# 在CDO中使用FMT將FDM移轉至cdFMC

目錄	
<u>簡介</u>	
<u>必要條件</u>	
<u>需求</u>	
<u>採用元件</u>	
<u>背景資訊</u>	
<u>設定</u>	
<u>驗證</u>	

## 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。

Monitoring Policies Objects	vice	> 🖨 @ ?	admin Administrator
Model Cisco Firepower Threat De	Software VDB Intrusion Rul fense for Azure 7.4.1-172 376.0 20231011-1	e Update Cloud Services High Availat 536 Connected   SEC TAC Not Configu	CONFIGURE
Fig. Inside Ne	Vvork Cisco Firepower Threat Defense for Azure () 0/0 0/1 () 0/0	MGMT CONSOLE ISP/WAN/Gateway	DNS Server DNS Server NTP Server
Interfaces	Routing	Updates	System Settings
Management: Unmerged Enabled 2 of 2	1 static route	Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds	Management Access Logging Settings
View All Interfaces	View Configuration	View Configuration > s	DHCP Server / Rola) SL Settings Ioud Service
Smart License Registered Tier: FTDv20 - 3 Gbps	Backup and Restore	Troubleshoot No files created yet	TTP Proxy Service eboot/Shutdown tinterface entral Management RL Filtering Preferences
View Configuration >	View Configuration	REQUEST FILE TO BE CREATED	See more
Site-to-Site VPN There are no connections yet	Remote Access VPN Requires Secure Client License No connections   1 Group Policy	Advanced Configuration Includes: FlexConfig, Smart CLI	Device Administration Audit Events, Deployment History, Download Configuration
View Configuration	Configure >	View Configuration	View Configuration

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。

Firewall Device Manager	版 砂 苹王 Monitoring Policies Objects Device	S (a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
System Settings +- Management Access Logging Settings	Device Summary Cloud Services Not Registered	
DHCP DDNS Service DNS Server Management Interface	You can register the device with the Clisco cloud to use additional cloud-based services. If you want to use Clisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other searchy account registration itsy, you can alternatively auto-enroll with CDO or a Secure Firewall Management Clearer using the device serial number, if you want to secure service and the classical security account are ready to licements the device, then cooling the security and the security account provide the device with the Clicco cloud. After you register with the cloud, you can enable or disable features an ededd.	
Hostname Time Services SSL Settings	Enrollment Type Security/CDO Account Smart Licensing Region	
HTTP Proxy	US Region 🗸 🖉	
Reboot/Shutdown Remote Management	Registration Key Enter Registration Key	
Cloud Services Central Management	Service Enrolment     Cisco Defense Orchestrator     Cisco Defense Orchestrator     Cisco Defense Orchestrator is a cloud-based management tool used for managing network	
Traffic Settings	devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.	
	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 our the Sample Data that will be sent to Cisco. See more > profile Enrol Cisco Success Network Need help?(5)	

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。

cisco Defense Orchestrator	Inventory	Q Search	ଓ ୨୫- ୦୦- ଲା ଓ	)· ·
Hide Menu	Devices Templates     Q. Search by Device Name, IP Address, or Serial Number	Displaying 8 of 8 results		<b>C</b> ()
Dashboard     Multicloud	All ASA FTD			
Defense     Inventory	Name ©	Configuration Status 🗘	Connectivity \$	

內建FDM,新增選項

出現一個選單,用於選擇裝置或服務型別。



選擇裝置或服務型別

#### 對於此文檔,已選擇「選擇註冊金鑰」。



### 此處,它顯示上一步所需的註冊金鑰。

FTD SOOD TO THE SOUTH STATES	A 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. (FTD 6.7+, 1000, 2100 and 3100 series only)
1 Device Name	
2 Database Updates	Enabled
3 Create Registration Key	7a53c
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  for 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。

