在CDO中使用FMT將FDM移轉至cdFMC

目錄

簡介

必要條件

- 需求
- 採用元件

背景資訊

設定

驗證

簡介

本文檔介紹如何使用CDO中的Firepower遷移工具(FMT)將Firepower裝置管理器(FDM)遷移到雲交付的FMC (cdFMC)。

必要條件

需求

- Firepower裝置管理器(FDM) 7.2+
- 雲端提供的防火牆管理中心(cdFMC)
- CDO中包含Firepower遷移工具(FMT)

採用元件

本檔案是根據前述要求所建立。

- Firepower裝置管理器(FDM) 7.4.1版
- 雲端提供的防火牆管理中心(cdFMC)
- Cloud Defense Orchestrator (CDO)

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

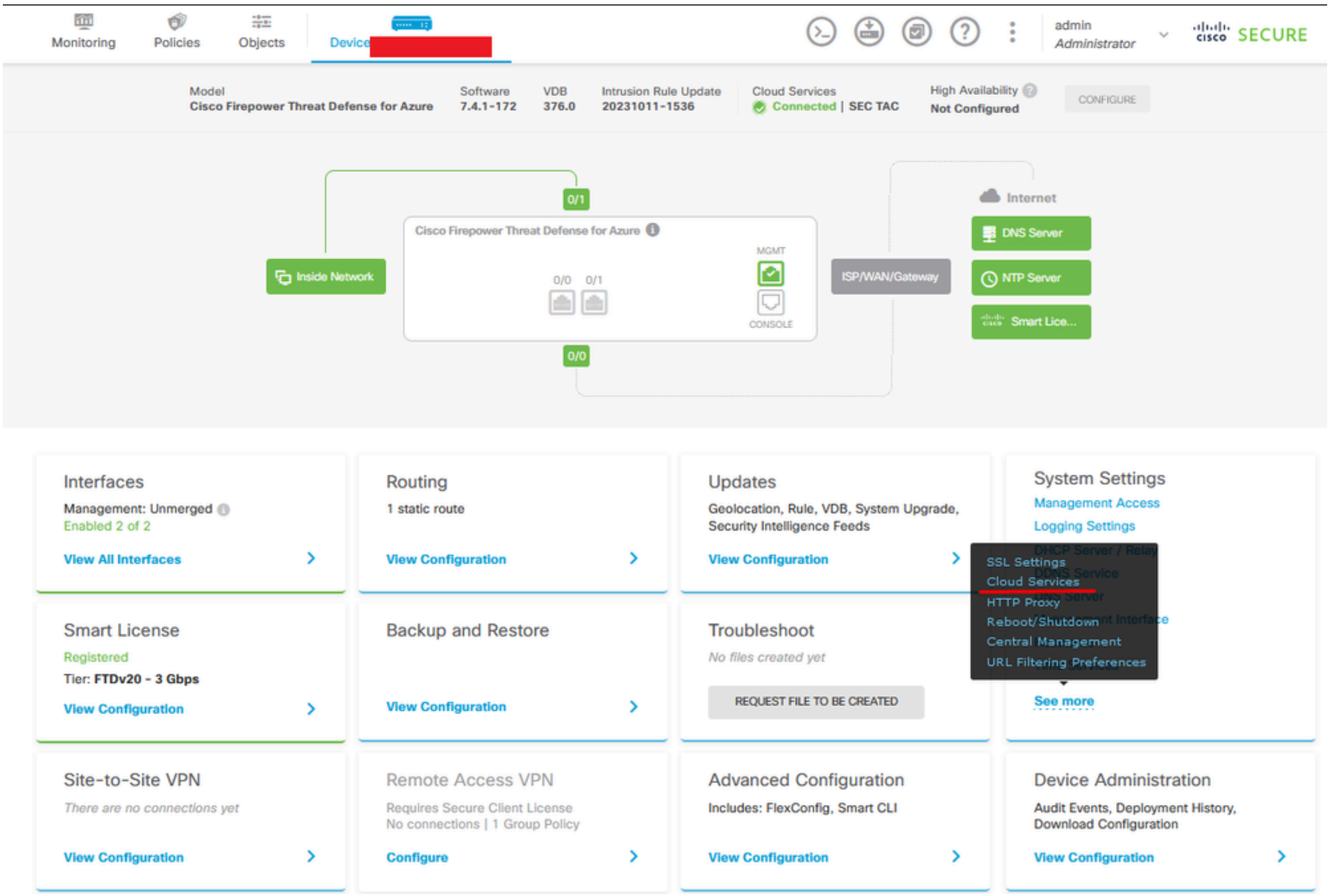
CDO管理員使用者可以在裝置使用版本7.2或更新版本時，將裝置移轉至cdFMC。在本文檔中描述的遷移中，cdFMC已在CDO租戶上啟用。

設定

1.-在FDM上啟用思科雲服務

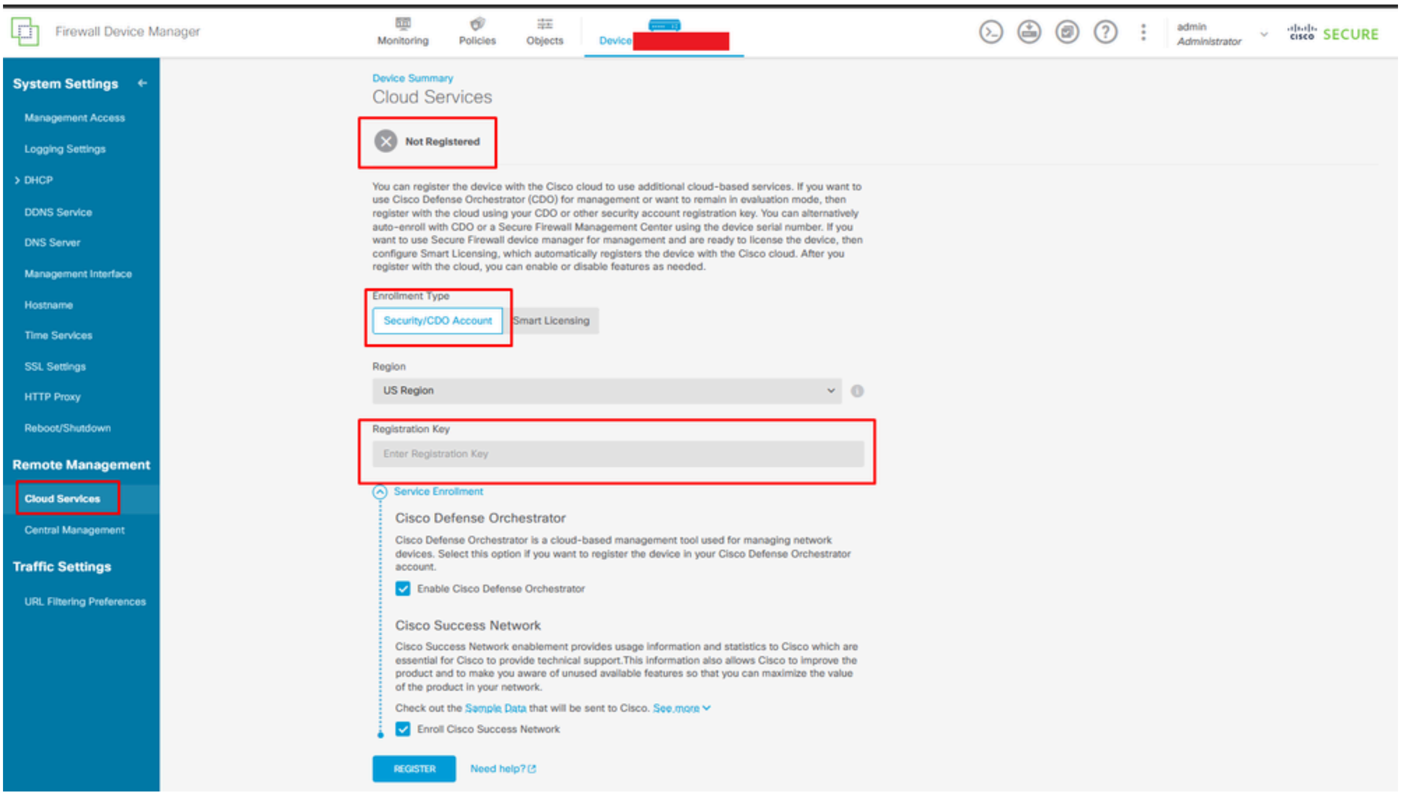
要開始遷移，FDM裝置必須沒有任何掛起部署並註冊到雲服務。要註冊到雲服務，請導航到系統設定>檢視更多>雲服務。

在雲服務部分中，您發現裝置未註冊，因此必須使用型別安全/CDO帳戶執行註冊。必須配置註冊金鑰，然後配置註冊。



註冊雲服務

在雲服務上，顯示未註冊。選擇CDO帳戶註冊型別，並提供CDO的註冊金鑰。



Device Summary

Cloud Services

Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type: Security/CDO Account | Smart Licensing

Region: US Region

Registration Key: Enter Registration Key

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

☑ Enable Cisco Defense Orchestrator

Cisco Success Network

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the Sample Data that will be sent to Cisco. See more

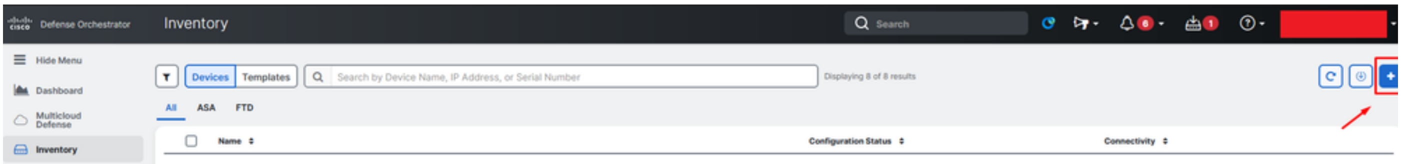
☑ Enroll Cisco Success Network

REGISTER   Need help?

註冊雲服務

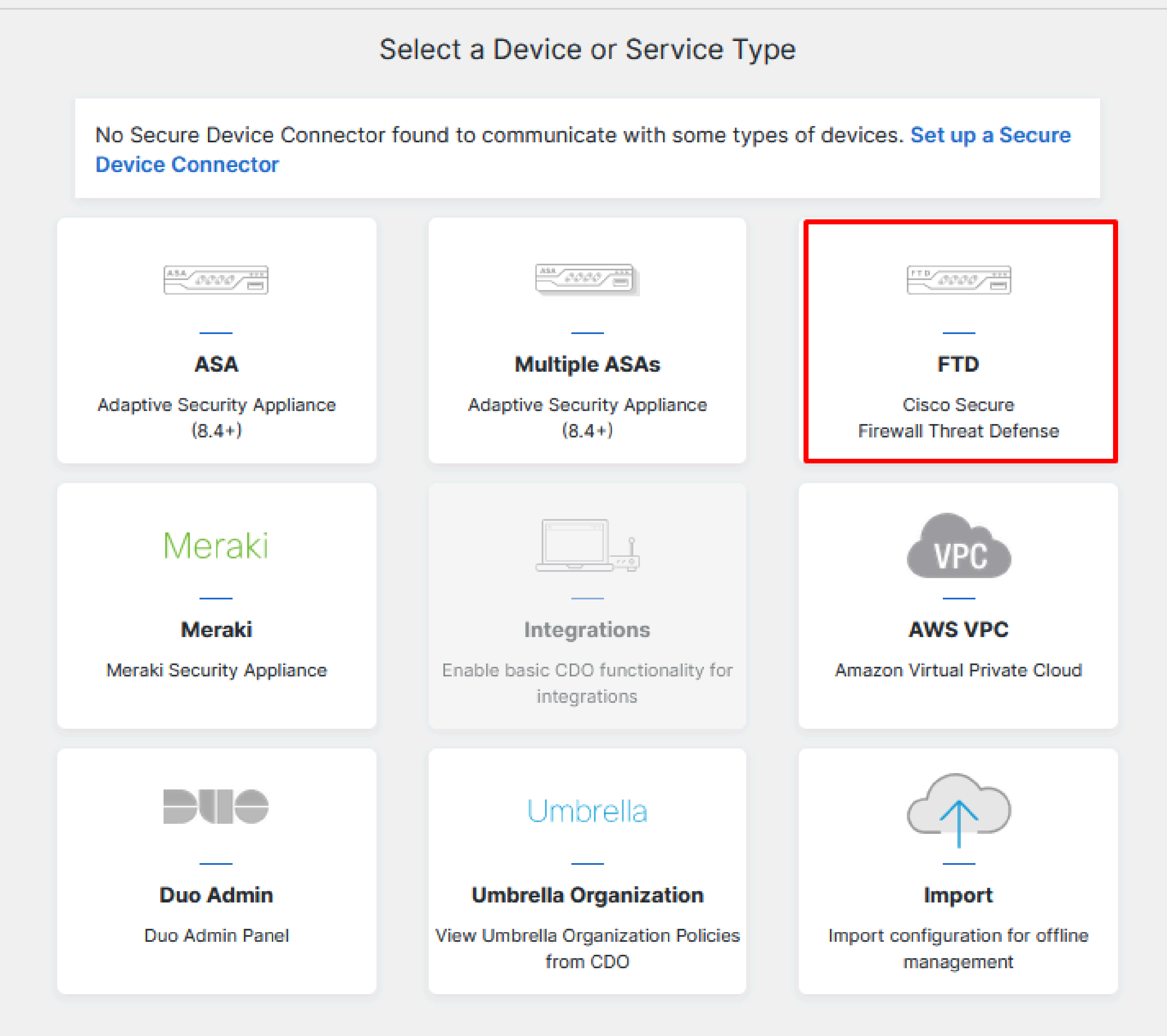
您可以在CDO中找到註冊金鑰。導航到CDO，轉至資產>增加符號。

出現一個選單，用於選擇您擁有的裝置型別。選取FTD選項。您必須啟用FDM選項；否則，將無法執行對應的移轉。註冊型別使用使用註冊金鑰。在此選項中，註冊金鑰會顯示在步驟編號3，我們必須將其複製並貼到FDM中。



內建FDM，新增選項

出現一個選單，用於選擇裝置或服務型別。



Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. Set up a Secure Device Connector

ASA
Adaptive Security Appliance (8.4+)

Multiple ASAs
Adaptive Security Appliance (8.4+)

FTD
Cisco Secure Firewall Threat Defense

Meraki
Meraki Security Appliance

Integrations
Enable basic CDO functionality for integrations

AWS VPC
Amazon Virtual Private Cloud

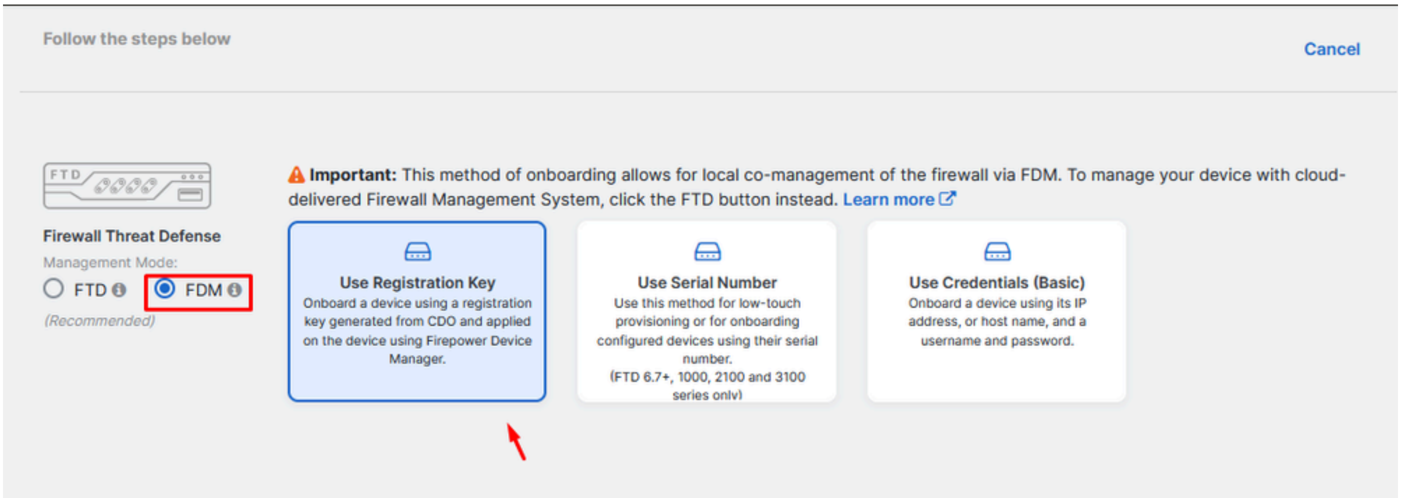
Duo Admin
Duo Admin Panel

Umbrella Organization
View Umbrella Organization Policies from CDO

Import
Import configuration for offline management

選擇裝置或服務型別

對於此文檔，已選擇「選擇註冊金鑰」。



Follow the steps below

Cancel

Firewall Threat Defense
Management Mode:
○ FTD ● FDM
(Recommended)

⚠ **Important:** This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. Learn more

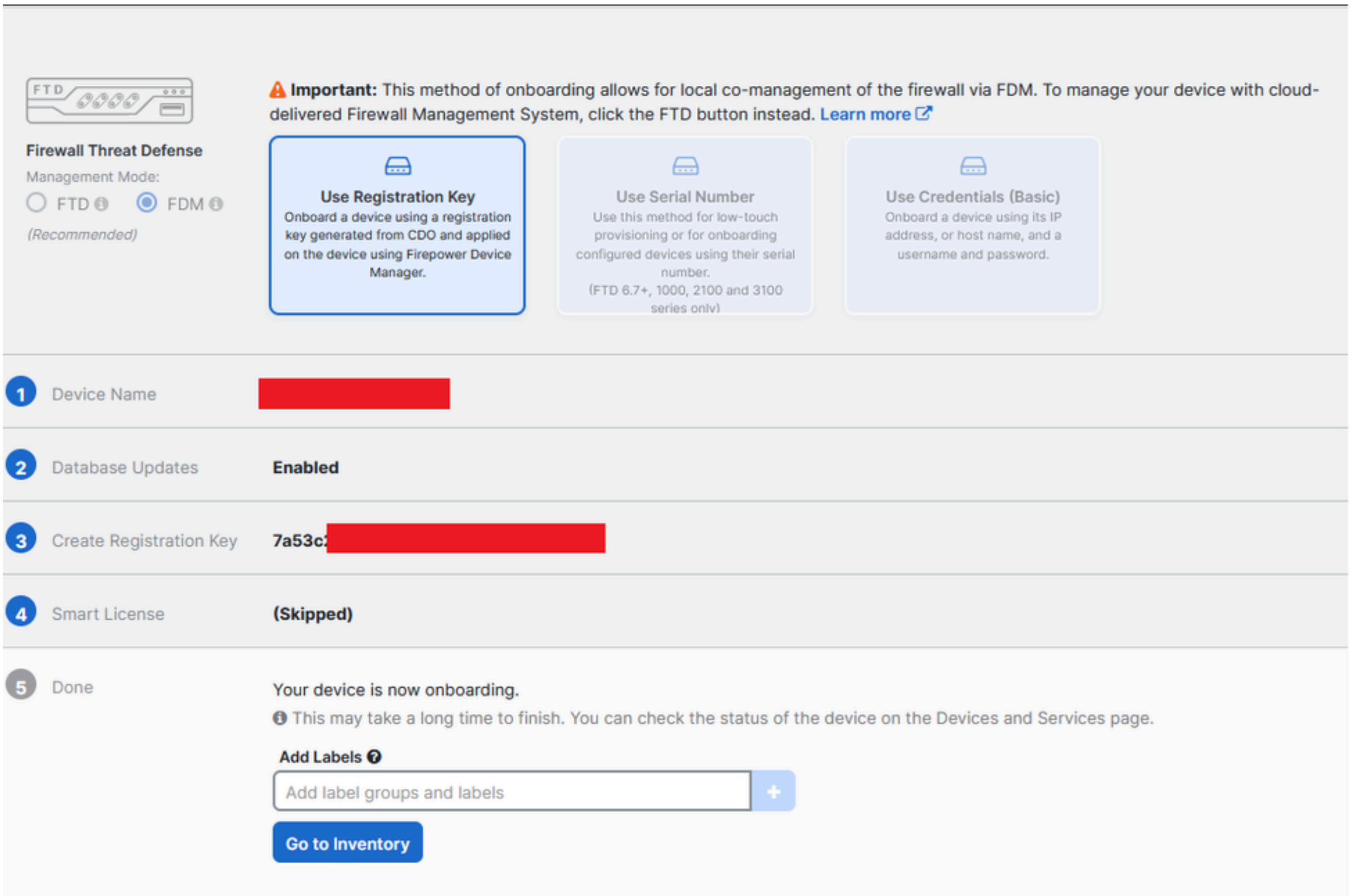
Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)

Use Credentials (Basic)
Onboard a device using its IP address, or host name, and a username and password.

