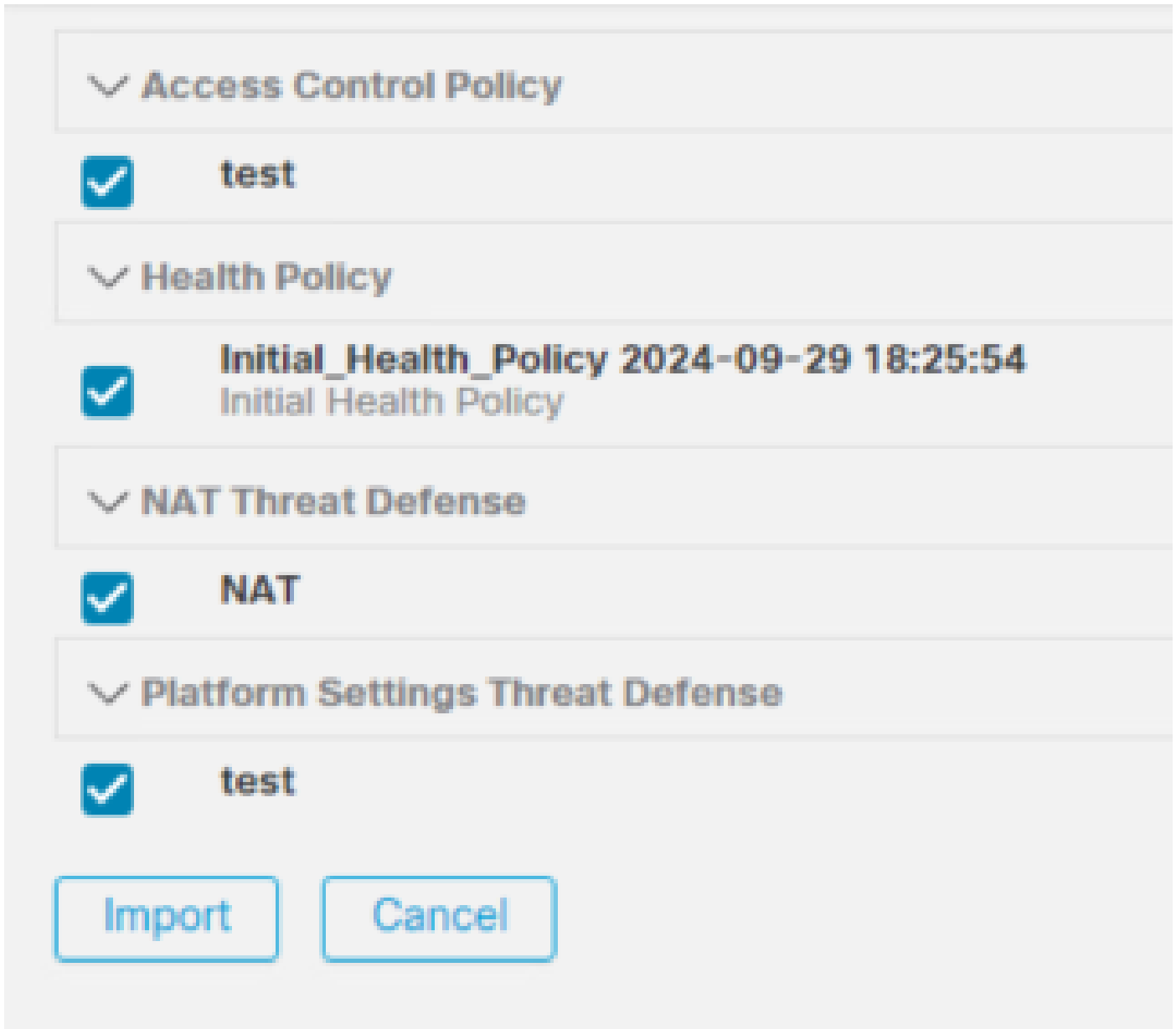
- Delete
- Packet Tracer
- Packet Capture
- Revert Upgrade
- Health Monitor
- Troubleshoot Files