Monitoring	Policies	:::: Objects	Device: joroa-fdm-tech
Device Summa Cloud Se Not Reg	rvices istered		
You can registe use Cisco Defe register with the auto-enroll with want to use Se configure Smar register with the	r the device w nse Orchestra e cloud using n CDO or a Se cure Firewall ( t Licensing, w e cloud, you c	with the Cisco clo ator (CDO) for ma your CDO or oth ocure Firewall Ma device manager which automatica an enable or dis	bud to use additional cloud-based services. If you want to anagement or want to remain in evaluation mode, then her security account registration key. You can alternatively anagement Center using the device serial number. If you for management and are ready to license the device, then lly registers the device with the Cisco cloud. After you able features as needed.
Enrollment Type	e Account	Smort Licensing	
Region US Region Registration Ke 7a53c2t	y		~ ()
Service En	rollment		
Cisco D	efense Orc	hestrator	
Cisco Defe devices. S account.	ense Orchestr elect this opti	ator is a cloud-b on if you want to	pased management tool used for managing network o register the device in your Cisco Defense Orchestrator
🔽 Enable	e Cisco Defen	se Orchestrator	
Cisco Si	iccess Net	work	
Cisco Suc essential f product ar of the prod	cess Network or Cisco to pr d to make you duct in your ne	enablement pro ovide technical s u aware of unuse atwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ed available features so that you can maximize the value
Cisco Suci essential fo product ar of the prod Check out	cess Network or Cisco to pr d to make you luct in your ne the <u>Sample</u> D	enablement pro ovide technical s u aware of unuse atwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ed available features so that you can maximize the value sent to Cisco. See.more V
Cisco Suci essential fi product ar of the proo Check out	cess Network or Cisco to pri id to make you duct in your ne the <u>Sample</u> D Cisco Succes	enablement pro ovide technical s u aware of unuse atwork. Data that will be s ss Network	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ed available features so that you can maximize the value sent to Cisco. See.more >

FDM註冊

註冊FDM時,它會顯示「租戶」、「已連線的雲服務」和「已註冊」。

Monitoring Policies Objects Device:	()_ (interpretation of the second sec
Device Summary         Cloud Services         Connected       Enrollment Type: Security/CDO Account       Tenancy:         Registered	<b>0</b>
Cisco Defense Orchestrator DISABLE	Cisco Success Network DISABLE
Note: If the device is registered to cloud services using Smart Licensing, the device will not work with CDO. Rease <u>unregister</u> the device and re-on-board using the registration key method with the "Security/CDO account" option.  Cisco Defense Orchestrator (2 allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your 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 <u>Sample Data</u> that will be sent to Cisco.
Send Events to the Cisco Cloud	
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 (2, 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」。

shalls Defense Orchestrator	Inventory		Q Search C by -	¢®• ≝1 ⑦•
⊟ Hide Menu				3
Dashboard	T Devices Templates Q Search by Device Name, IP Address, or Serial Number	Displa	aying 9 of 9 results	FDM Device Details
Multicloud Defense	All ASA FTD			Model Cisco Firepower Threat Defense for
inventory	Name 0	Configuration Status \$	Connectivity 0	Azure Serial
Configuration	O ASA	-	A Unreachable	Version 7.4.1-172 Onboarding Registration Key Method
⊕ Objects →	D FOM		O Serial Number Mismatch	Snort Version 3.1.53.100-56
-& VPN >	O 110	Ø Not Synced	Pending Setup	Syncing CDO is communicating with your device. Please check back in a moment.
√r Analytics →	O FED		Pending Setup	Device Actions
<ul> <li>Change Log</li> <li>dia Jobs</li> </ul>	О гто		Pending Setup	API Tool     Workflows     Manage Backups
	C FOM	Syncing	Online	Remove Management
ημ oerungs /			Online	Notes
	O FTD		Online	Lecutive Report
	O FTD	Not Synced	A Unreachable	Conflict Detection     Oisabled      Check every:     Tenant default (24 hours) =
				Label Groups and Labels
				Add Labels 0

已登入CDO清查FDM

裝置同步後,將顯示為「聯機」和「已同步」。

FDM Online
------------

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。

🛠 Tools & Services		Tools & Services	Migrations		
{ُنُ} Settings	>	Oynamic Attributes Connector	Firewall Migration Tool		
•		⇒ Secure Connectors	會 ASA to FDM Migration		
		🖨 Firewall Management Center	备 Migrate FTD to cdFMC		
		ASA Templates			

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。

$\fbox{\begin{tabular}{ c c } \hline \hline $Q_i$ & Search for a migration by name \\ \hline \end{tabular}$		Displaying 0 of 0 results			I C 💽
Name 2	Status	Created Date (2	Deprevisioning Date 0	Actions	/
		o 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。

	C Sea
Initialize Migration	×
To initialize the migration process, name this migration and click OK. Cl notify you when the migration tool is ready for use. When ready, select migration and launch the tool.	)O will this named
Name *	
.fdm_migration	
O This is an auto-generated name. You can change it if you wish.	
Can	celOK