註冊型別

此處，它顯示上一步所需的註冊金鑰。



Firewall Threat Defense

Management Mode:

○ FTD ● FDM

(Recommended)

Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with cloud-delivered Firewall Management System, click the FTD button instead. Learn more

Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

Use Serial Number
Use this method for low-touch provisioning or for onboarding configured devices using their serial number.
(FTD 6.7+, 1000, 2100 and 3100 series only)

Use Credentials (Basic)
Onboard a device using its IP address, or host name, and a username and password.

1 Device Name [redacted]

2 Database Updates **Enabled**

3 Create Registration Key **7a53c**[redacted]

4 Smart License **(Skipped)**

5 Done

Your device is now onboarding.

This may take a long time to finish. You can check the status of the device on the Devices and Services page.

Add Labels

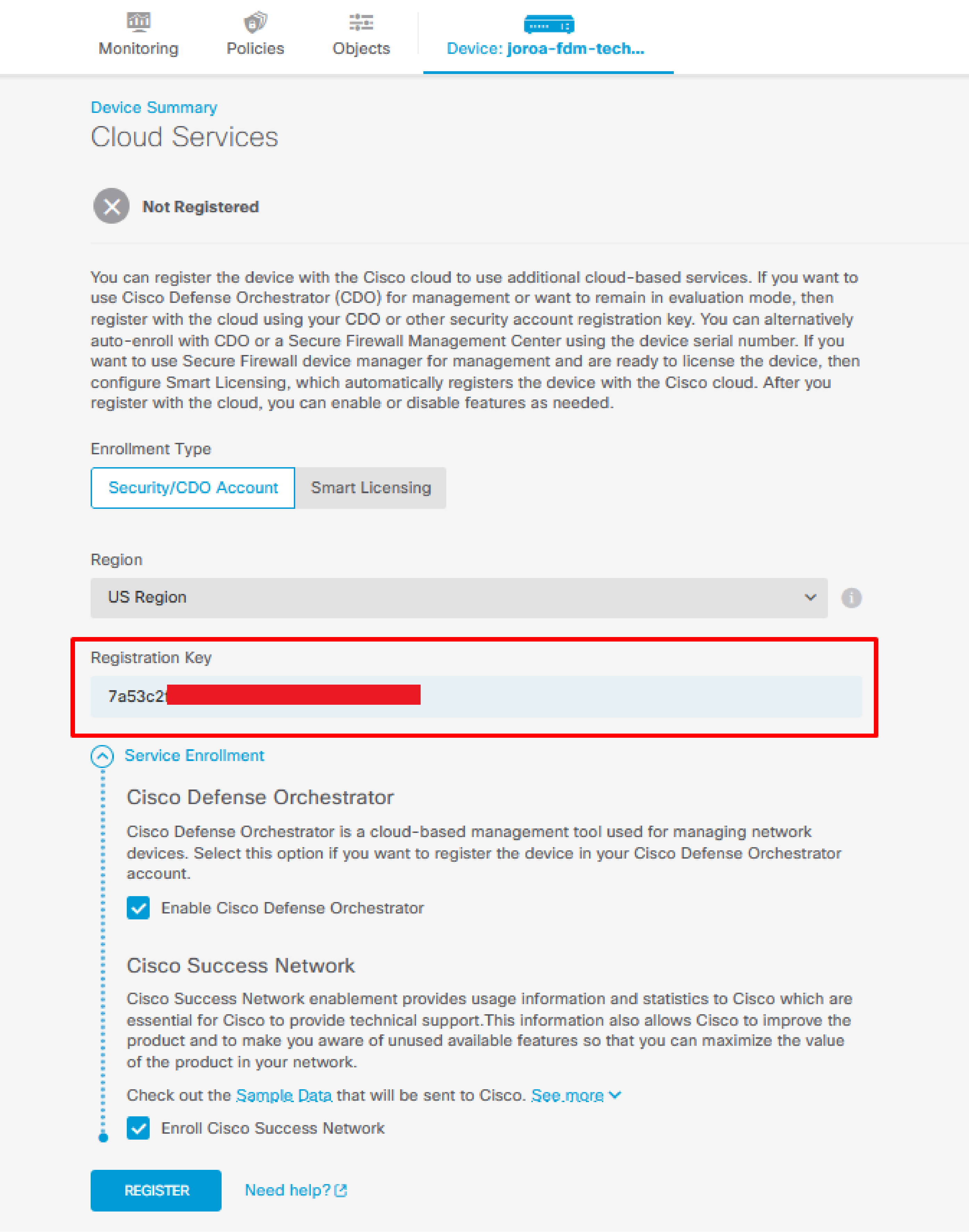
Add label groups and labels

Go to Inventory

註冊程式

取得註冊金鑰後，將其複製並貼到FDM中，然後按一下「註冊」。在Cloud Services中註冊FDM後，其將顯示為Enabled，如下圖所示。

已跳過智慧許可證，因為裝置將在啟動並運行後進行註冊。



Device Summary

Cloud Services

Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account | Smart Licensing

Region

US Region

Registration Key

7a53c2[redacted]

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

☑ Enable Cisco Defense Orchestrator

Cisco Success Network

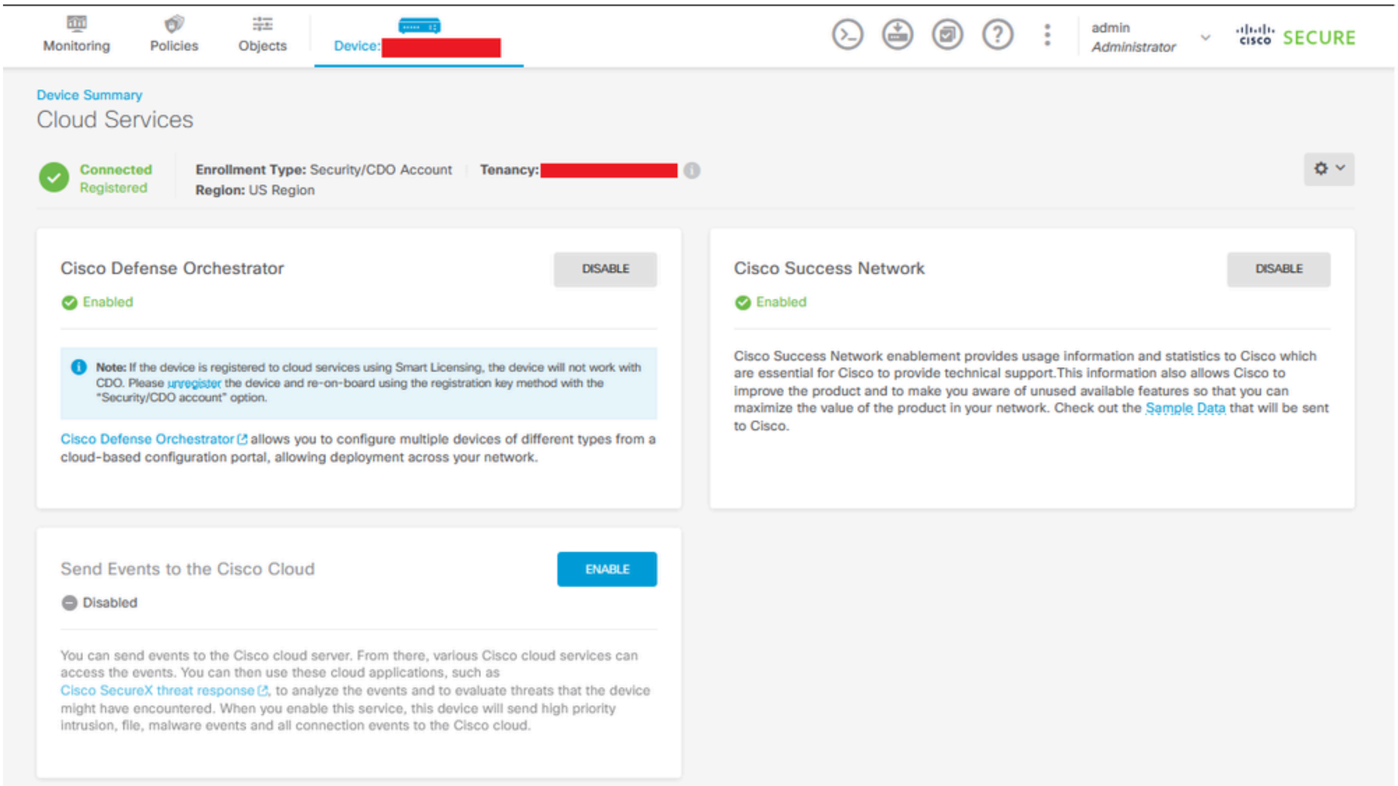
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network.

Check out the Sample Data that will be sent to Cisco. See more

☑ Enroll Cisco Success Network

FDM註冊

註冊FDM時，它會顯示「租戶」、「已連線的雲服務」和「已註冊」。



Device Summary

Cloud Services

Connected
Registered

Enrollment Type: Security/CDO Account | **Tenancy:** [redacted]
Region: US Region

Cisco Defense Orchestrator — DISABLE

Enabled

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with CDO. Please unregister the device and re-on-board using the registration key method with the "Security/CDO account" option.

Cisco Defense Orchestrator allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network — DISABLE

Enabled

Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the Sample Data that will be sent to Cisco.

Send Events to the Cisco Cloud — ENABLE

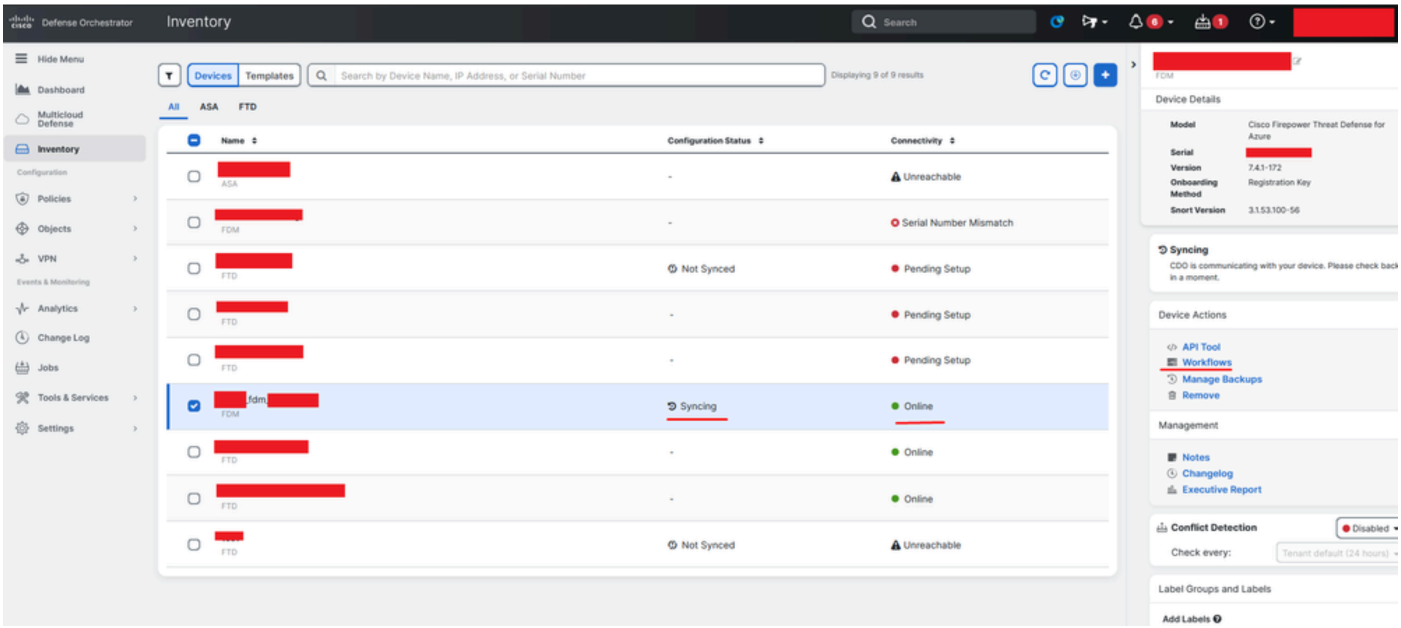
Disabled

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco SecureX threat response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.

FDM註冊完成

在CDO的「存貨」功能表中，FDM可在登入和同步化過程中找到。可以在工作流部分中檢視此同步的進度和流。

此程式完成後，會顯示為「已同步」和「線上」。



☐	Name	Configuration Status	Connectivity
☐	[redacted] ASA	-	Unreachable
☐	[redacted] FDM	-	Serial Number Mismatch
☐	[redacted] FTD	Not Synced	Pending Setup
☐	[redacted] FTD	-	Pending Setup
☐	[redacted] FTD	-	Pending Setup
☑	[redacted]fdm[redacted] FDM	Syncing	Online
☐	[redacted] FTD	-	Online
☐	[redacted] FTD	-	Online
☐	[redacted] FTD	Not Synced	Unreachable

[redacted]
FDM

Device Details

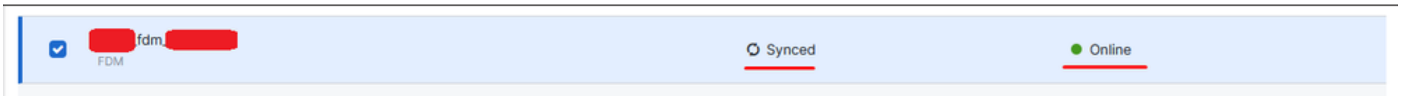
Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.4.1-172
Onboarding Method	Registration Key
Snort Version	3.1.53.100-56

Syncing
CDO is communicating with your device. Please check back in a moment.

Conflict Detection: Disabled
Check every: Tenant default (24 hours)

已登入CDO清查FDM

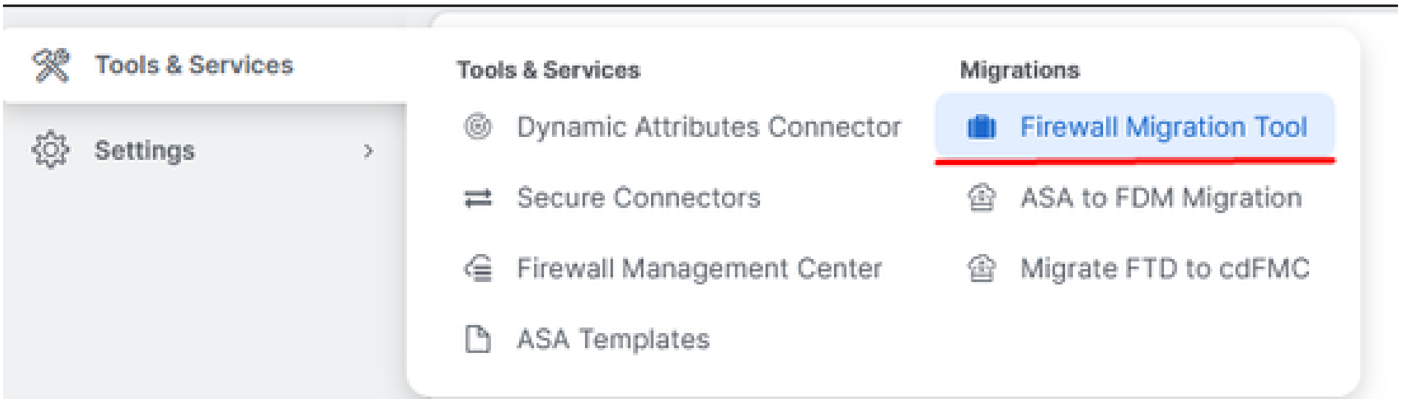
裝置同步後，將顯示為「聯機」和「已同步」。



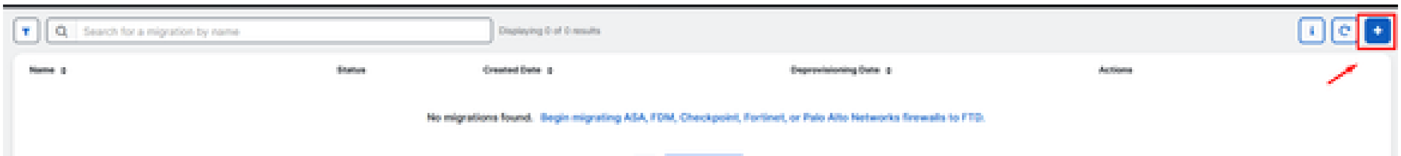
☑	[redacted]fdm[redacted] FDM	Synced	Online

FDM已登入

當FDM成功登入CDO後，我們必須登出FDM。註銷FDM後，在CDO中導航至工具和服務>遷移>防火牆遷移工具。

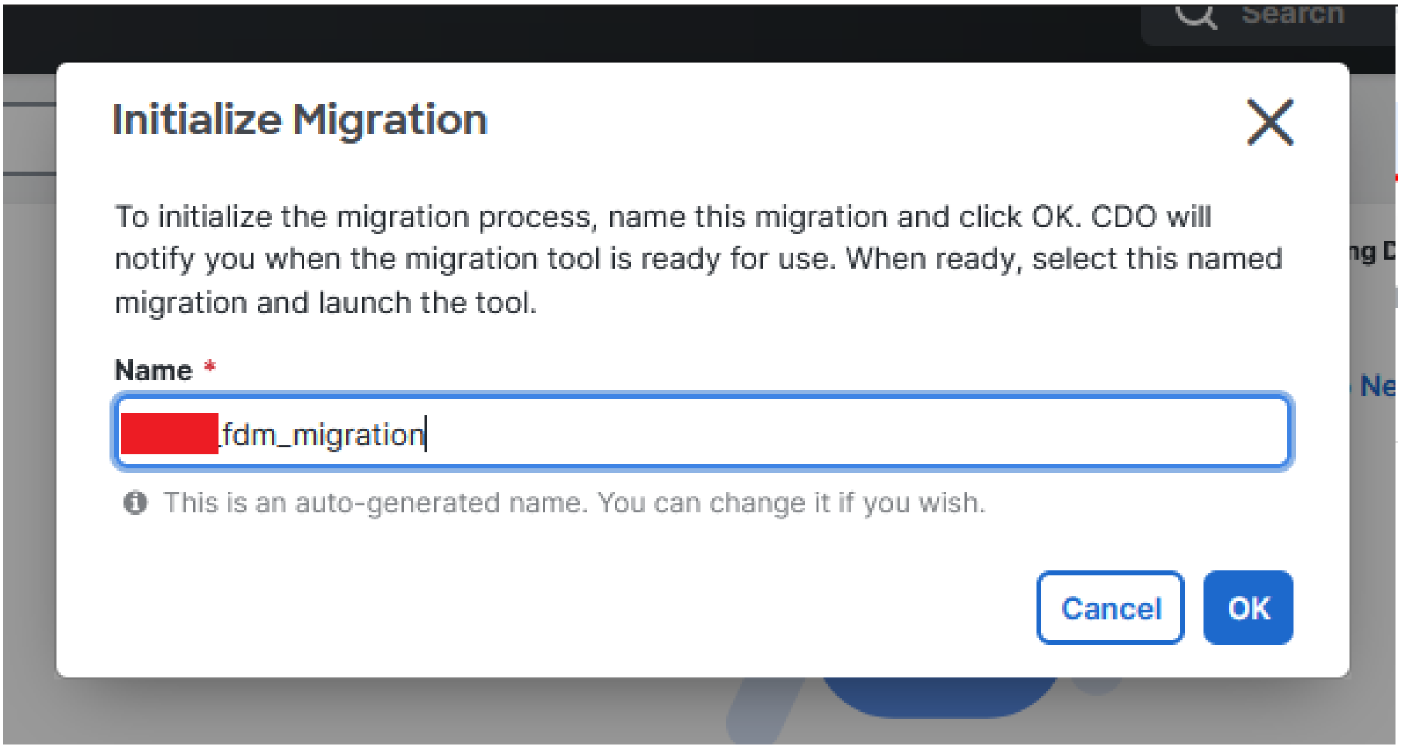


按一下Add符號，系統會顯示一個隨機名稱，指示需要重新命名該名稱以啟動遷移過程。



No migrations found. Begin migrating ASA, FDM, Checkpoint, Fortinet, or Palo Alto Networks firewalls to FTD.