7. 準備目標FMC：

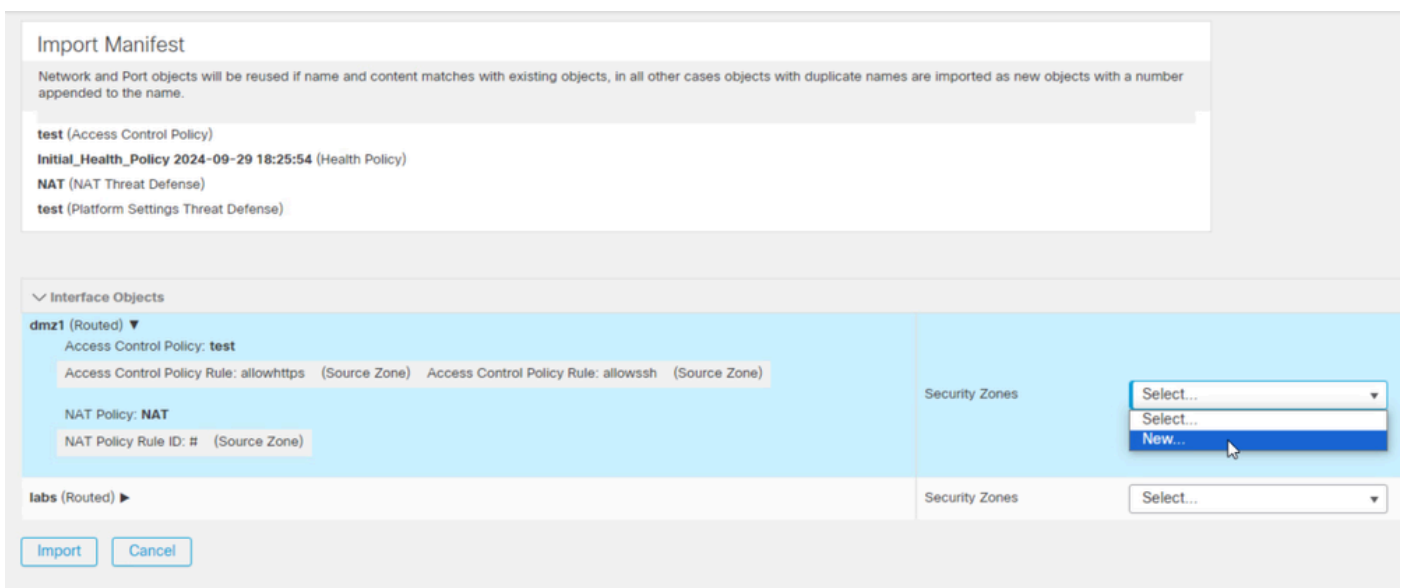
- 登入到目標FMC。
- 透過導入您在步驟5中下載的源FMC策略，確保FMC已準備好接受新裝置。導航到系統>工具>導入/導出，然後按一下上傳資料包。上傳要導入的檔案，然後按一下上傳。