初始化移轉

按一下Launch開始遷移配置。

Firewall Migration Tool			Q Search 🕐 🏹 -	¢7· ±1 0·	•
Q         Search for a migration by name		Displaying 1 of 1 results			i C +
Name ©	Status	Created Date 0	Deprovisioning Date 0	Actions	
fdm_migration	<ul> <li>Ready to Migrate</li> </ul>	Jun 12, 2024	Jun 19, 2024	C' 🚖 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)。

C	lick 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)	$\sim$
	<ul> <li>This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.</li> </ul>	
	<ul> <li>The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.</li> </ul>	
	<ul> <li>Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.</li> </ul>	
	<ul> <li>User should provide FDM credentials to fetch details.</li> </ul>	
	<ul> <li>FDM Devices enrolled with the cloud management will lose access upon registration with FMC</li> </ul>	
	<ul> <li>Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.</li> </ul>	
	<ul> <li>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.</li> </ul>	
	<ul> <li>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.</li> </ul>	
	<ul> <li>FDM with Universal PLR cannot be moved from FDM to FMC.</li> </ul>	
	• 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.	

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.						
<ul> <li>Only devices with online connectivity and synced status will be displayed in the dropdown.</li> </ul>						
<ul> <li>Click on change device status button to update the FDM device status from In-Use to Available.</li> <li>Select FDM Managed Device</li> </ul>						
Select FDM Managed Device						
fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_						
Connect						

FDM裝置選擇



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。



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	
	Save Cancel	, 1
-		

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	-2-	3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 shou	d be carried o	out in a maintena	nce window.						
Select Target 🕡					^			Science	ource: Cisco Secure I cted Migration: Inclu	Firewall Device Manager (7.2+) des Device and Shared Config
Firewall Management -	Cloud-delivered FMC									>
Select Features										~
Device Configuration		SI	nared Configura	ation			1	Optimization		
✓ Interfaces		~	Access Control					✓ Migrate Only Re	eferenced Objects	
Routes			🧹 Migrate tunn	elled rules as Pref	ilter			Object Group S	earch 🕠	
ECMP			NAT							
Static		~	Network Objects							
BGP			Port Objects(no	data)						
EIGRP			Access List Obj	ects(Standard, Ext	ended)					
Site-to-Site VPN Tunn	els (no data)		Access Control I	Policy Objects (Ge	olocation, Applic	ation, URL objects a	nd Intrusion Rul	e		
Policy Based (Cr	(pto Map)		- Group) Time based Obi	ects (no data)						
Route Based (V7	7)		Remote Access	VPN						
Platform Settings			File and Malware	Policy						
- DHCP				1 0.009						
Server										
Relay										
DDNS										
Proceed	-									
Note:Platform settings an	d file and malware policy migra	tion is supporte	d in FMC 7.4 and I	ater versions.						

要選取的特徵

### 然後開始轉換。

	Extract FDM Information	2 Select Target Ma	3 ap FTD Interface M	4 lap Security Zones & Interface Groups	5 Review & Validate (Shared Config)	6 Push Shared Config To FMC	7 Nove Manager	8 Review & Validate (Device Config)	9 Complete Migration	
	Note: Steps 7,8 and 9 should	be carried out in	a maintenance	e window.						
Select Target 0				,				Selec	ource: Cisco Secure Firewa sted Migration: Includes D	all Device Manager (7.2+ Device and Shared Confi
Firewall Management - O	loud-delivered FMC									>
Select Features										>
Rule Conversion/ Proce	s Config									~
Start Conversion										

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。



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。

Note: Steps 7,8 and 9 should be carried out in a maintenance window.
Map FTD Interface
FDD Interface Name       OgabEEthernetD0     OgabEEthernetD0       OgabEEthernetD1     OgabEEthernetD1
OgabEthernet50 OgabEthernet51 OgabEthernet51
GgabEEhernet0/1 GgabEEhernet0/1

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。

#### Firewall Migration Tool (Version 6.0.1)

	1 Extract FDM Information	2 Select Target Map FTD In	terface 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	ld be carried out in a mai	ntenance window.						
Map Security Zone	es and Interface Grou	ibe 🛈			Add	SZ & IG	nto-Create	Source: Cisco Secure Fir Selected Option: Include	ewall Device Manager (7.2+) is Device and Shared Config
FDM Logical Interface	FDM Security Zone	es FTD Interf	ace	FMC Security Zo	nes	FMC Interface Gro	oups		
outside	outside_zone	GigabitEthernet	0/0 eu	tside_zone (A)	Se	elect Interface Groups	v		
inside	inside_zone	GigabitEthernet	0/1 ins	ide_zone (A)	Se	elect Interface Groups	×		
Note: Pick on Auto Consta			~	cuitu acos Cita	k oo aad kulloo la				