重新命名後，按一下Launch開始遷移。



Initialize Migration

To initialize the migration process, name this migration and click OK. CDO will notify you when the migration tool is ready for use. When ready, select this named migration and launch the tool.

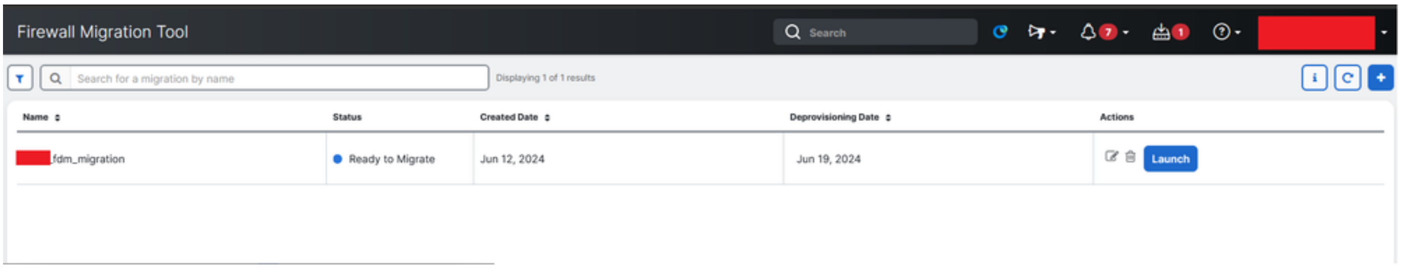
Name *

[redacted]fdm_migration

This is an auto-generated name. You can change it if you wish.

初始化移轉

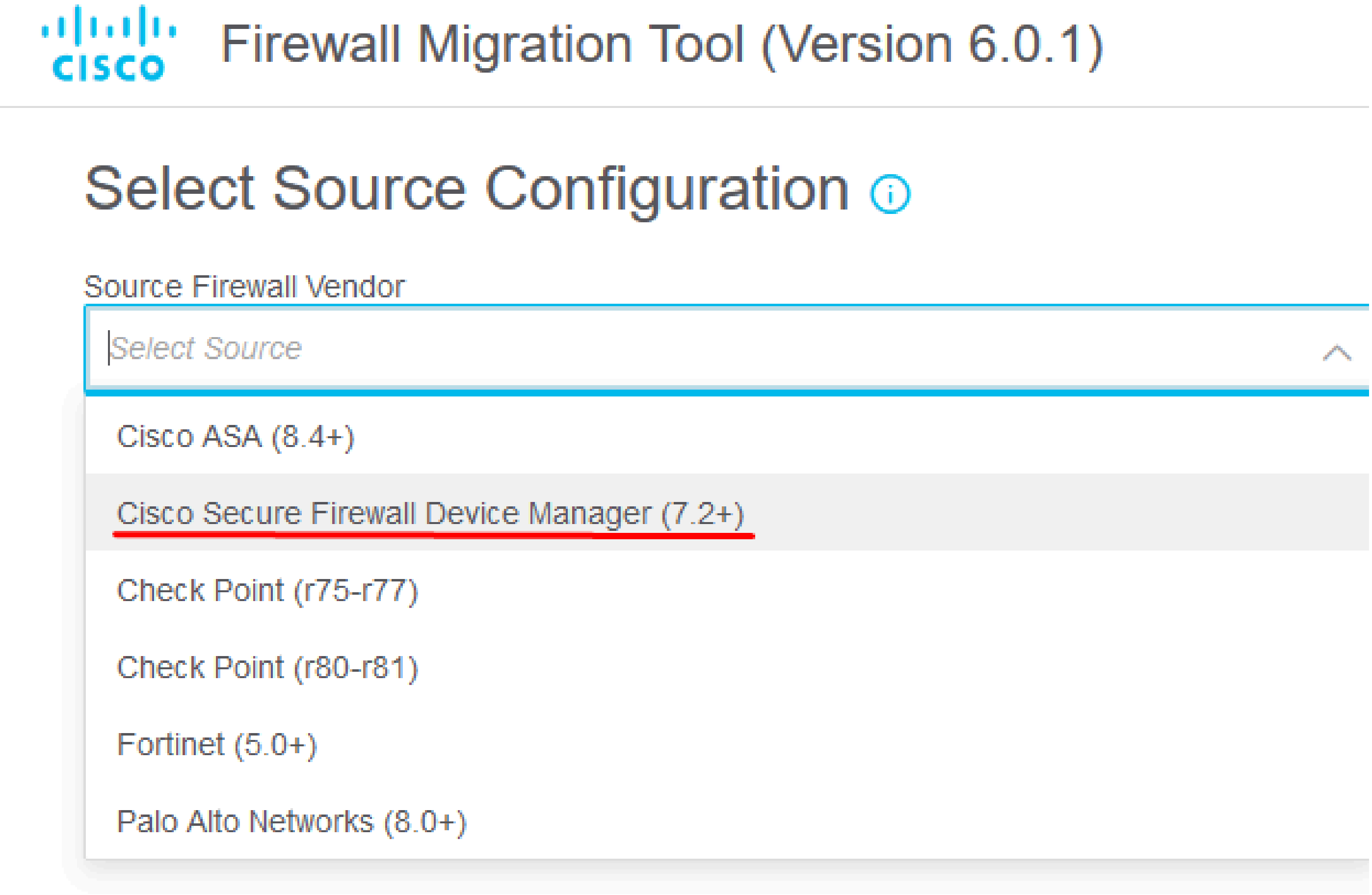
按一下Launch開始遷移配置。



Name	Status	Created Date	Deprovisioning Date	Actions
[redacted]fdm_migration	● Ready to Migrate	Jun 12, 2024	Jun 19, 2024	Launch

移轉啟動程式

點選啟動後，將打開一個窗口，供選擇思科安全防火牆裝置管理器(7.2+)選項的遷移進程使用。如前所述，此選項從版本7.2開始啟用。

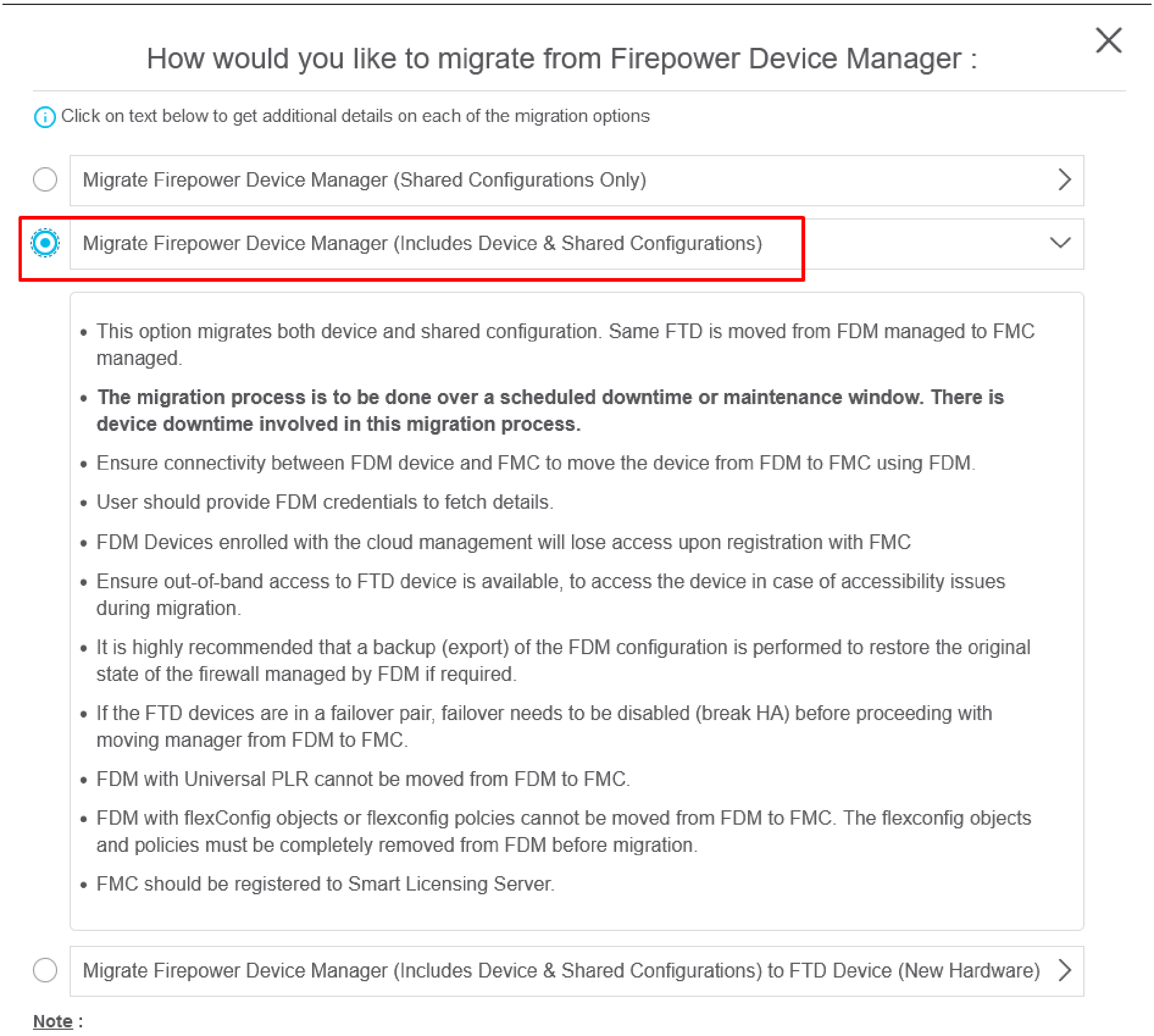


Firewall Migration Tool (Version 6.0.1)
Select Source Configuration
Source Firewall Vendor
Select Source
Cisco ASA (8.4+)
Cisco Secure Firewall Device Manager (7.2+)
Check Point (r75-r77)
Check Point (r80-r81)
Fortinet (5.0+)
Palo Alto Networks (8.0+)

FMT選取來源組態

選取此選項後，會顯示三種不同的移轉選項：僅限共用組態、包含裝置與共用組態，以及包含裝置與FTD新硬體的共用組態。

對於此例項，將執行第二個選項「遷移Firepower裝置管理器」（包括裝置和共用配置）。



How would you like to migrate from Firepower Device Manager :

Click on text below to get additional details on each of the migration options

○ Migrate Firepower Device Manager (Shared Configurations Only)

● Migrate Firepower Device Manager (Includes Device & Shared Configurations)

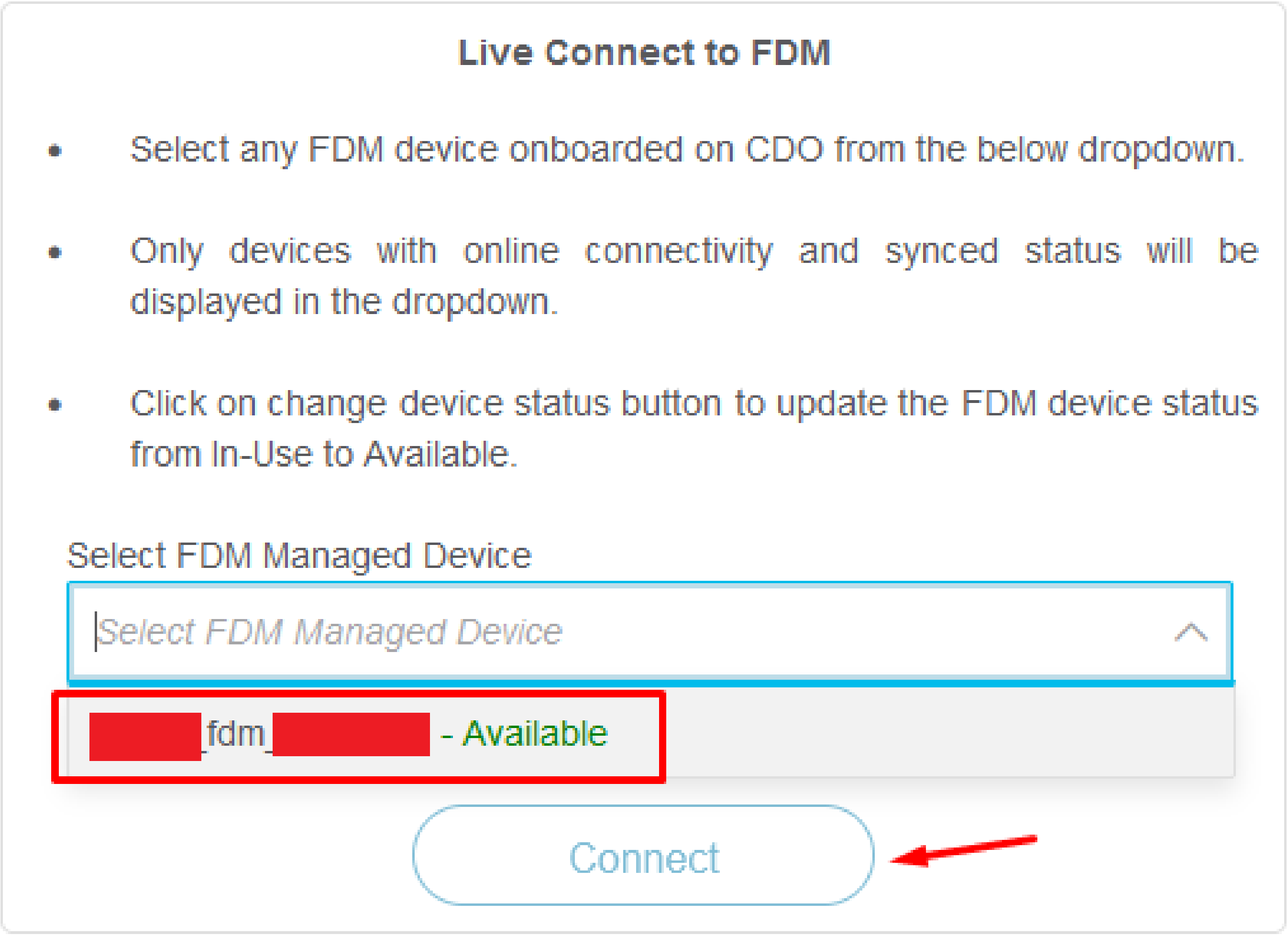
- This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
- **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
- Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
- User should provide FDM credentials to fetch details.
- FDM Devices enrolled with the cloud management will lose access upon registration with FMC
- Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.
- It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required.
- If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC.
- FDM with Universal PLR cannot be moved from FDM to FMC.
- FDM with flexConfig objects or flexconfig polcies cannot be moved from FDM to FMC. The flexconfig objects and policies must be completely removed from FDM before migration.
- FMC should be registered to Smart Licensing Server.

○ Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware)

Note :

移轉選項

選擇遷移方法後，繼續從提供的清單中選擇裝置。



Live Connect to FDM

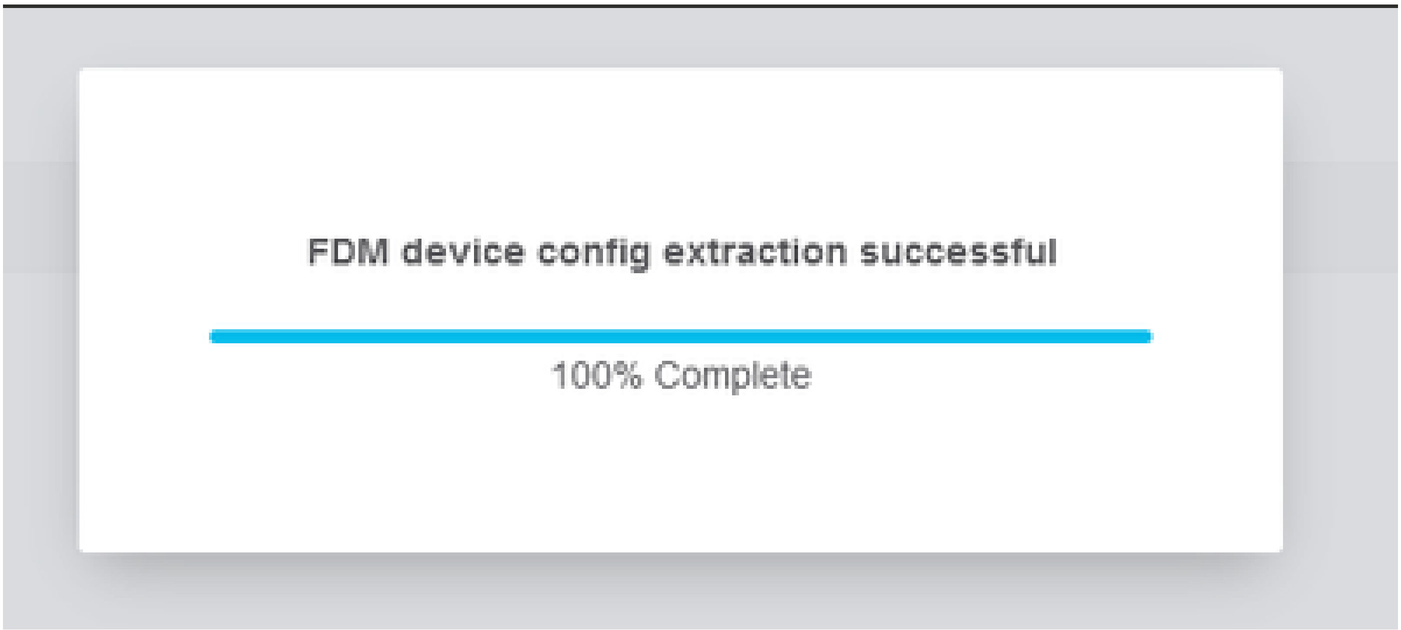
- Select any FDM device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.
- Click on change device status button to update the FDM device status from In-Use to Available.