8. 選擇要導入目標FMC的策略。

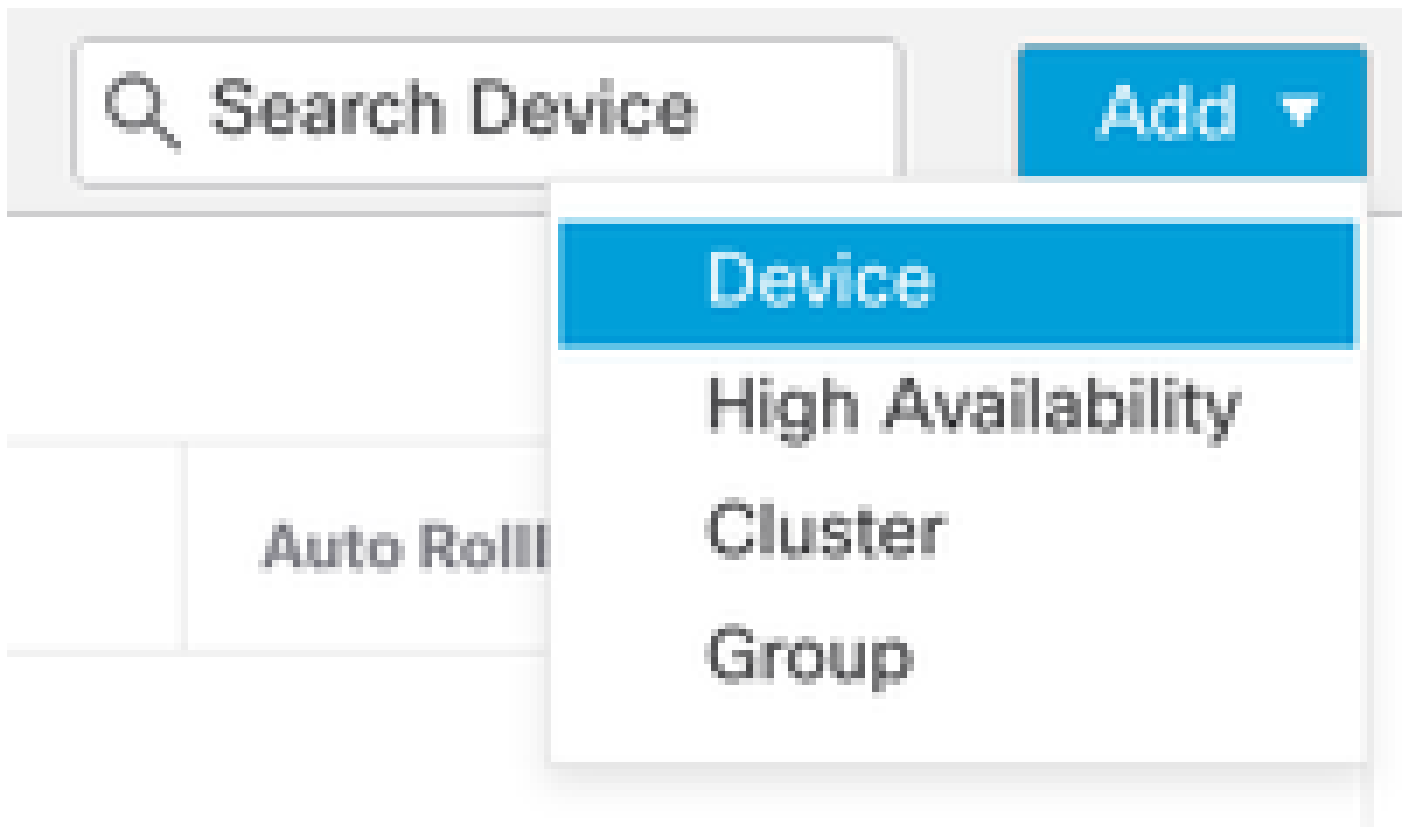


9. 在匯入資訊清單中，選取安全性區域或建立新的區域以指定給介面物件，然後按一下「匯入」。



10. 將FTD註冊至目的地FMC：

- 在目標FMC上，導航到Device > Management頁籤，然後選擇Add > Device。
- 回應提示來完成註冊程式。



Add Device



CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

- Malware
- Threat
- URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

† Either host or NAT ID is required.

Cancel

Register




有關其他詳細資訊，請檢視《Firepower管理中心配置指南》[向Firepower管理中心增加裝置](#)

11. 導航到裝置>裝置管理>選擇FTD >裝置，然後按一下導入。出現警告，要求您確認更換裝置配置，按一下yes。

FTD1

Cisco Firepower Threat Defense for VMware

Device Routing Interfaces Inline Sets DHCP VTEP

| General | |    |
|--------------------------|---------------------------------------|---|
| Name: | FTD1 | |
| Transfer Packets: | Yes | |
| Mode: | Routed | |
| Compliance Mode: | None | |
| TLS Crypto Acceleration: | Disabled | |
| Device Configuration: | <input type="button" value="Import"/> | <input type="button" value="Export"/> <input type="button" value="Download"/> |