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。

	(Add 52 d 10)	Charot
FTD		Group
Gigabiti	Auto-Create	ups
Gigabiti	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 Cancel Auto-Create	ups

自動建立選項。

然後選擇Next。

Firewall Migration	n Tool (Version 6.0	.1)					
		1 2 Extract FDM Information Select T	3 (1) and the security Zinterface and the security Zinterf	5 6 ones & Review & Validate Push Shared O ups (Shared Config) FMC	7 8 Config To Move Manager Review & Vali (Device Con	9 fate Complete Migration	
		Note: Steps 7,8 and 9 should be car	ried out in a maintenance window.				
	Map Security Zone	es and Interface Groups 🕕		<u>^</u>		Source: Cisco Secure Firewai Selected Option: Includes De	I Device Manager (7.2+) evice and Shared Config
				(	Add SZ & IG Auto-Create	)	
	FDM Logical Interface I	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 b	vutton to auto map the FDM nameif as th	e name of the FMC interface objects a	nd security zones. Click on next b	utton to proceed ahead.		
	10 v Pet/JPB98 2 4	< Page 1 of 1 ▶ ▶					Back Next

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	n Tool	(Versic	on 6.0.1)			
			1 2 Extract FDM information Select Target	3 4 5 Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Barred Contig)	6 7 8 Push Shared Config To Move Manager (Device Config) FMC (Device Config)	9 Complete Migration
			Note: Steps 7,8 and 9 should be carried of	ut in a maintenance window.		
	Opti	mize, F	Review and Validate Shared Con	figuration Only 💿	)	Source: Cisco Secure Firewall Device Manager (7.24
	Access	Control	Objects NAT Interfaces Routes Site-to-5	ite VPN Tunnels 🚯 Remote Access VPN SN	MP DHCP	rected migration, includes period and shared conin
	_					
	Acc	ess List Obj	tries Selected: 0 / 3	Introl Policy Objects VPN Objects Dynamic-Route	e Objects	O Samb
			North Selected VIS	Mellideden finne	Tree	C Search *
		1	Q.	Q.	Q.	
		1	Outside/Pv4Gateway	Validation pending	Network Object	172.18.1.1
		2	Outside/Pv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
		3	Banned	Validation pending	Network Object	103.104.73.155
rpage 1 to3 of3 [∢ ∢	Page	1 of 1	► ►]			Validate

訪問控制、對象和NAT配置

### 然後僅推送共用配置

	$\oslash$	Successfully Validat	ed	
lation Summary (Pre-pu	ush)			
3		4		3
ccess Control List Lines		Network Objects		Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2	Not selected for migration			
Network Address Translation				
Tanoladon				

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 Migrati	on Tool (Version 6.0.1)				
	Push Shared Config to I	FMC		DICHING	Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Migration Status			24% Complete	
	Network Objects	0		Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.	
	Network Address Translation	0			
	Access Control Policies	0			
	Policy Assignment				
	Please download the Post-Push migratio	n report for a detailed s	summary. Download		

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。

	1 Extract FDM Informati	2 3	4 5 Interface Map Security Zones & Review & Validate Interface Groups (Shared Confg)	6 7 8 h Shared Config To FIMC (Device Config (Device Config	9 are Complete Mgration 2)
	Note: Steps 7,8 and 9 sh	ould be carried out in a ma	intenance window.		
Push Shared Co	nfig to FMC				Source: Cisco Secure Firewall Device Manag
Migration Status					serected migration. Includes before and onder
Live Connect: Selected Context: Single Migration Summary (Post	Context Mode Push)		4		3
Live Connect: Selected Context: Single Migration Summary (Post	Context Mode Push) Not s		4 Network Objects		3 Access Control Policy Objects
Live Connect: Selected Context: Single Migration Summary (Post Access Control List Lin	Context Mode Push) es A Cland		4 Network Objects		3 Access Control Policy Objects (Geo, Appleation, URL objects and Intrusion Rule Oroup)
Live Connect: Selected Context: Single Migration Summary (Post Access Control List Lin Not selected for migra	Context Mode Push) RS Column	selected for migration locenss List Objects and, Ditended used in BOPY RAVITMEDRAY	4 Network Objects Not selected for migration		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group) Not selected for migration
Live Connect: Selected Context: Single Migration Summary (Post Access Control List Lin Not selected for migra Dynamic-Roote Obje	Context Mode Push) Ps A CStand ts Not	selected for migration access List Objects Isnt, Objects RAVINECORY 2 vork Address Translation	4 Network Objects Not selected for migration Logical Interfaces		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group) Not selected for migration DHCP

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.