Select FDM Managed Device

Select FDM Managed Device

[redacted]_fdm_[redacted] - Available

FDM裝置選擇

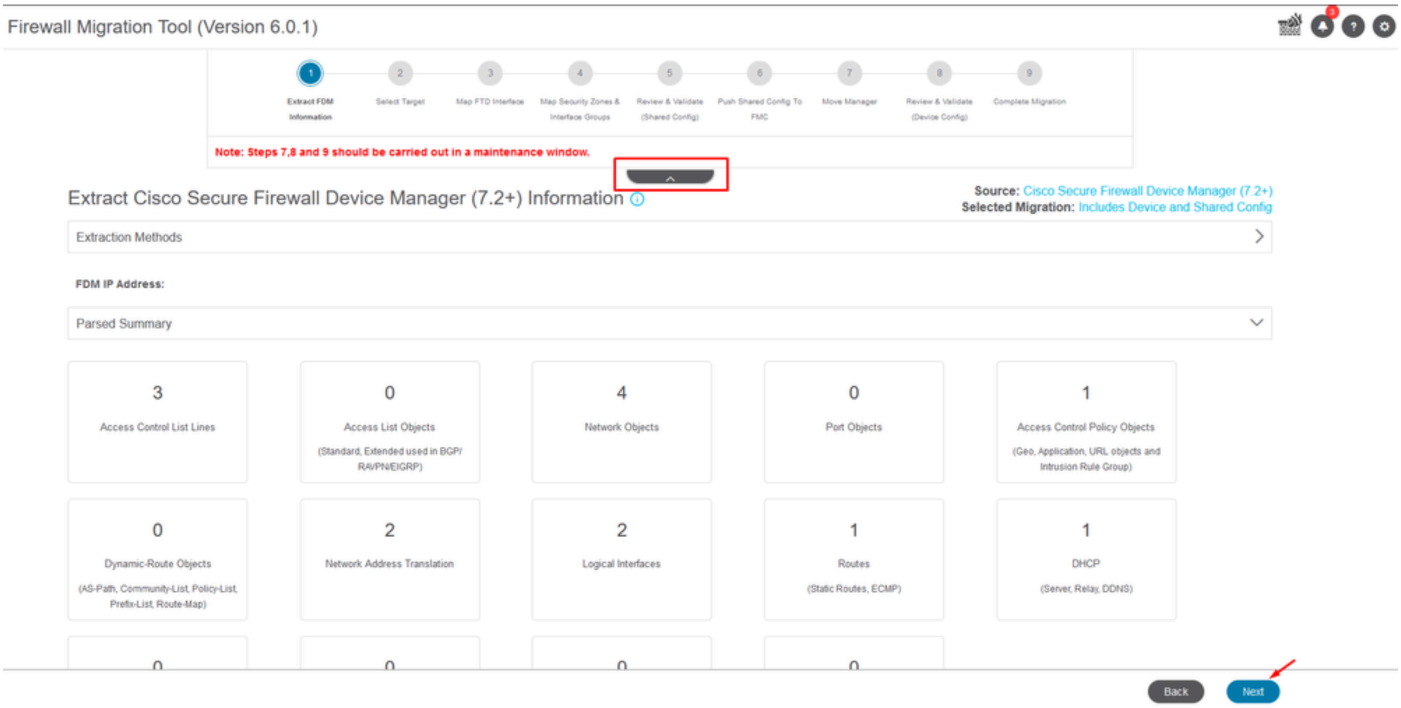


FDM device config extraction successful

100% Complete

配置提取已完成

建議打開位於頂部的頁籤，檢視並瞭解選擇裝置時的步驟。



Firewall Migration Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration
Extraction Methods
Parsed Summary
Back
Next

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Extract Cisco Secure Firewall Device Manager (7.2+) Information

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

FDM IP Address:

3 Access Control List Lines

0 Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)

4 Network Objects

0 Port Objects

1 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)

0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)

2 Network Address Translation

2 Logical Interfaces

1 Routes (Static Routes, ECMP)

1 DHCP (Server, Relay, DDNS)

0

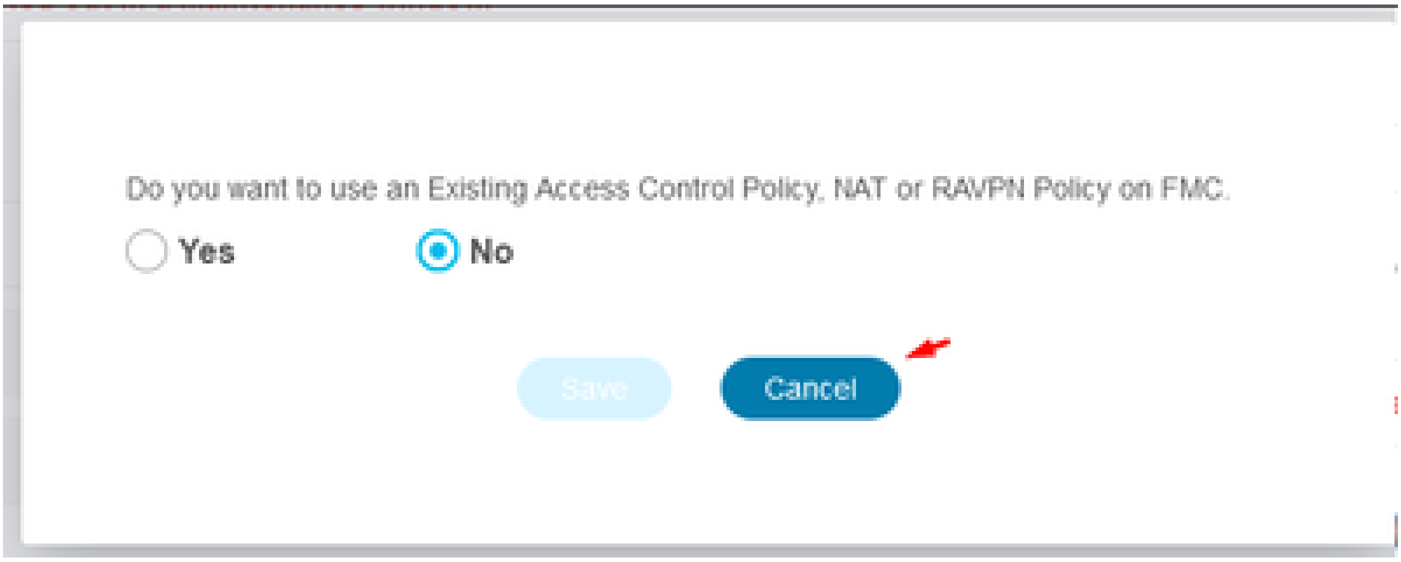
0

0

0

移轉程式的步驟

作為新遷移，當系統提示Do you want to use an Existing Access Control Policy， NAT or RAVPN Policy on FMC？ 選項時，請選擇Cancel

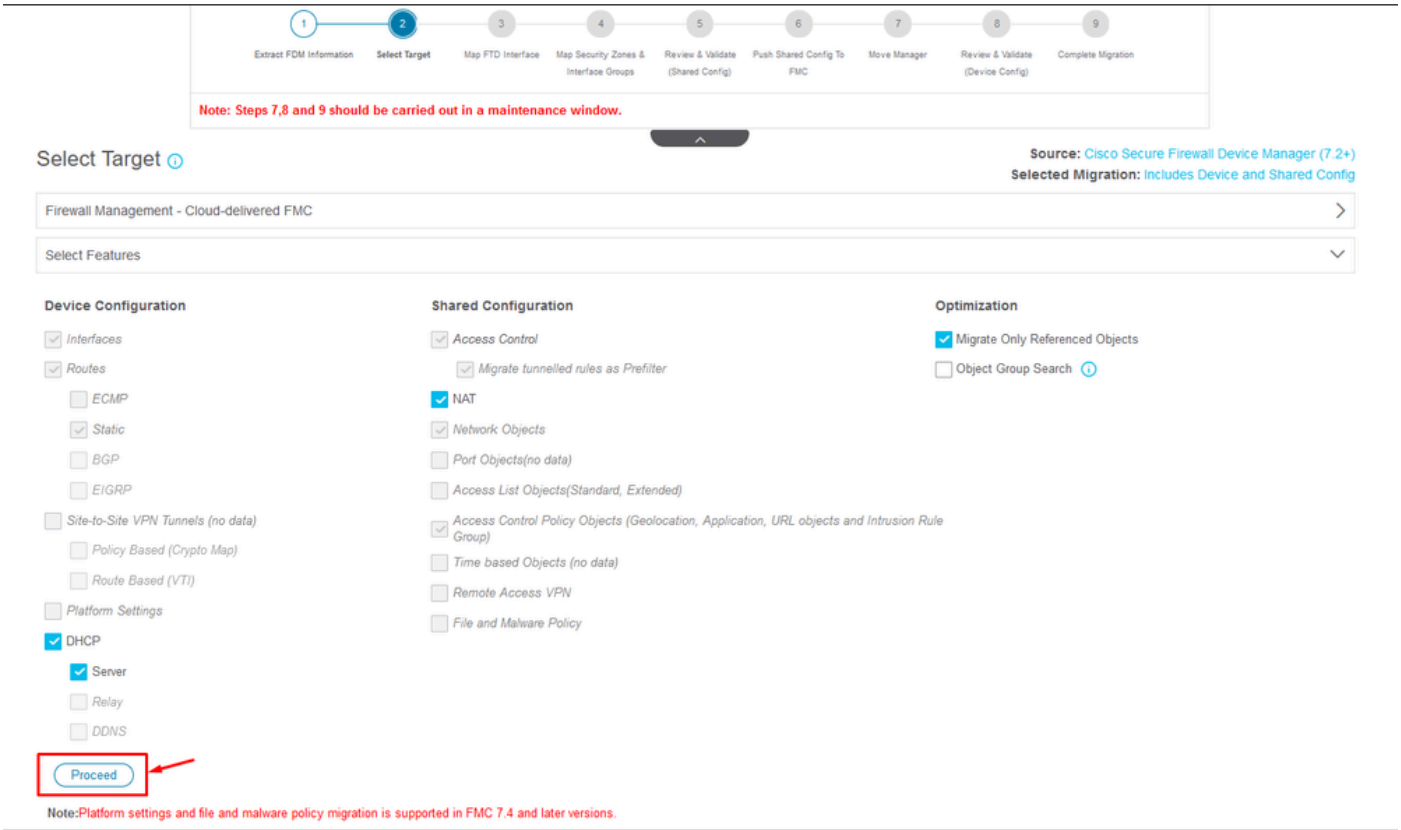


Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.

○ Yes ● No

現有組態的取消選項

之後，會提供選項來選取要移轉的功能，如圖所示。按一下Proceed。



1 Extract FDM Information — 2 Select Target — 3 Map FTD Interface — 4 Map Security Zones & Interface Groups — 5 Review & Validate (Shared Config) — 6 Push Shared Config To FMC — 7 Move Manager — 8 Review & Validate (Device Config) — 9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Select Target

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

Firewall Management - Cloud-delivered FMC

Select Features

Device Configuration

- ☑ Interfaces
- ☑ Routes
  - □ ECMP
  - ☑ Static
  - □ BGP
  - □ EIGRP
- □ Site-to-Site VPN Tunnels (no data)
  - □ Policy Based (Crypto Map)
  - □ Route Based (VTI)
- □ Platform Settings
- ☑ DHCP
  - ☑ Server
  - □ Relay
  - □ DDNS

Shared Configuration

- ☑ Access Control
  - ☑ Migrate tunnelled rules as Prefilter
- ☑ NAT
- ☑ Network Objects
- □ Port Objects(no data)
- □ Access List Objects(Standard, Extended)
- ☑ Access Control Policy Objects (Geolocation, Application, URL objects and Intrusion Rule Group)
- □ Time based Objects (no data)
- □ Remote Access VPN
- □ File and Malware Policy

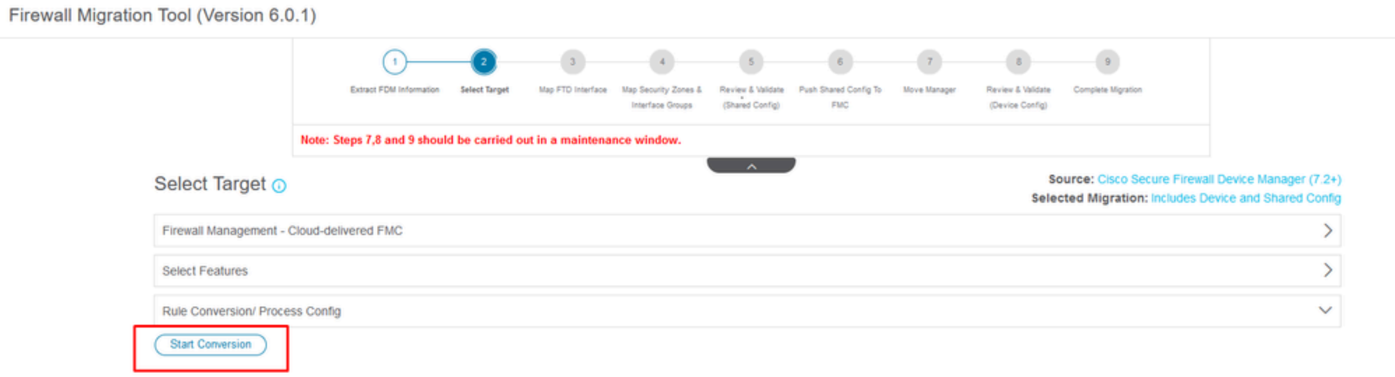
Optimization

- ☑ Migrate Only Referenced Objects
- □ Object Group Search

Note:Platform settings and file and malware policy migration is supported in FMC 7.4 and later versions.

要選取的特徵

然後開始轉換。



Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information — 2 Select Target — 3 Map FTD Interface — 4 Map Security Zones & Interface Groups — 5 Review & Validate (Shared Config) — 6 Push Shared Config To FMC — 7 Move Manager — 8 Review & Validate (Device Config) — 9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Select Target

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

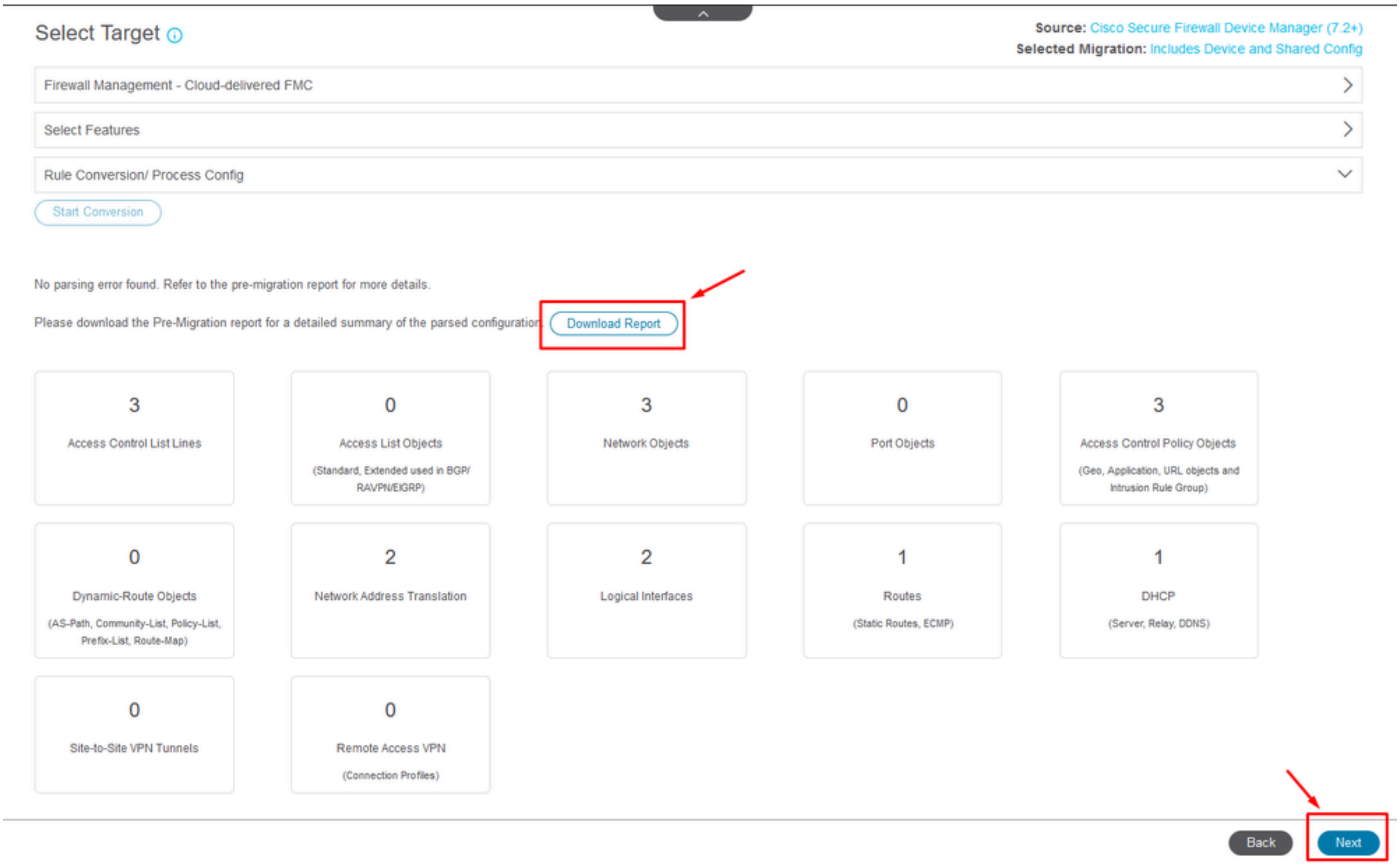
Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