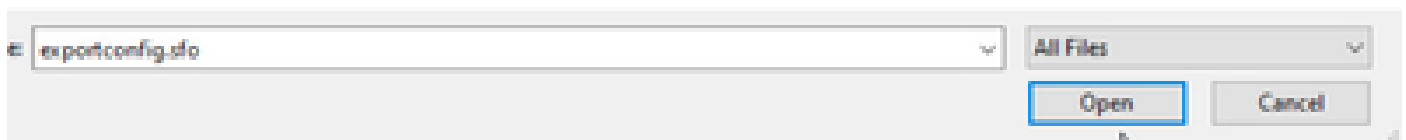
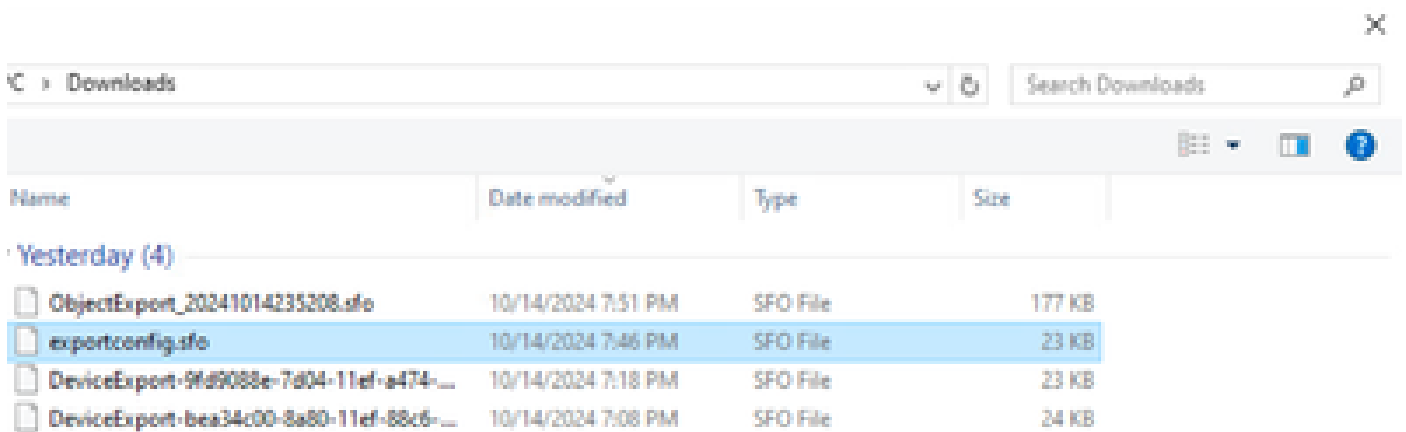
Device Configuration Import

This will replace current device configuration with new configuration from imported file. Do you want to continue?

No

Yes

12. 選擇副檔名為.SFO的導入配置檔案，點選上傳，系統會顯示一則消息，指示導入已啟動。



Device Configuration Import

Device configuration import task initiated. View the progress of task from Tasks view.

OK

Only:

13.最後，當匯入完成時，系統會顯示警示並自動產生報表，讓您複查已匯入的物件與政策。

The screenshot displays the Cisco Secure management interface. At the top, there is a navigation bar with 'Deploy', a search icon, a notification bell with '2', a settings gear, a user profile 'admin', and the 'cisco SECURE' logo. Below this is a secondary navigation bar with tabs for 'Deployments', 'Upgrades', 'Health' (with a red indicator), and 'Tasks' (with a red indicator and a blue underline). A 'Show Notifications' toggle is on the right. The main content area shows a summary of tasks: '20+ total', '0 waiting', '0 running', '0 retrying', '20+ success', and '1 failure'. A search box labeled 'Filter' is present. A notification card is visible, featuring a green checkmark icon, the title 'Device Configuration Import', the message 'Device configurations imported successfully', and a link 'View Import Report'. The notification has a '6s' timer and a close 'X' button.

Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

| Type | Name |
|--|---|
| PG.PLATFORM.AutomaticApplicationBypassPage | .9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage |
| PG.PLATFORM.PixInterface | .9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface |
| PG.PLATFORM.NgfwinlineSetPage | .9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwinlineSetPage |

驗證

完成移轉後，請確認FTD裝置已正確註冊，並在目的地FMC中運作：

- 檢查目的FMC上的裝置狀態。
- 確保正確應用所有策略和配置。
- 執行測試以確認裝置運行正常。

疑難排解

如果在遷移過程中遇到任何問題，請考慮以下故障排除步驟：

- 驗證FTD裝置與兩個FMC之間的網路連線。
- 確保兩個FMC上的軟體版本相同。
- 檢查兩個FMC上的警報以瞭解任何錯誤消息或警告。

相關資訊

- [Cisco Secure Firewall Management Center管理指南](#)
- [配置、驗證Firepower裝置註冊並排除故障](#)

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）。