

# 在CDO上初始化並啟動防火牆遷移工具

## 目錄

---

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[初始](#)

[啟動](#)

[遷移示例](#)

[相關資訊](#)

---

## 簡介

本文檔介紹如何在Cisco Defense Orchestrator(CDO)平台上初始化、啟動和使用Firepower遷移工具(FMT)。

## 必要條件

### 需求

思科建議瞭解以下主題：

Firepower遷移工具(FMT)。

Cisco Defense Orchestrator(CDO)。

Firepower威脅防禦(FTD)。

調適型安全裝置(ASA)

### 採用元件

防火牆遷移工具 ( 版本4.0.3 ) 。

Cisco Defense Orchestrator。

雲交付的防火牆管理中心。

自適應安全裝置。

Firepower執行緒防禦。

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

CDO中的遷移工具從您選擇的源裝置或您上傳的配置檔案提取裝置配置，並將它們遷移到CDO租戶上調配的雲交付的防火牆管理中心。

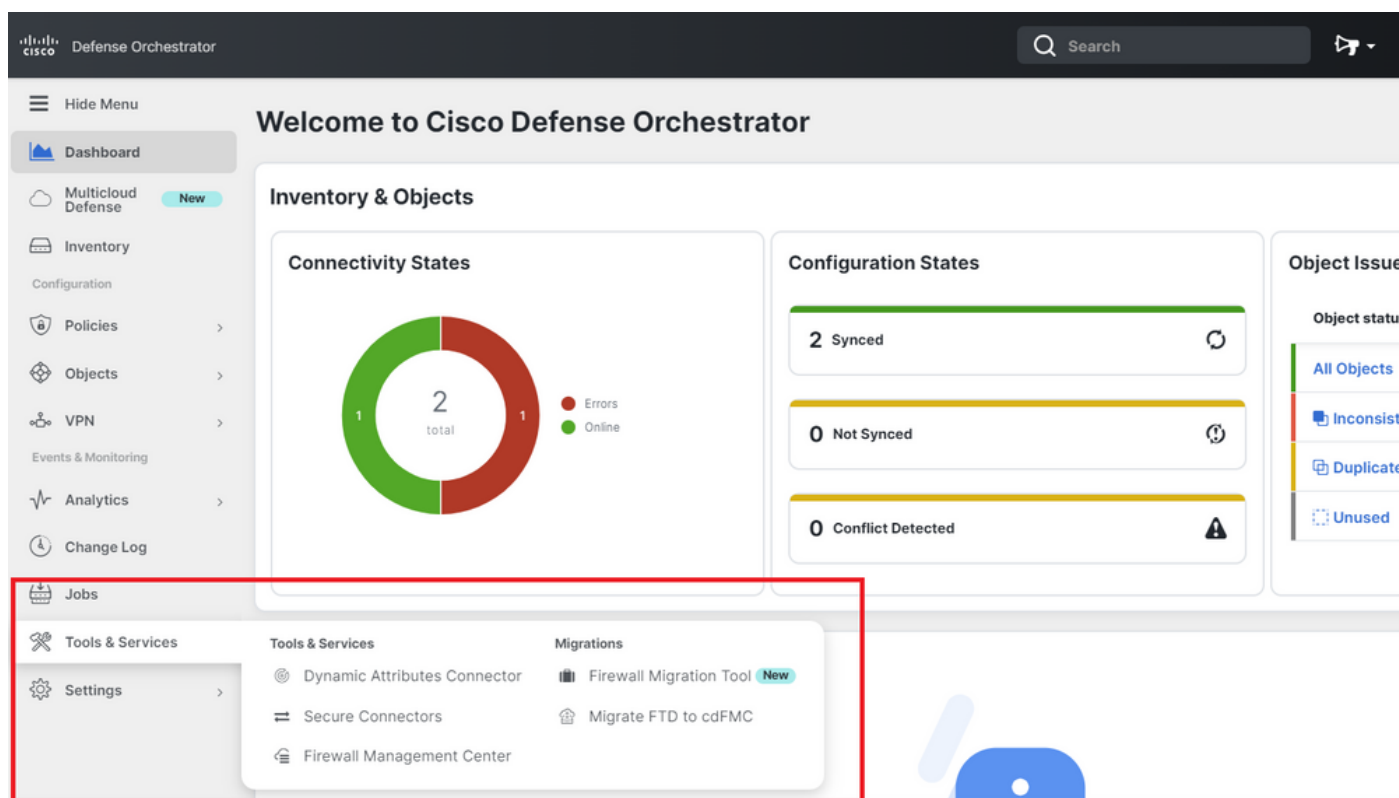
驗證配置後，您可以在雲交付的防火牆管理中心上手動配置不受支援的配置。

## 設定

### 初始

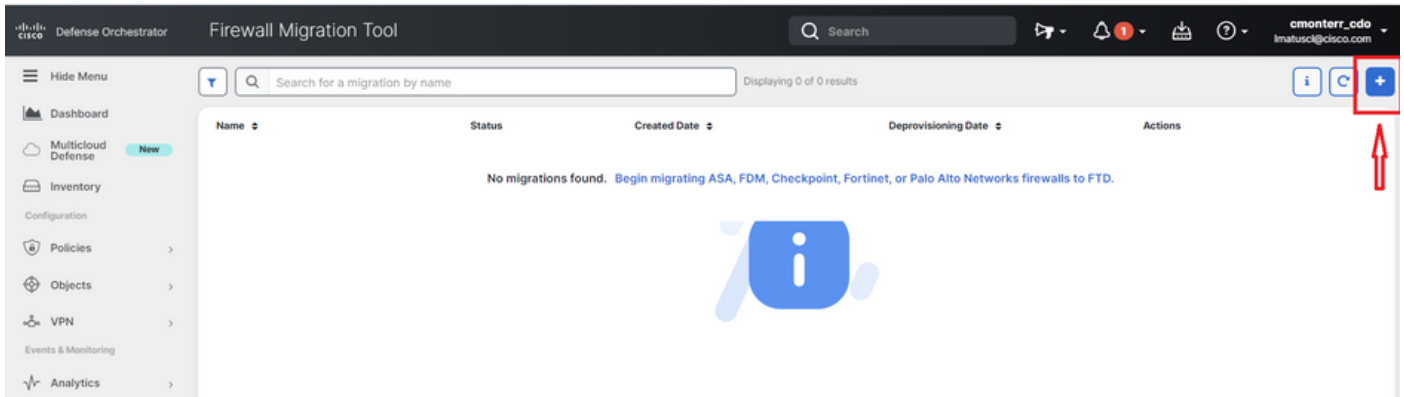
以下影象介紹了如何在CDO上初始化Firepower遷移工具。

1. — 要初始化防火牆遷移工具，請開啟您的CDO租戶並導航到工具與服務>防火牆遷移工具。