開始轉換。

解析過程完成後，可以使用兩個選項：下載文檔並透過按一下下一步繼續遷移。



Select Target

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

Start Conversion

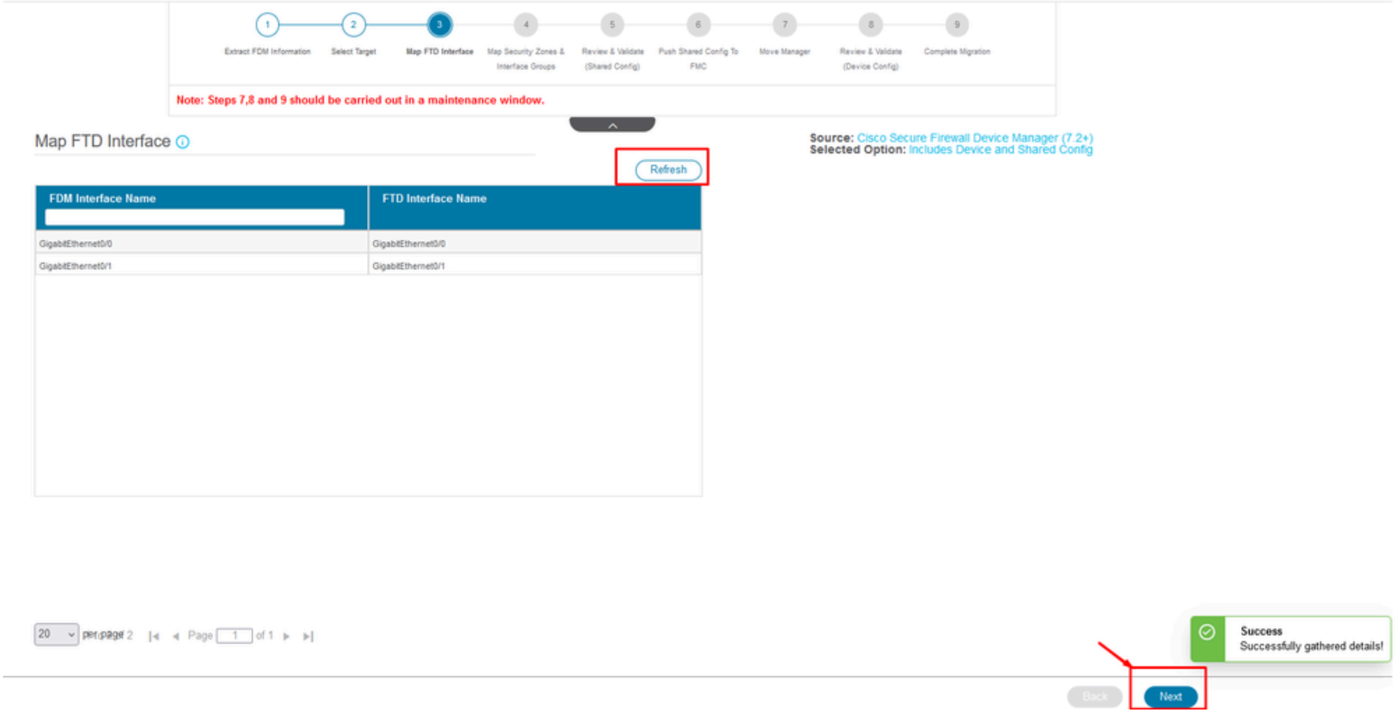
No parsing error found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration. Download Report

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPN/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	2 Network Address Translation	2 Logical Interfaces	1 Routes (Static Routes, ECMP)	1 DHCP (Server, Relay, DDNS)
0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)			

下載報告。

裝置介面已設定為顯示。作為一種最佳實踐，建議按一下Refresh更新介面。驗證之後，您可以點選下一步繼續。



1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Map FTD Interface

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

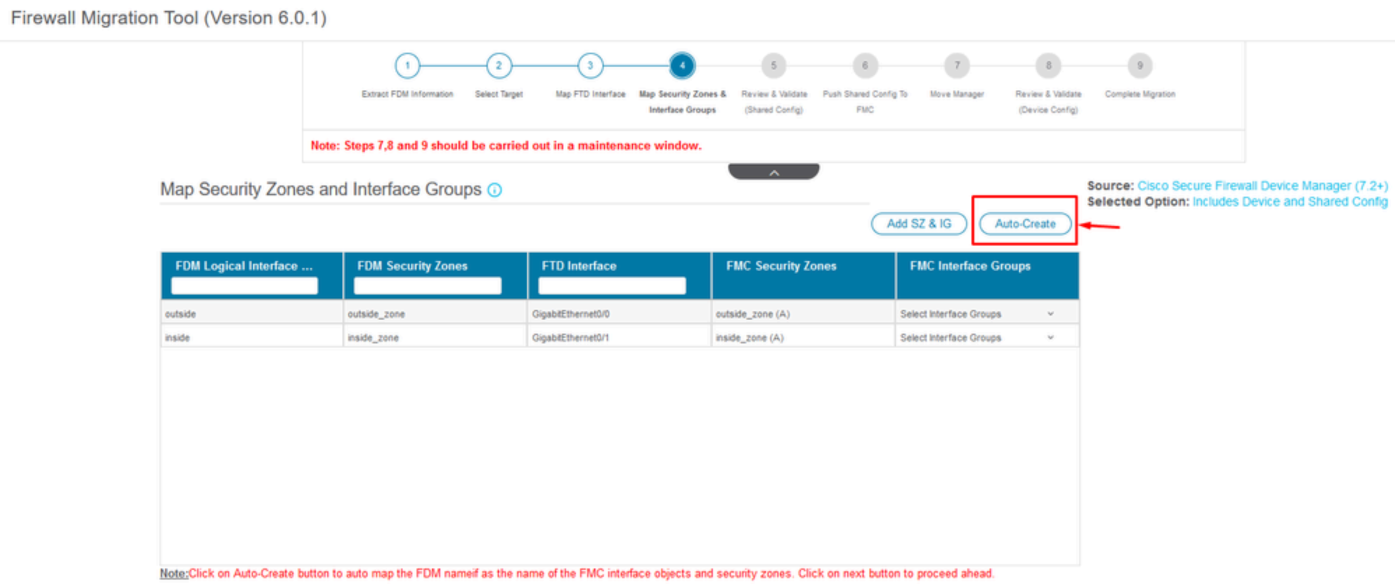
FDM Interface Name	FTD Interface Name
GigabitEthernet0/0	GigabitEthernet0/0
GigabitEthernet0/1	GigabitEthernet0/1

20 per page 2 Page 1 of 1

Success
Successfully gathered details!

顯示的介面

導航到安全區域和介面組部分，需要使用「增加SZ和IG」手動增加。 對於此示例，已選擇Auto-Create。這有助於自動生成要遷移到的FMC中的介面。完成後，按一下Next按鈕。


1
Extract FDM Information
2
Select Target
3
Map FTD Interface
4
Map Security Zones & Interface Groups
5
Review & Validate (Shared Config)
6
Push Shared Config To FMC
7
Move Manager
8
Review & Validate (Device Config)
9
Complete Migration
Add SZ & IG
Auto-Create

Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Map Security Zones and Interface Groups

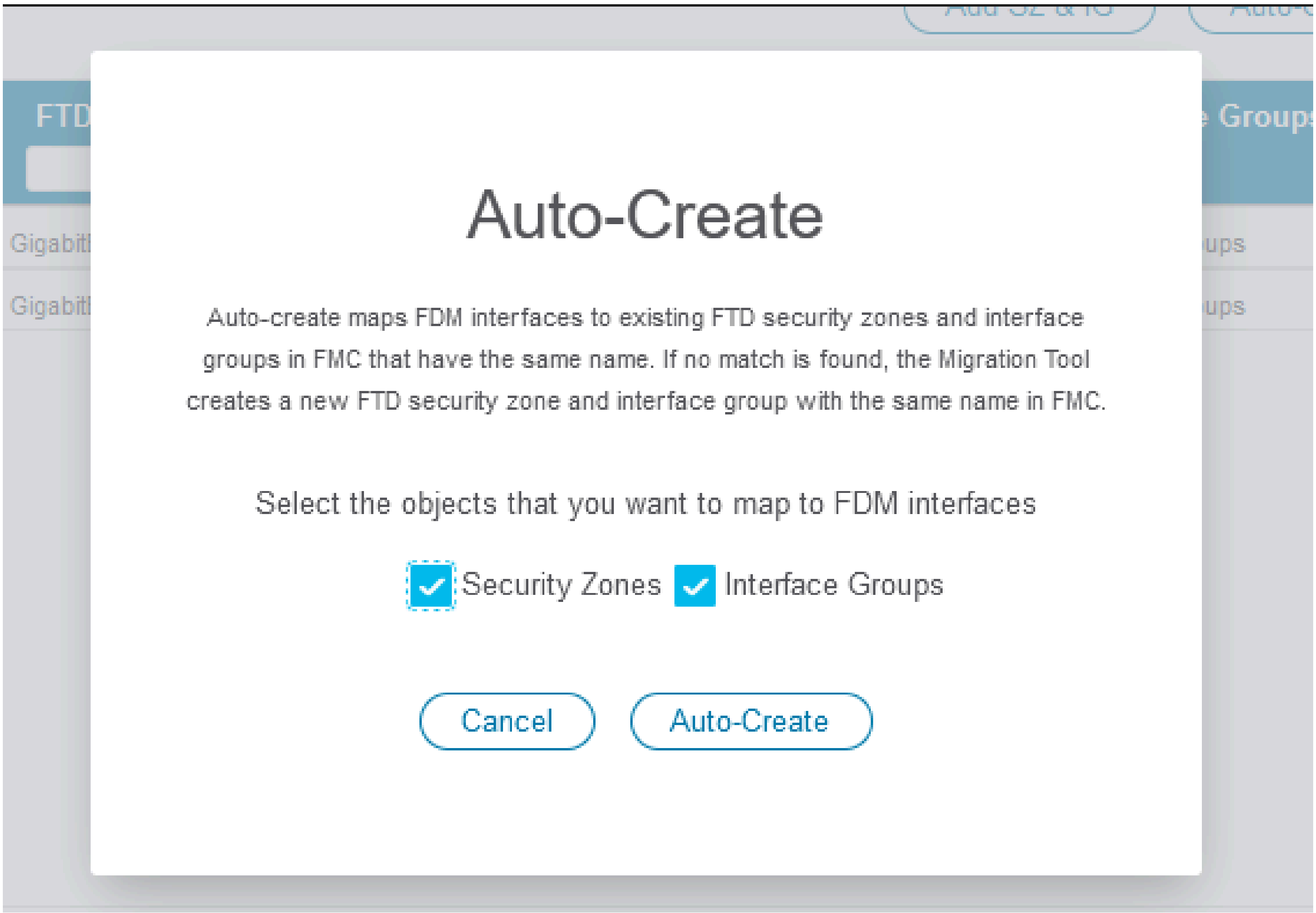
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Logical Interface ...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	Select Interface Groups
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups

Note:Click on Auto-Create button to auto map the FDM nameif as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

安全區域和介面組

「自動建立」選項會將FDM介面對映至現有FTD安全性區域和FMC中具有相同名稱的介面群組。



Auto-Create

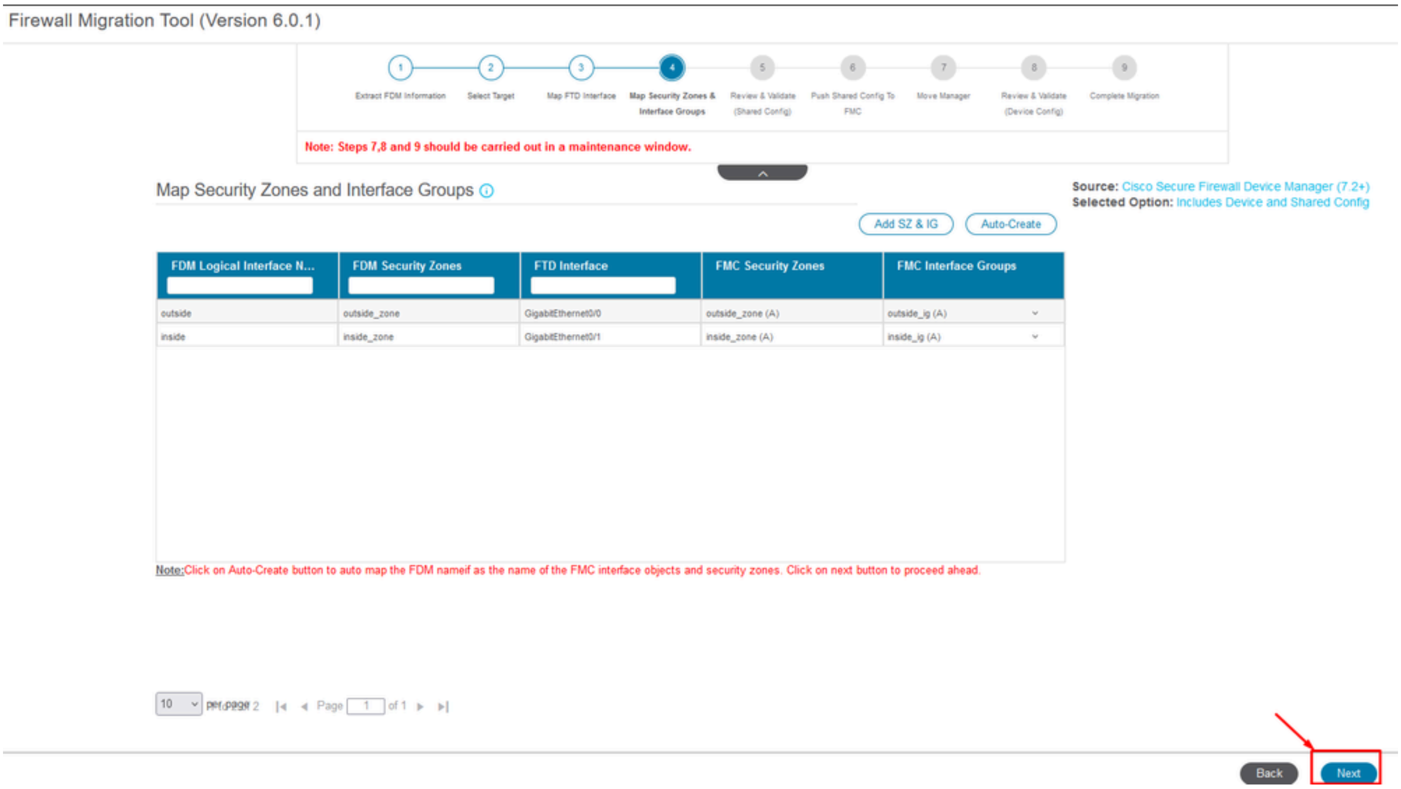
Auto-create maps FDM interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to FDM interfaces

☑ Security Zones ☑ Interface Groups

自動建立選項。

然後選擇Next。



Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Map Security Zones and Interface Groups

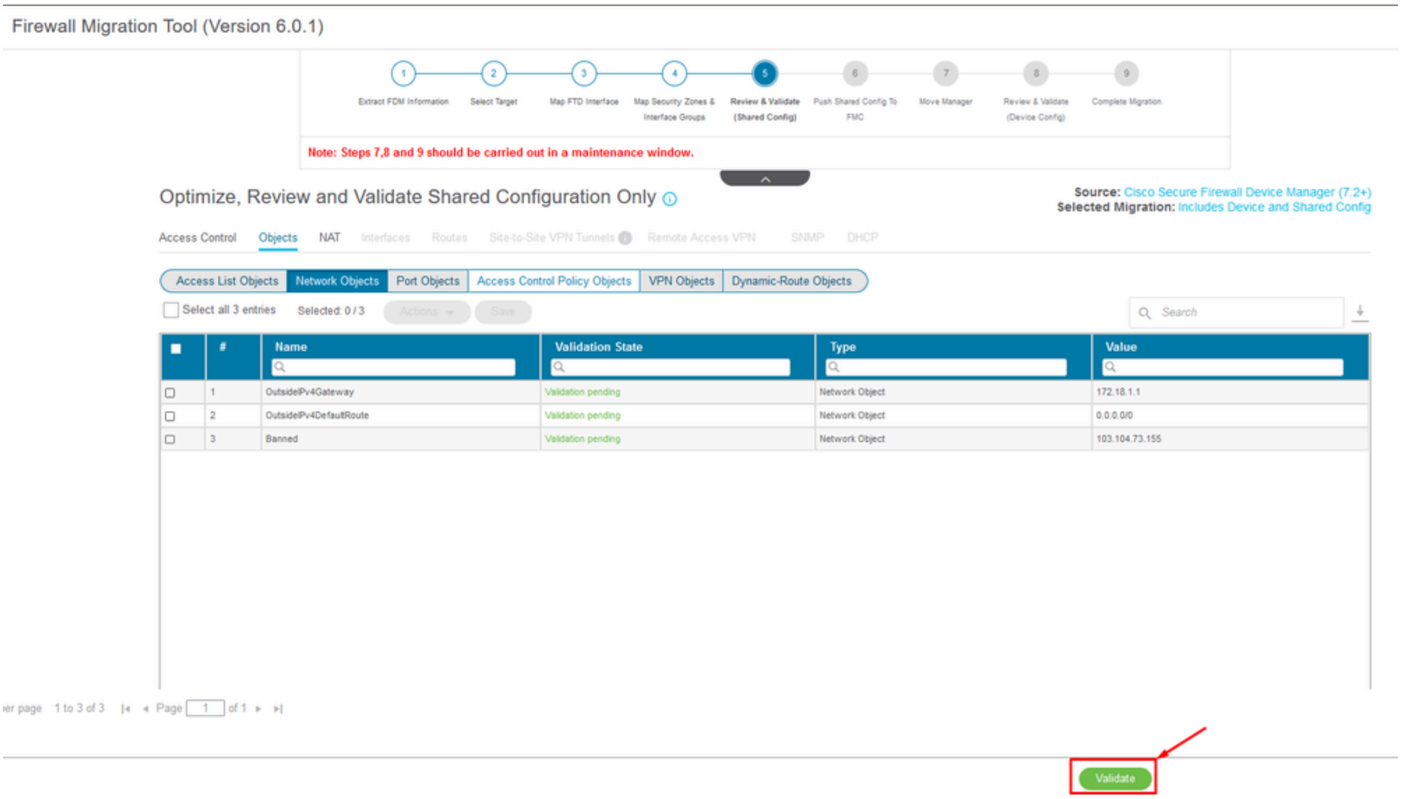
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Logical Interface N...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A)
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)

Note:Click on Auto-Create button to auto map the FDM nameif as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

自動建立後選項。

如頂欄所示，在步驟5中，請花時間檢查訪問控制策略(ACP)、對象和NAT規則。繼續仔細檢視每個專案，然後按一下Validate確認名稱或配置沒有問題。



Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

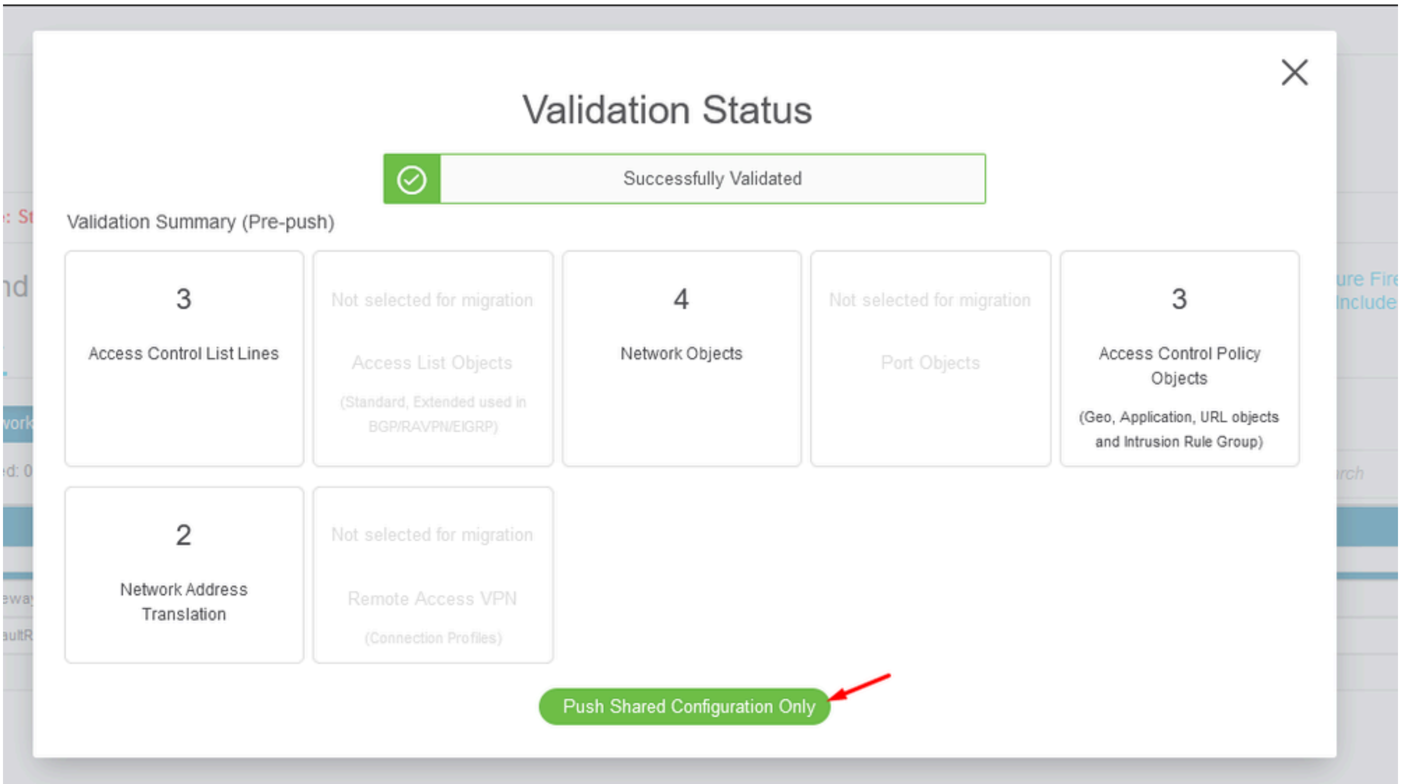
Optimize, Review and Validate Shared Configuration Only

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

■	#	Name	Validation State	Type	Value
□	1	OutsideIPv4Gateway	Validation pending	Network Object	172.18.1.1
□	2	OutsideIPv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
□	3	Banned	Validation pending	Network Object	103.104.73.155

訪問控制、對象和NAT配置

然後僅推送共用配置



Validation Status

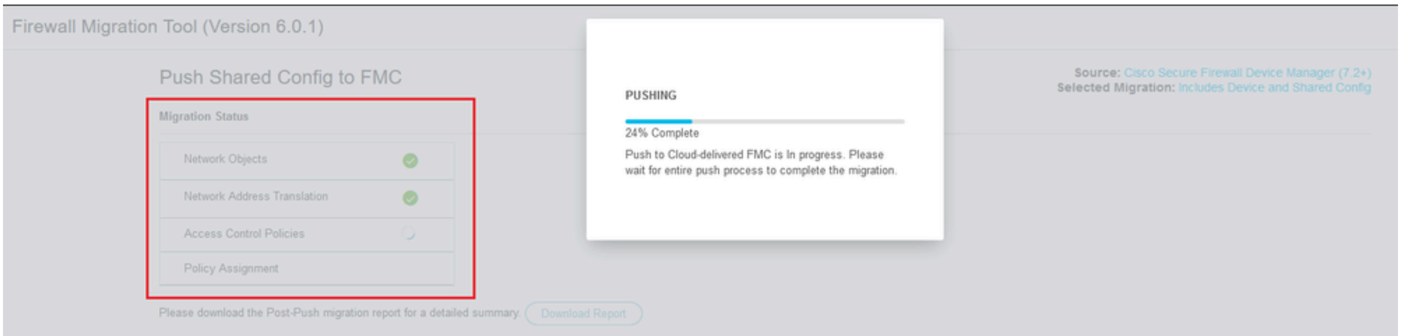
Successfully Validated

Validation Summary (Pre-push)

3 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2 Network Address Translation	Not selected for migration Remote Access VPN (Connection Profiles)			

僅推送共用配置

可以觀察到完成百分比和正在處理的特定任務。



Firewall Migration Tool (Version 6.0.1)

Push Shared Config to FMC

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

Migration Status

- Network Objects ✓
- Network Address Translation ✓
- Access Control Policies
- Policy Assignment

PUSHING

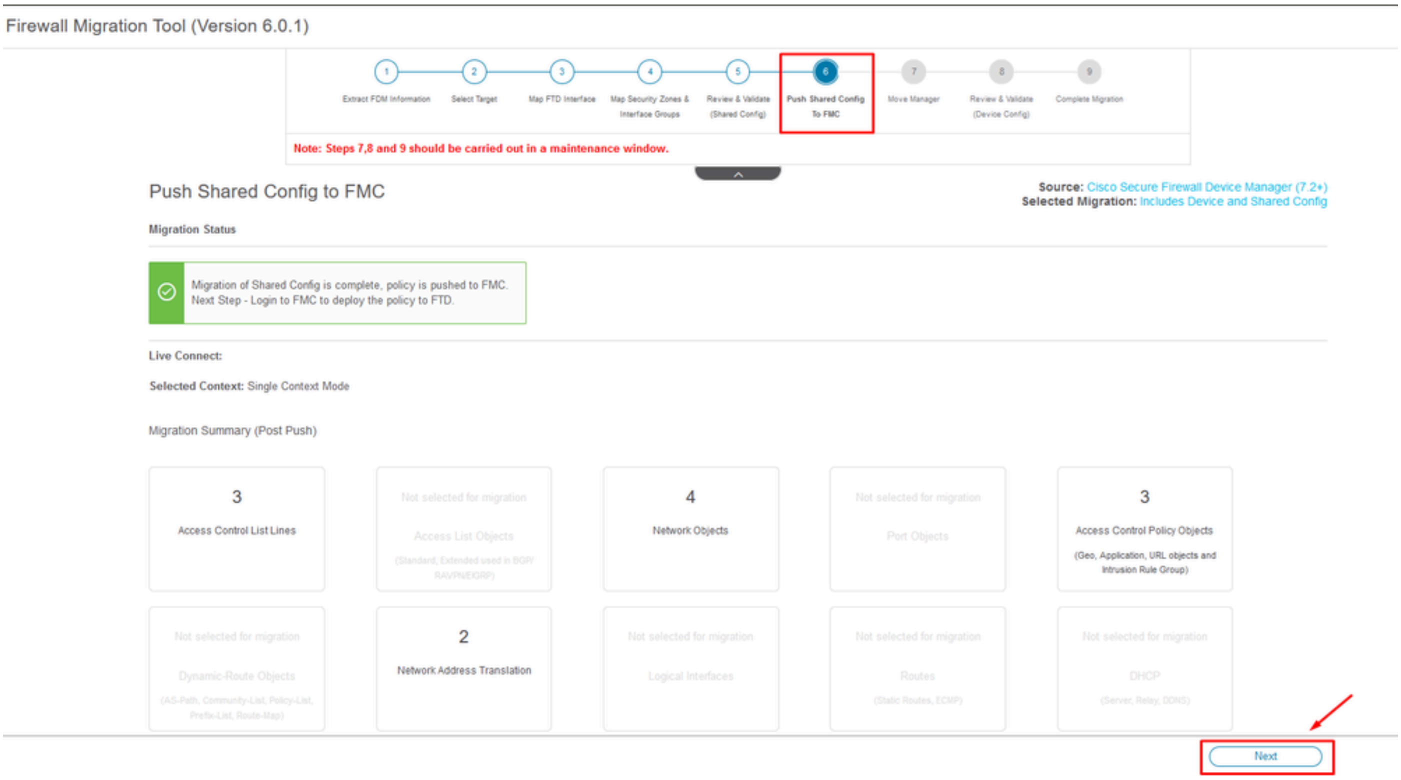
24% Complete

Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.

Please download the Post-Push migration report for a detailed summary.

推進百分比

完成步驟5後，繼續執行步驟6（如頂欄所示），在此步驟中會執行將共用配置推送到FMC。這時，請選擇Next按鈕以繼續。


Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Push Shared Config to FMC

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

Migration Status

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

3 Access Control List Lines

Not selected for migration – Access List Objects (Standard, Extended used in BGP/ RAVPN/EIGRP)

4 Network Objects

Not selected for migration – Port Objects

3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)

Not selected for migration – Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)

2 Network Address Translation

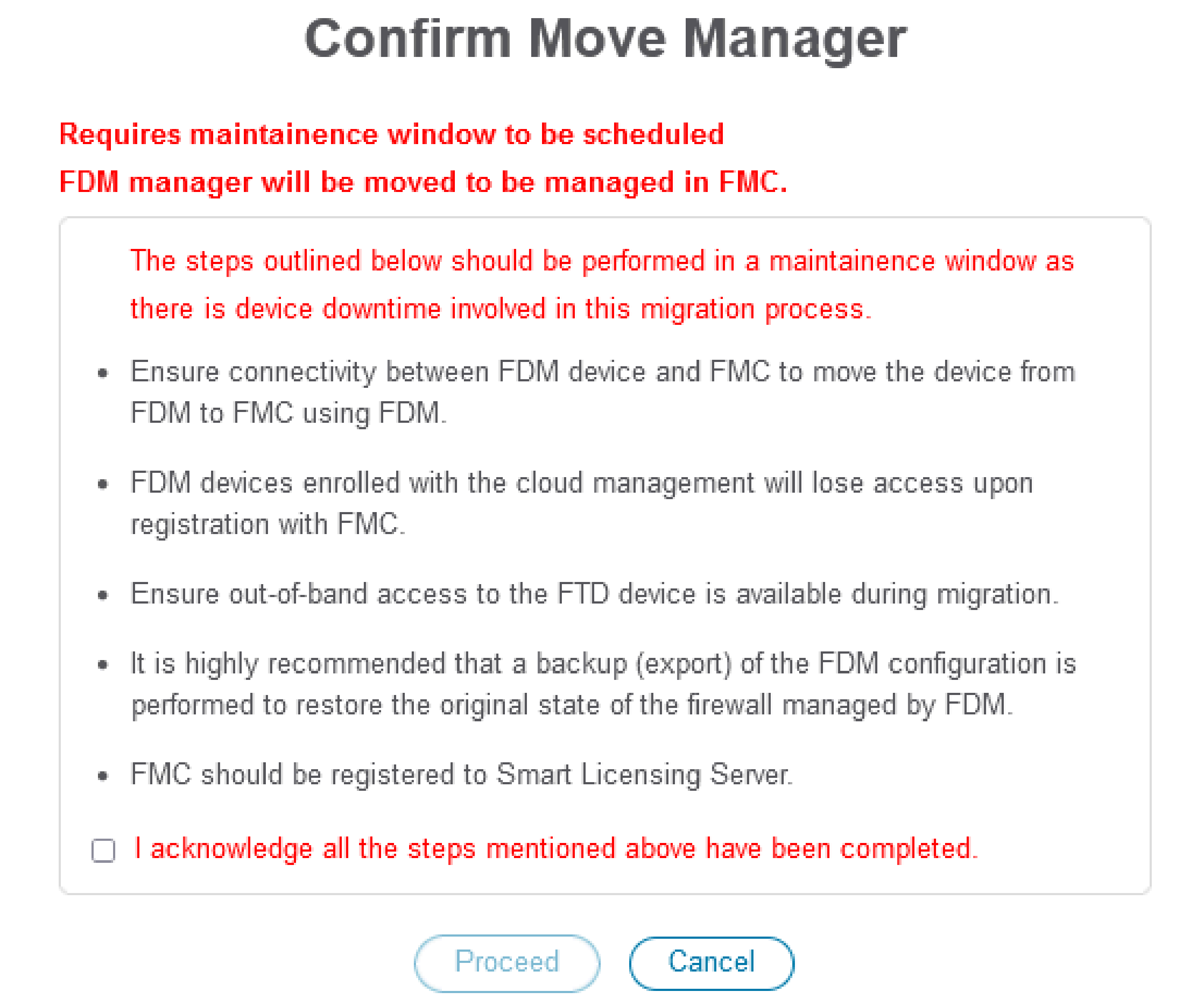
Not selected for migration – Logical Interfaces

Not selected for migration – Routes (Static Routes, ECMP)

Not selected for migration – DHCP (Server, Relay, DDNS)

將共用配置推送到FMC已完成

此選項會觸發確認訊息，提示繼續移轉管理員。



Confirm Move Manager

Requires maintainence window to be scheduled

FDM manager will be moved to be managed in FMC.

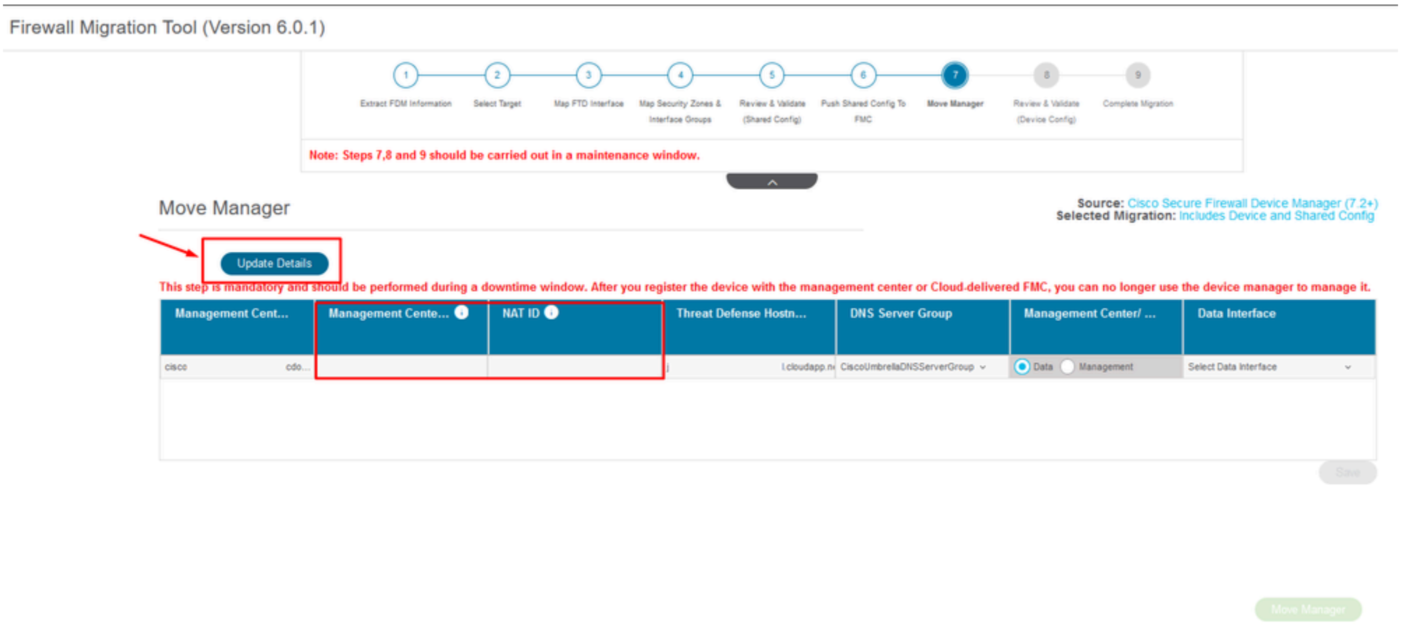
The steps outlined below should be performed in a maintainence window as there is device downtime involved in this migration process.

- Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
- FDM devices enrolled with the cloud management will lose access upon registration with FMC.
- Ensure out-of-band access to the FTD device is available during migration.
- It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM.
- FMC should be registered to Smart Licensing Server.

□ I acknowledge all the steps mentioned above have been completed.