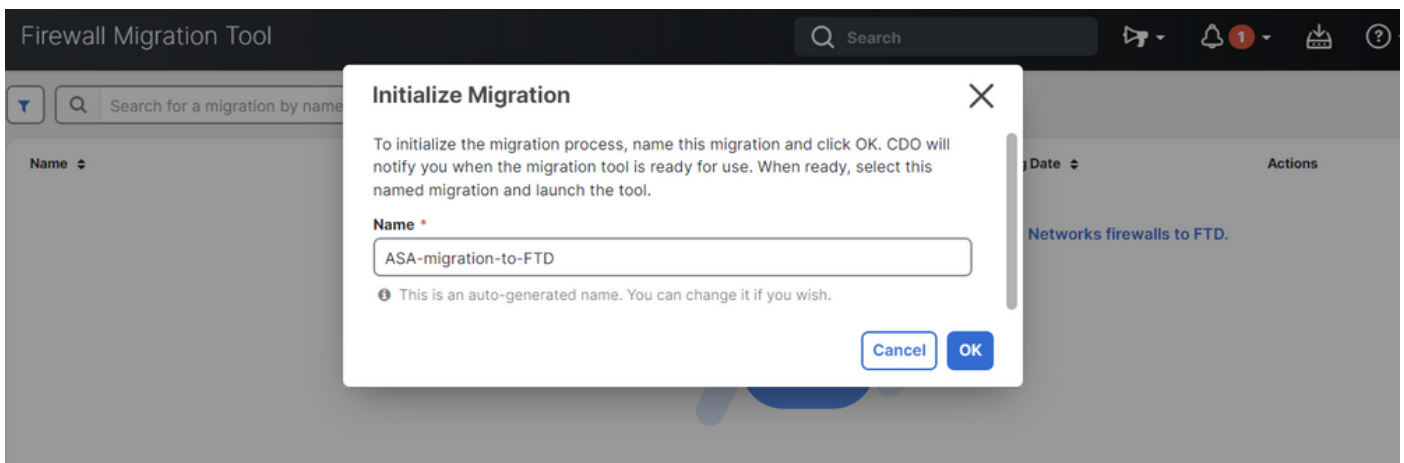


The screenshot displays the Cisco Defense Orchestrator (CDO) dashboard. The main content area is titled 'Welcome to Cisco Defense Orchestrator' and 'Inventory & Objects'. It features three primary panels: 'Connectivity States' with a donut chart showing 2 total objects (1 Online, 1 Errors), 'Configuration States' with 2 Synced, 0 Not Synced, and 0 Conflict Detected items, and 'Object Issue' with filters for Object status (All Objects, Inconsistent, Duplicate, Unused). A red box highlights the 'Tools & Services' menu, which is expanded to show 'Tools & Services' (Dynamic Attributes Connector, Secure Connectors, Firewall Management Center) and 'Migrations' (Firewall Migration Tool - New, Migrate FTD to cdFMC).