確認移動管理員

要繼續管理員遷移，必須擁有管理中心ID和NAT ID，這一點非常重要。透過選擇Update Details可以檢索這些ID。此動作會啟動一個快顯視窗，在此視窗中輸入cdFMC中FDM表示的所需名稱，然後儲存變更。



Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

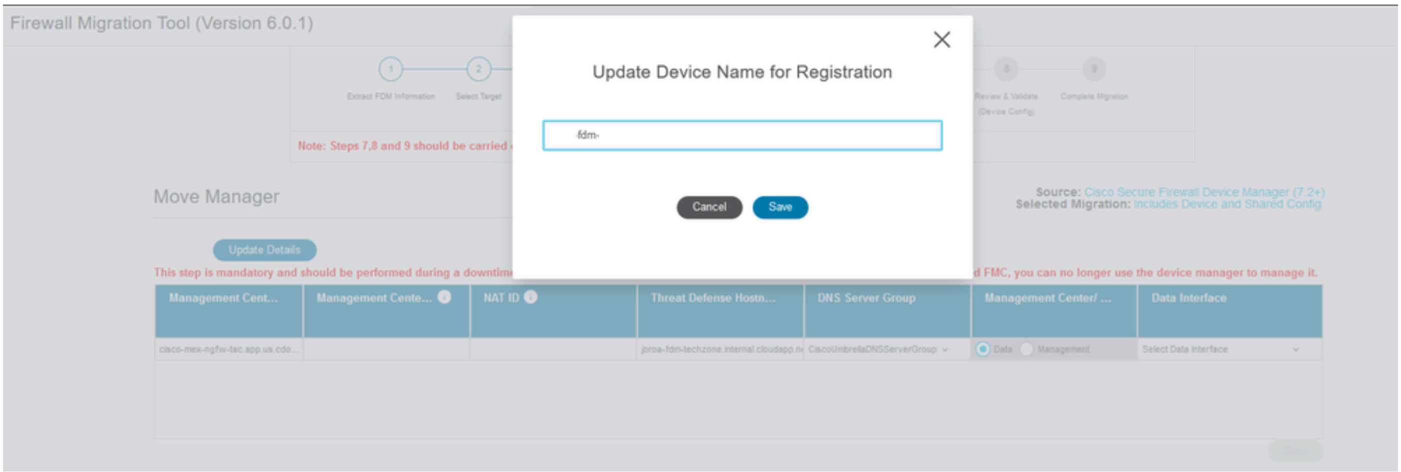
Move Manager

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

This step is mandatory and should be performed during a downtime window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco cdo...			j l.cloudapp.n	CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

管理員中心ID和NAT ID



Firewall Migration Tool (Version 6.0.1)

Update Device Name for Registration

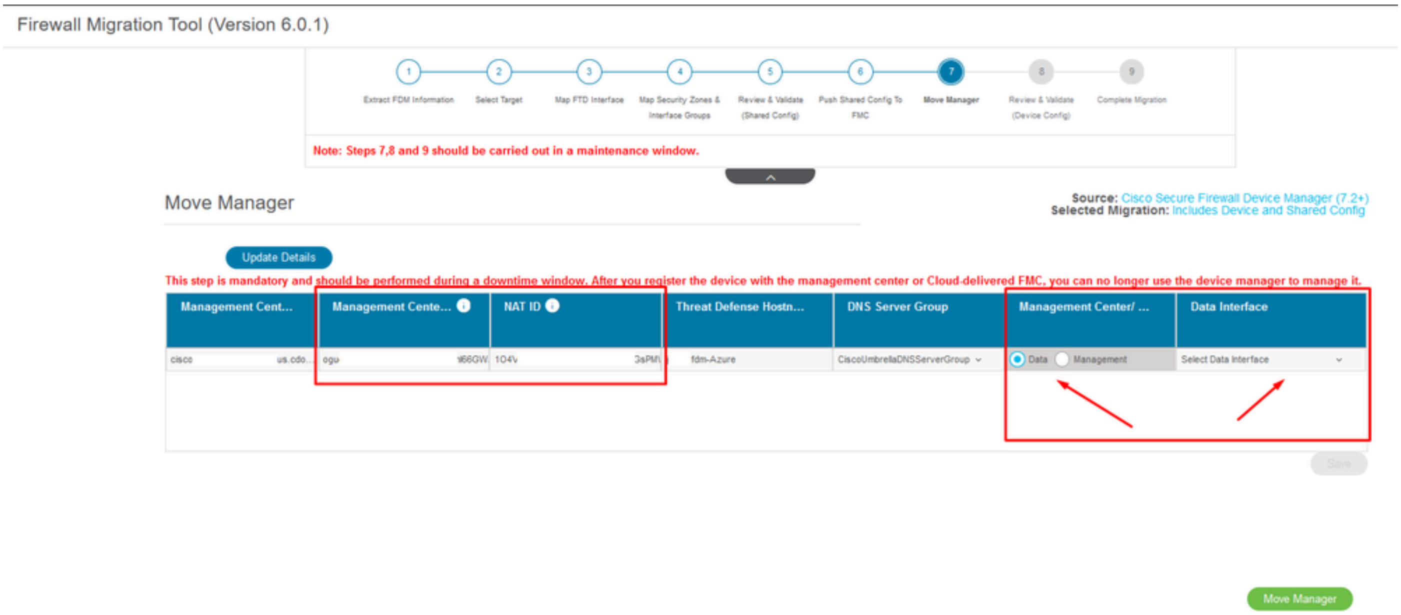
-fdm-

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco-mex-ngfw-tac.app.us.cdo...			joroa-fdm-techzone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

更新裝置名稱以進行註冊。

執行此操作後，將顯示上述欄位的ID。

警告：請勿對管理中心介面進行任何變更。依預設，會選取「管理」選項，保留此選項為預設設定。



Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Move Manager

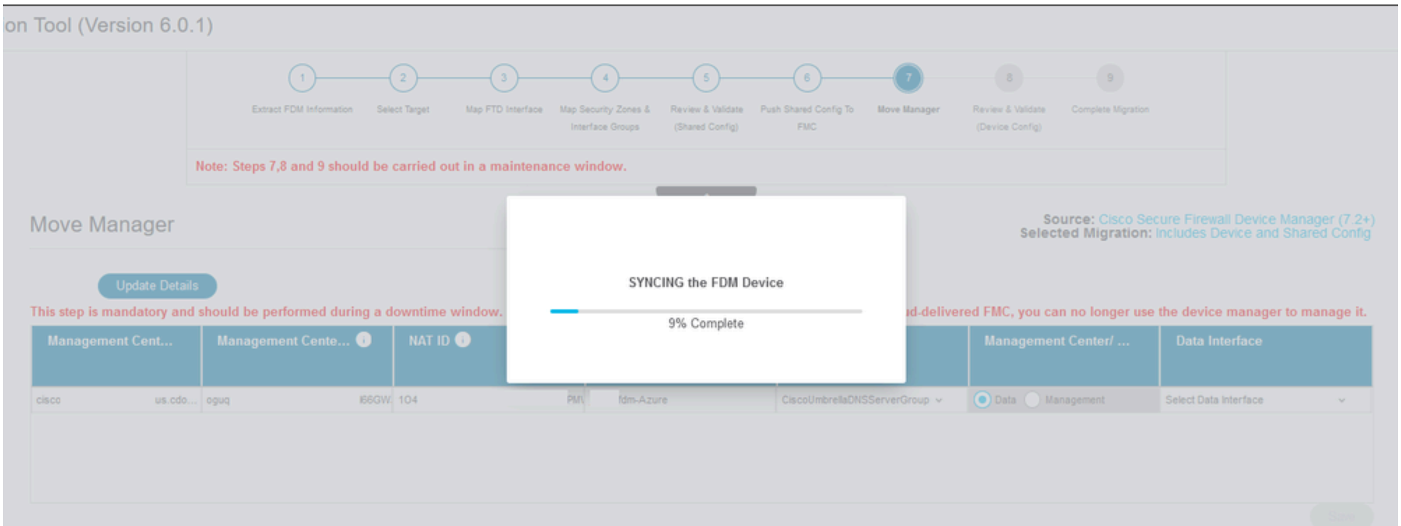
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

This step is mandatory and should be performed during a downtime window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco us.cdo...	ogu ‎‎ ‎‎ ‎‎ ‎‎ i66GW	1O4\ ‎‎ ‎‎ ‎‎ 3sPM\	fdm-Azure	CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

管理中心ID和NAT ID。

選擇Update Details 選項後，裝置將開始同步。



on Tool (Version 6.0.1)

1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Move Manager

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

This step is mandatory and should be performed during a downtime window. d-delivered FMC, you can no longer use the device manager to manage it.

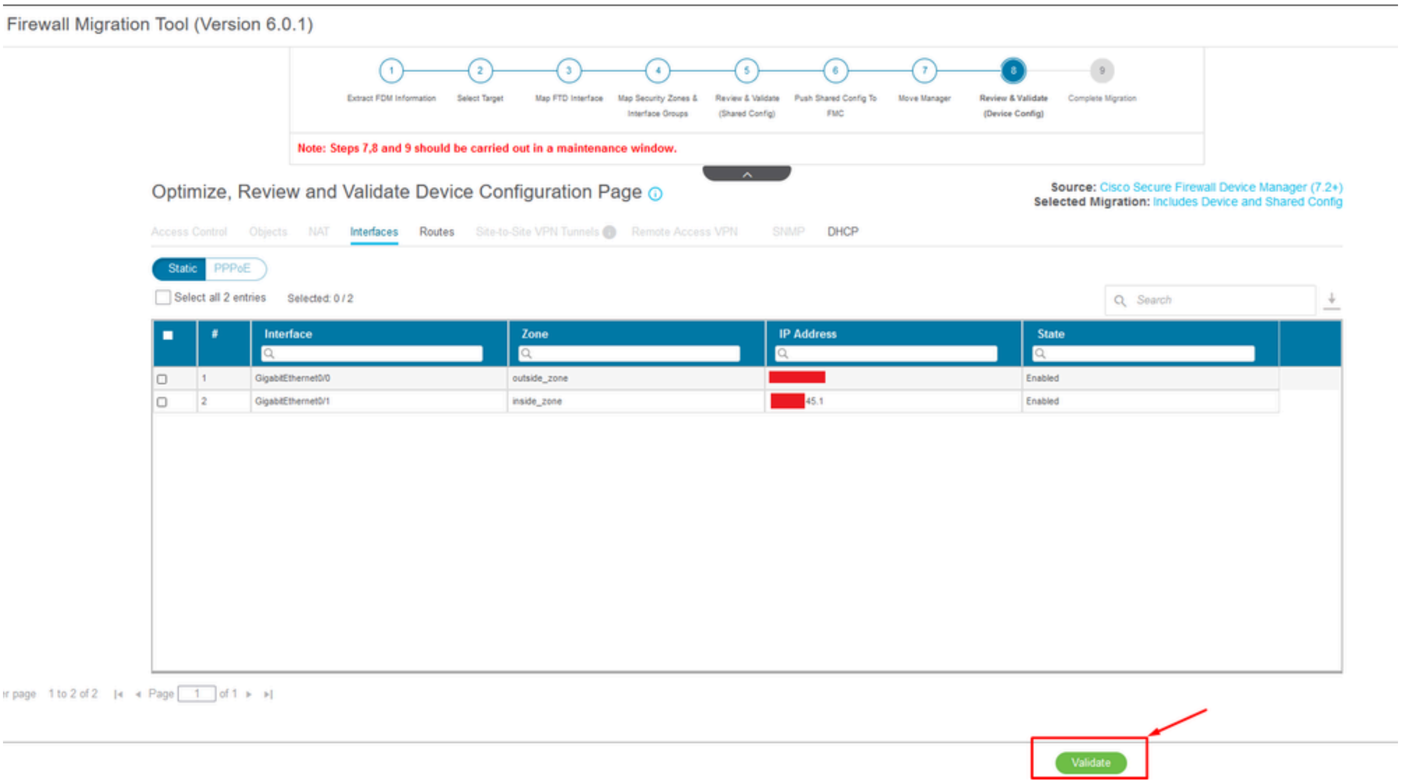
SYNCING the FDM Device

9% Complete

Management Cent...	Management Cente...	NAT ID		Management Center/ ...	Data Interface
cisco us.cdo...	oguq i66GW	104 PM\	fdm-Azure CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

同步FDM裝置

完成遷移後，下一步是透過選擇驗證來檢查FDM中配置的介面、路由和DHCP設定。



Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Optimize, Review and Validate Device Configuration Page

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

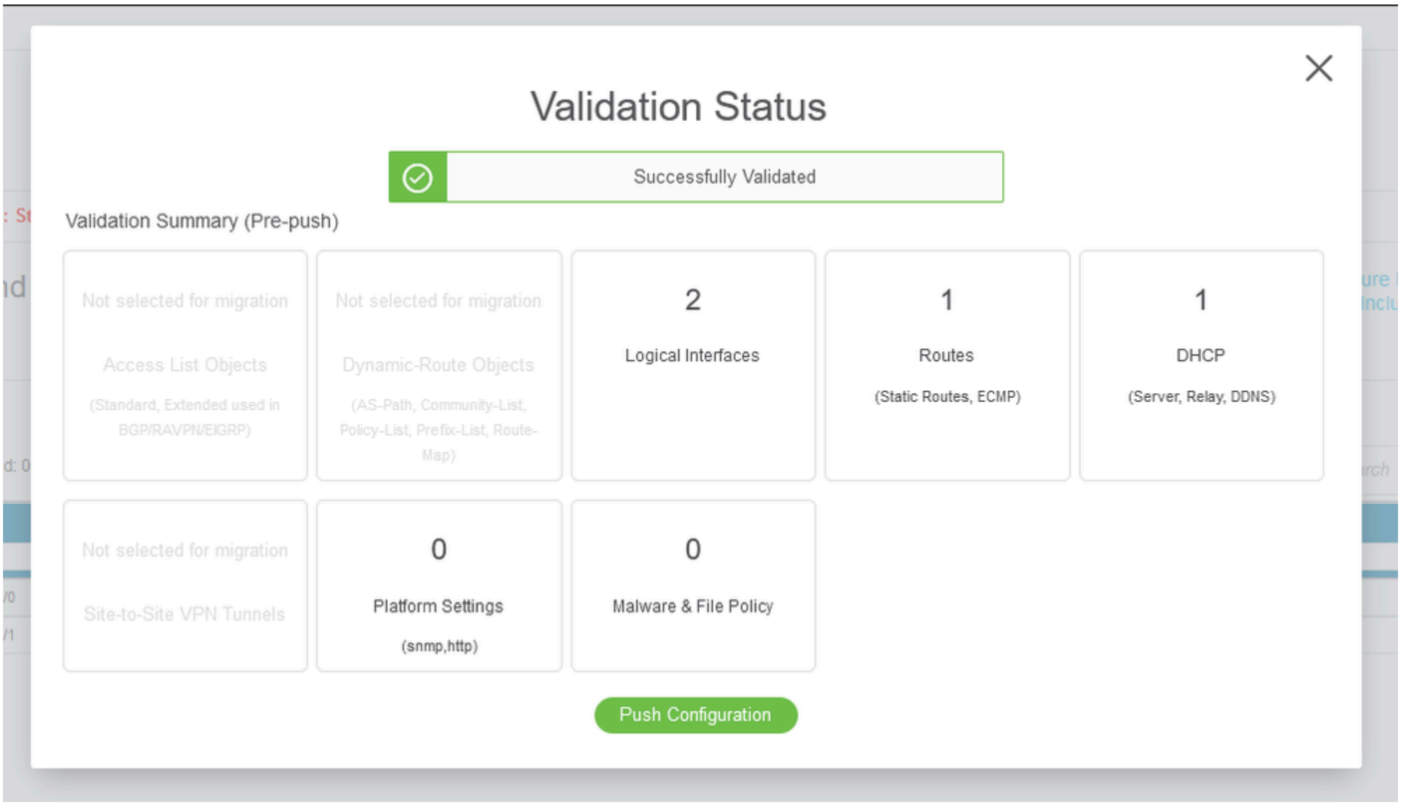
□ Select all 2 entries   Selected: 0 / 2

■	#	Interface	Zone	IP Address	State
□	1	GigabitEthernet0/0	outside_zone	[redacted]	Enabled
□	2	GigabitEthernet0/1	inside_zone	[redacted]45.1	Enabled

r page 1 to 2 of 2 |◂ ◂ Page 1 of 1 ▸ ▸|

驗證FDM組態設定

驗證後，選擇Push Configuration以啟動配置推送過程，該過程將一直持續到遷移結束。此外，還可以監視正在執行的任務。



Validation Status

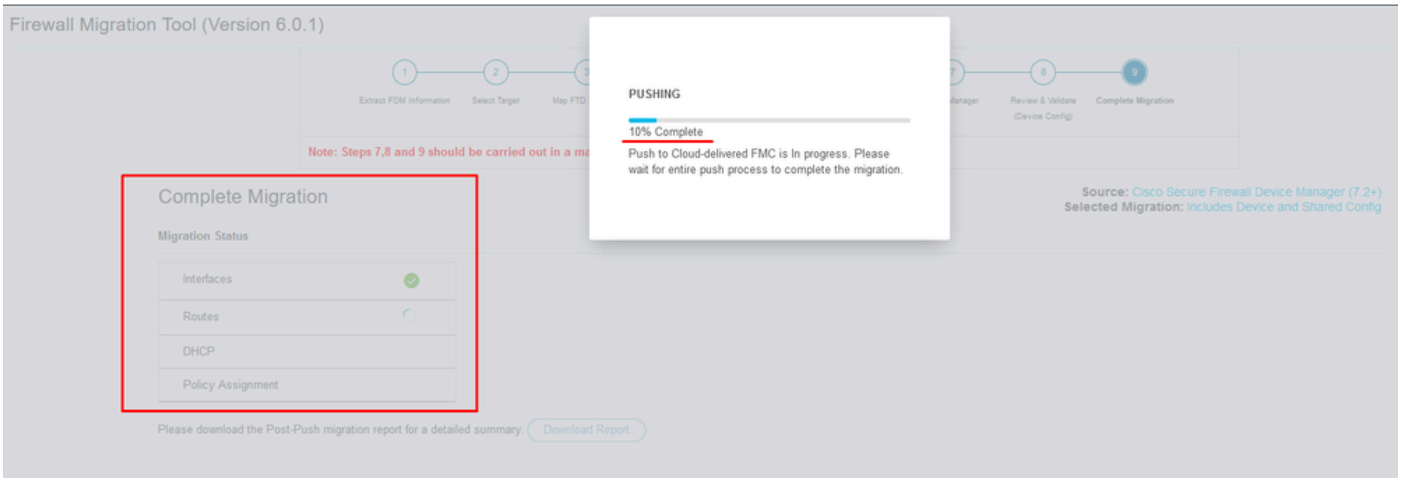
✓ Successfully Validated

Validation Summary (Pre-push)

Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	2 Logical Interfaces	1 Routes (Static Routes, ECMP)	1 DHCP (Server, Relay, DDNS)
Not selected for migration Site-to-Site VPN Tunnels	0 Platform Settings (snmp,http)	0 Malware & File Policy		

驗證狀態-推送配置。

具有百分比推入配置的彈出窗口。



Firewall Migration Tool (Version 6.0.1)

PUSHING

10% Complete

Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.

Note: Steps 7,8 and 9 should be carried out in a ma

Complete Migration

Migration Status

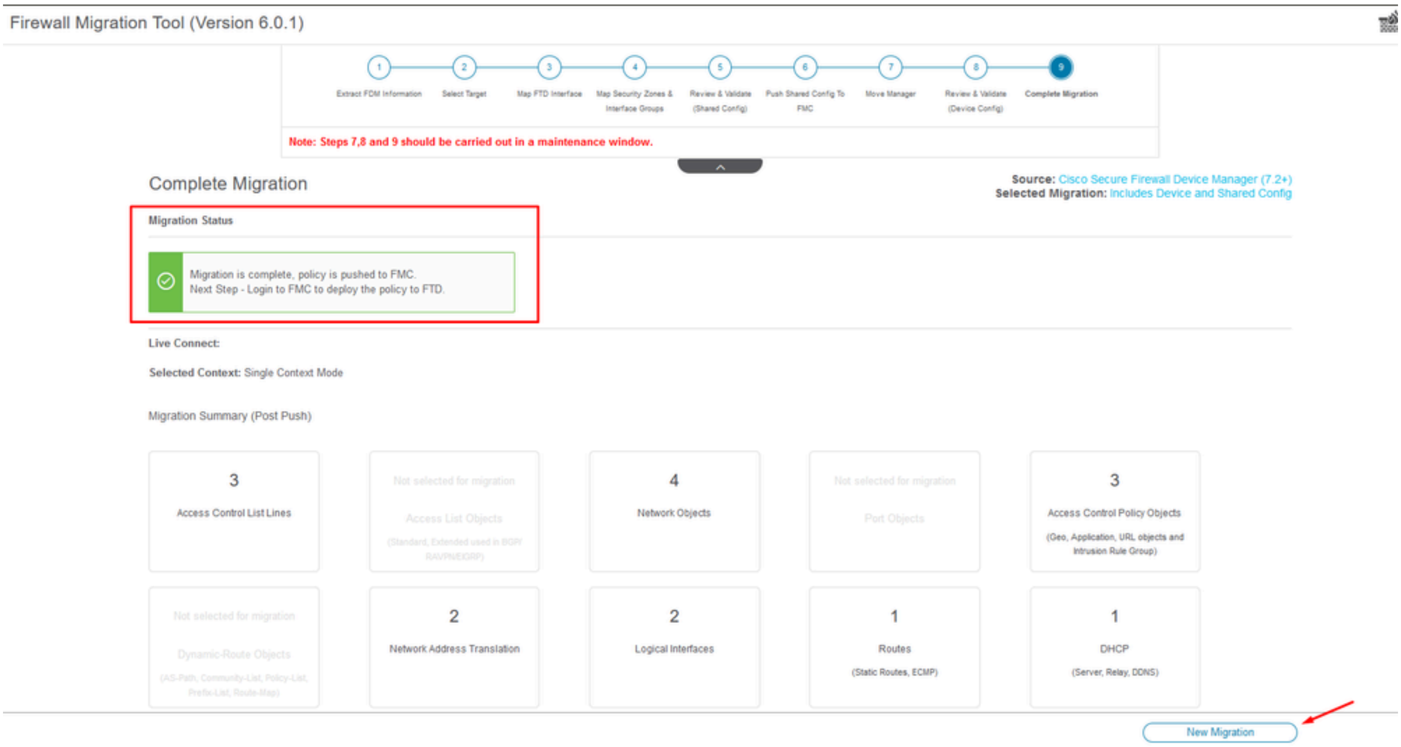
- Interfaces ✓
- Routes
- DHCP
- Policy Assignment

Please download the Post-Push migration report for a detailed summary.

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

推送完成百分比

完成時，會顯示啟動新移轉的選項，標示從FDM到cdFMC的移轉程式結束。



Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a maintenance window.

Complete Migration

Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

Migration Status

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

3 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/ RAVPN/EIGRP)	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Not selected for migration Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	2 Network Address Translation	2 Logical Interfaces	1 Routes (Static Routes, ECMP)	1 DHCP (Server, Relay, DDNS)

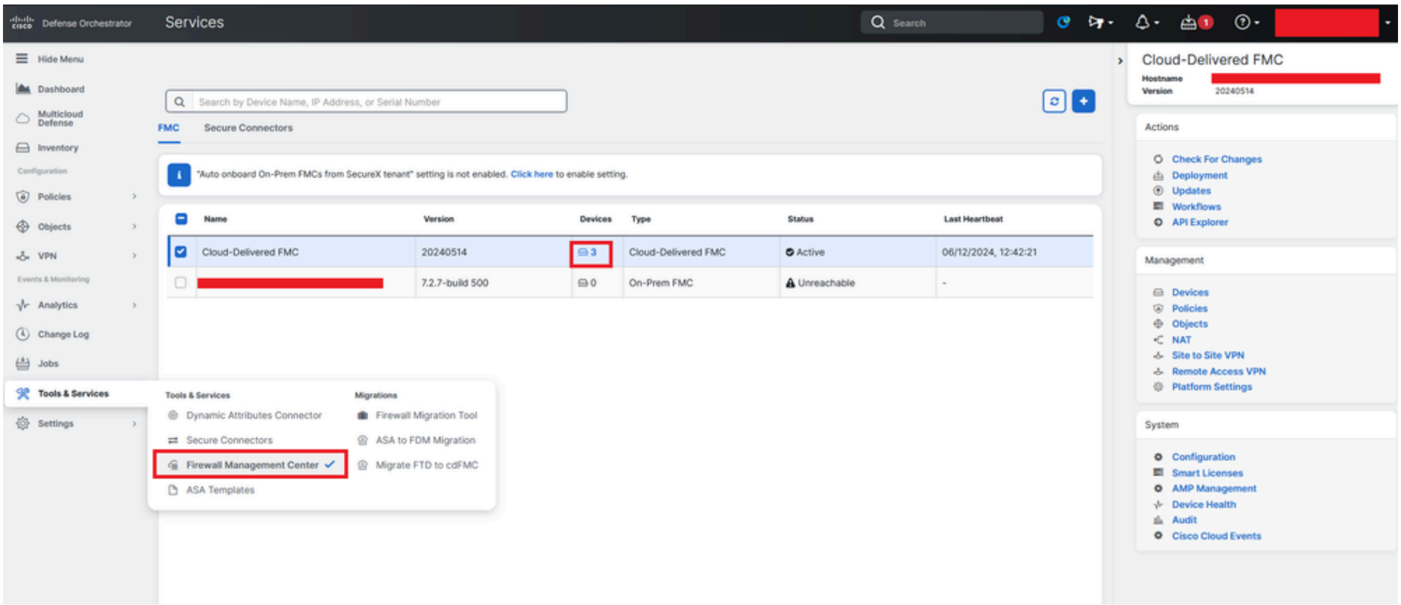
1
Extract FDM Information
2
Select Target
3
Map FTD Interface
4
Map Security Zones & Interface Groups
5
Review & Validate (Shared Config)
6
Push Shared Config To FMC
7
Move Manager
8
Review & Validate (Device Config)
9
Complete Migration
New Migration

完成移轉

驗證

確認FDM已成功移轉至cdFMC。

導航到CDO > Tools & Services > Firepower Management Center。您會發現註冊裝置的數量增加了。



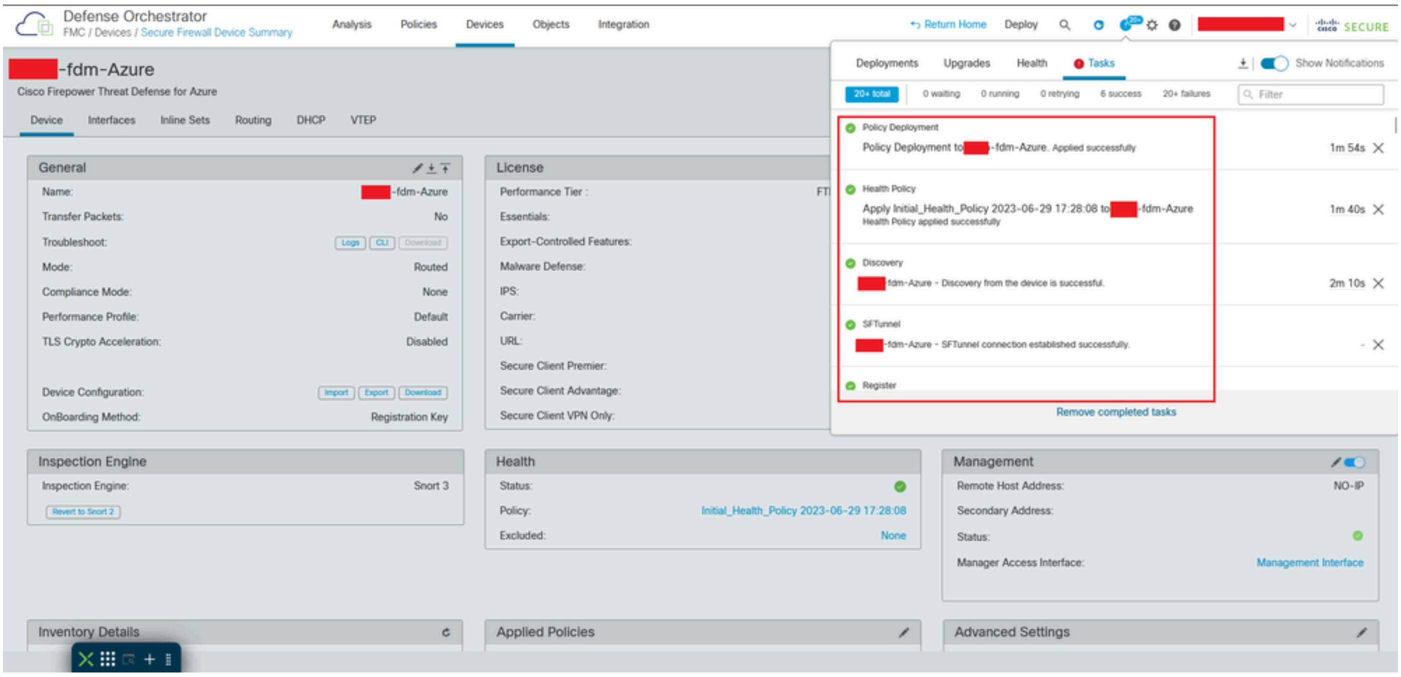
"Auto onboard On-Prem FMCs from SecureX tenant" setting is not enabled. Click here to enable setting.

Name	Version	Devices	Type	Status	Last Heartbeat
Cloud-Delivered FMC	20240514	3	Cloud-Delivered FMC	Active	06/12/2024, 12:42:21
[redacted]	7.2.7-build 500	0	On-Prem FMC	Unreachable	-

Cloud-Delivered FMC
Hostname [redacted]
Version 20240514

cdFMC註冊裝置

在Devices > Device Management中檢查裝置。此外，在FMC的任務中，您可以找到裝置成功註冊和首次部署成功完成的時間。



[redacted]-fdm-Azure
Cisco Firepower Threat Defense for Azure

General
Name: [redacted]-fdm-Azure
Transfer Packets: No
Mode: Routed
Compliance Mode: None
Performance Profile: Default
TLS Crypto Acceleration: Disabled
OnBoarding Method: Registration Key

Inspection Engine
Inspection Engine: Snort 3

Health
Policy: Initial_Health_Policy 2023-06-29 17:28:08
Excluded: None

Management
Remote Host Address: NO-IP

Tasks: 20+ total, 0 waiting, 0 running, 0 retrying, 6 success, 20+ failures

Policy Deployment
Policy Deployment to [redacted]-fdm-Azure. Applied successfully — 1m 54s

Health Policy
Apply Initial_Health_Policy 2023-06-29 17:28:08 to [redacted]-fdm-Azure
Health Policy applied successfully — 1m 40s

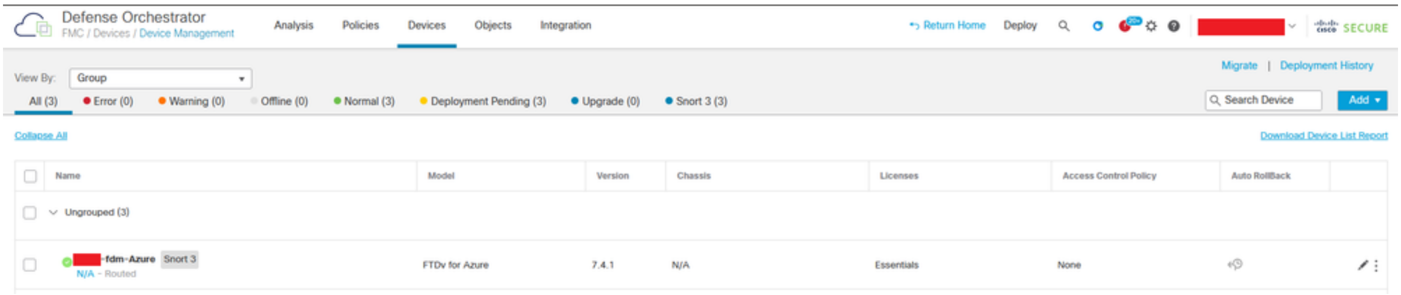
Discovery
[redacted]-fdm-Azure - Discovery from the device is successful. — 2m 10s

SFTunnel
[redacted]-fdm-Azure - SFTunnel connection established successfully. — -

Register

cdFMC註冊任務已完成。

裝置位於cdFMC > Device > Device Management中。

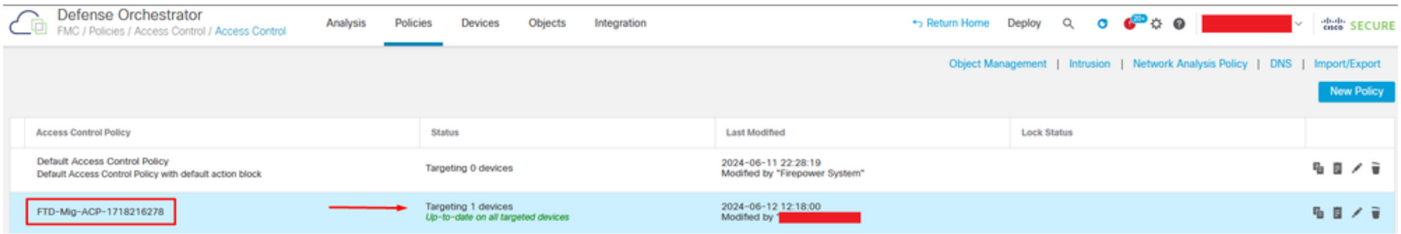


View By: Group
All (3) Error (0) Warning (0) Offline (0) Normal (3) Deployment Pending (3) Upgrade (0) Snort 3 (3)

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (3)						
[redacted]-fdm-Azure Snort 3 N/A - Routed	FTDv for Azure	7.4.1	N/A	Essentials	None	

在cdFMC上註冊的裝置

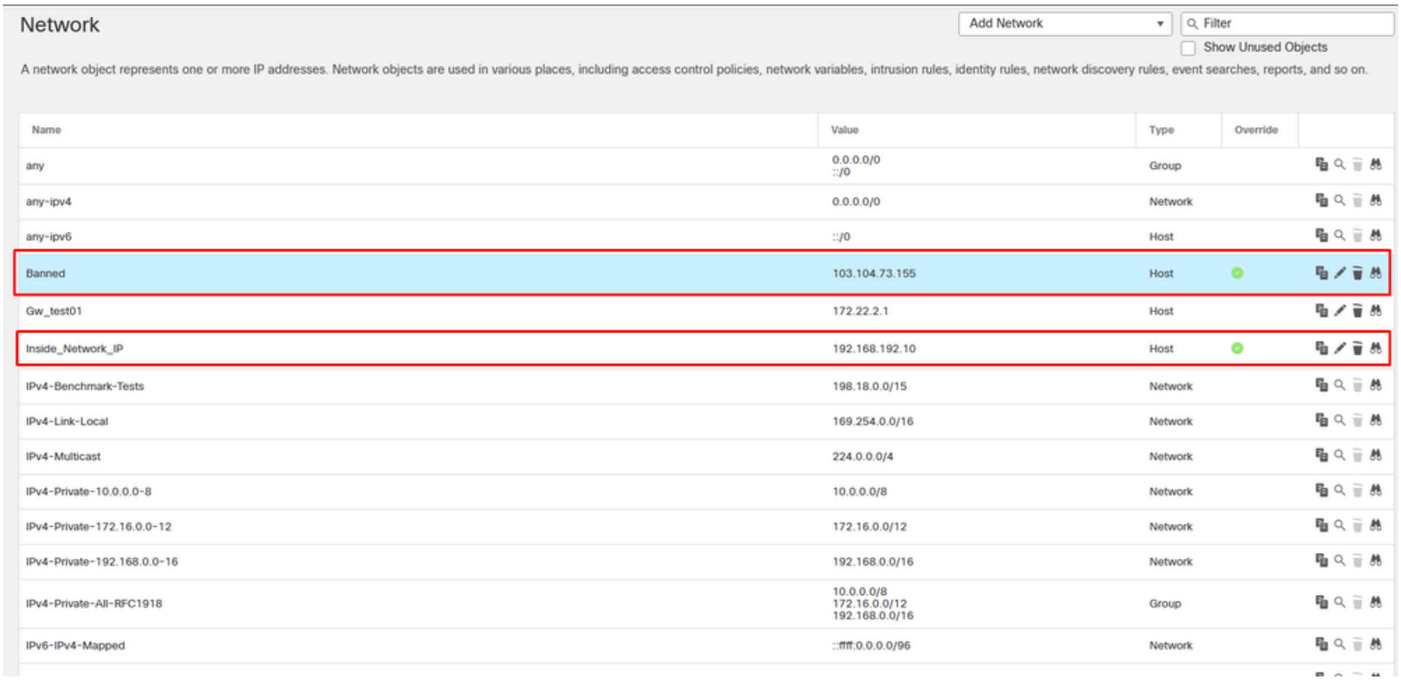
訪問控制策略在策略>訪問控制下遷移。


Defense Orchestrator
FMC / Policies / Access Control / Access Control
Analysis
Policies
Devices
Objects
Integration
Return Home
Deploy
[redacted]
SECURE
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
New Policy

Access Control Policy	Status	Last Modified	Lock Status
Default Access Control Policy Default Access Control Policy with default action block	Targeting 0 devices	2024-06-11 22:28:19 Modified by "Firepower System"	
FTD-Mig-ACP-1718216278	Targeting 1 devices *Up-to-date on all targeted devices*	2024-06-12 12:18:00 Modified by [redacted]	

遷移策略

同樣地，您可以檢視在FDM中建立的物件，這些物件已正確移轉至cdFMC。

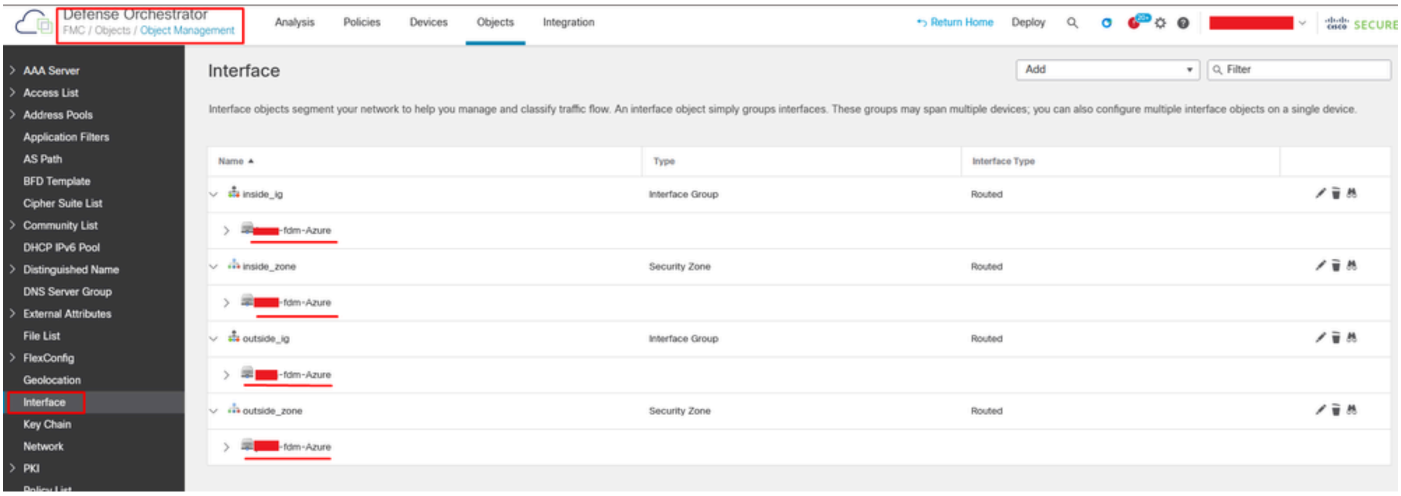

Network

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Value	Type	Override
any	0.0.0.0/0 ::/0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	::/0	Host	
Banned	103.104.73.155	Host	●
Gw_test01	172.22.2.1	Host	
Inside_Network_IP	192.168.192.10	Host	●
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	::ffff:0.0.0.0/96	Network	

從FDM移轉至cdFMC的物件

已遷移對象管理介面。



Interface

Interface objects segment your network to help you manage and classify traffic flow. An interface object simply groups interfaces. These groups may span multiple devices; you can also configure multiple interface objects on a single device.

Name ▲	Type	Interface Type
inside_ig	Interface Group	Routed
[redacted]-fdm-Azure		
inside_zone	Security Zone	Routed
[redacted]-fdm-Azure		
outside_ig	Interface Group	Routed
[redacted]-fdm-Azure		
outside_zone	Security Zone	Routed
[redacted]-fdm-Azure		

已遷移對象管理介面。

關於此翻譯