2. — 選擇藍色加號(+)按鈕以建立新的遷移流程。

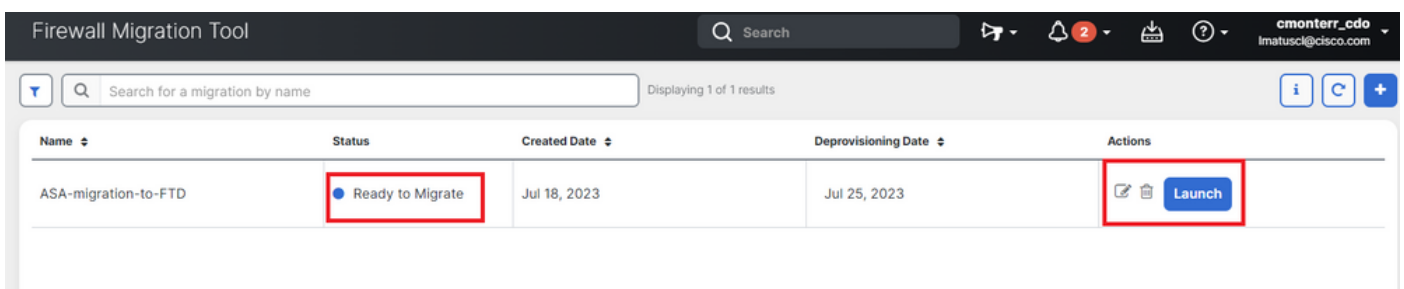


3. — 為了初始化遷移過程，CDO會自動生成預設名稱，如果您願意，可以更改該名稱，只需按一下「OK」即可。



## 啟動

1. — 等待遷移過程完成；狀態必須從「正在初始化」更改為「準備遷移」。一旦準備就緒，您就可以啟動FMT。



2. — 遷移工具的雲例項將在新的瀏覽器頁籤中開啟，並允許您使用指導式工作流執行遷移任務。

CDO中的遷移工具無需下載和維護安全防火牆遷移工具的案頭版本。



Extract Cisco ASA (8.4+) Information

Source: Cisco ASA (8.4+)

Extraction Methods >

Manual Upload: [shitech\\_asav-a.txt](#)

Context Selection

Selected Context: Single Context Mode

Parsed Summary

Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

2 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	0 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
--------------------------------	--------------------------------------------------------------------------	----------------------	-------------------	----------------------------------------------------------------------------------------------

Back Next

3.- FMT解析ASA配置並顯示您的配置摘要。驗證並點選「下一步」以繼續後續步驟。

Parsed Summary

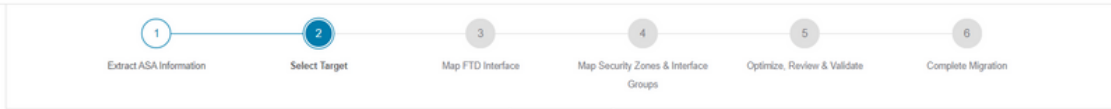
Collect Hitcounts: No. Hitcount information is only available when connected to a live ASA.

2 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	0 Network Objects	0 Port Objects	0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)
0 Network Address Translation	4 Logical Interfaces	3 Routes (Static Routes, Policy Based Routing, ECMP)	0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)

● Pre-migration report will be available after selecting the targets.

Back Next

3. — 繼續使用與案頭版本工具相同的常規FMT步驟。請注意，本示例中沒有為實際目的選擇目標裝置。



### Select Target ⓘ

Source: Cisco ASA (8.4+)

Firewall Management - Cloud-delivered FMC >

Choose FTD >

Select FTD Device  
Select FTD Device v

Proceed without FTD

Interface, Routes and Site-to-Site VPN Tunnels won't be migrated

Select Features >


Rule Conversion/ Process Config >

4. — 完成所有FMT驗證後，配置將推送到雲交付的Firepower管理中心。



### Complete Migration ⓘ

#### Migration Status



Migration is complete, policy is pushed to FMC.  
Next Step - Login to FMC to deploy the policy to FTD.

Manual Upload: shtech\_asav-a.txt

Selected Context: Single Context Mode

Migration Summary (Post Push)

## 相關資訊

- [安全防火牆遷移工具的故障排除。](#)
- [Cisco Defense Orchestrator中的防火牆遷移工具入門。](#)

## 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）。