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	0.1)									
	1			-(5)		•	8	9		
	Extract FDM Information	Select Target Map FTD Inte	rface Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration		
	Note: Steps 7,8 and 9 should	I be carried out in a main	tenance window.		_					
Move Manager				^			Selec	ource: Cisco Se ted Migration:	cure Firewall Device Includes Device and	Manager (7.2+) Shared Config
Update Deta	ils	a downtime window. Af	ter you register the de	avice with the m	anagement center	or Cloud-delive	ered FMC. vou ca	an no longer use	the device manager	r to manage it.
Management Cent	Management Cente (	NAT ID	Threat D	efense Hostn	DNS Serve	r Group	Managemen	nt Center/	Data Interface	
cisco cdi	»		1	Lcloud	app.n CiscoUmbrellaDN	SServerGroup ~	💿 Data 🔵 Ma	anagement	Select Data Interface	×

#### 管理員中心ID和NAT ID

-irewall Migration Tool (Version 6.	0.1)			×		
	1 Extract FDM Information Set	2 lect Target	Update Device Name for F	8 9 Review & Validate Complete Migration (Device Config)		
	Note: Steps 7,8 and 9 should be	carried	-fdm-			
Move Manager					Source: Cisco Se	
ino to managor			Cancel Save		Selected Migration:	
Update De This step is mandatory a	nis nd should be performed during a c	downtime	Cancel Save		d FMC, you can no longer use	a the device manager to manage it.
Update De This step is mandatory a Management Cont	nits nd should be performed during a c Management Cente •	downtime NAT ID 💿	Cancel Save	DNS Server Group	d FMC, you can no longer use Management Center/	the device manager to manage it.
Update De This step is mandatory a Management Cent Cisco-trex-refer-dac.sprint.co	Management Cente	downtime NAT ID ①	Cancel Save Threat Defense Hostn prea-film-techzone internal cloudago.n	DNS Server Group	d FMC, you can no longer use Management Center/	the device manager to manage it. Data Interface 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 Migratio	n Tool (Version 6.0	.1)						
		1 Extract FDM Information	2 3 Gelect Target Map FTD Interface	4 5 Map Security Zones & Review & Interface Groups (Shared	Valdate Push Shared Config To Config) FMC	7 Move Manager R	8 9 Iaview & Validate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should b	e carried out in a maintena	nce window.				
	Move Manager						Source: Cisco See Selected Migration:	ture Firewall Device Manager (7.2+) Includes Device and Shared Config
	Update Deta	ils						
	This step is mandatory an	d should be performed during a	downtime window. After y	ou 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	Inreat Defense n	ostn Dws Server	Group	Management Center/	Data Interface
	cisco us.cdo	ogu 1660	W 104V	3sPMI fdm-Azure	CiscoUmbrellaDNS	iServerGroup 🗸 🤇	Data Management	Select Data Interface v
		L					$\sim$	/
								Sare

Move Manager

#### 管理中心ID和NAT ID。

### 選擇Update Details 選項後,裝置將開始同步。

on Tool (Versi	ion 6.0.1)										
	Extract P	1 2 DM Information Select Targ	3 et Map FTD Interface	4 Map Security Zones & Interface Groups	S Review & Validate (Shared Config)	B Push Shared Config To FMC	() Move Manager	8 Review & Validate (Device Config)	9 Complete Migration		
	Note: Steps 7,8	and 9 should be carri	ed out in a maintena	ance window.							
Move Man	nager							Sou	irce: Cisco Se ed Migration:		
Up This stop is man	pdate Details	rmod during a doum	time window	SYN	CING the FDM D	evice	rd dolino	red EMC you can		the device manager	to manago it
Up This step is man Management	pdate Details Indatory and should be perf t Cent Managemen	ormed during a down ht Cente I N/	time window. AT ID 💿	SYN	CING the FDM D 9% Complete	evice	ıd-delive	red FMC, you can Management	no longer use Center/	e the device manager Data Interface	to manage it.
Up This step is man Management cisco	pdate Details Indatory and should be perfit t Cent Management us.cdo joguq	ormed during a down at Cente ① N/ IBEGW 104	time window. AT ID 💿	SYN	CING the FDM D 9% Complete	evice CiscoUmbrellaDNS	i <b>d-delive</b> ServerGroup ~	Management	n no longer use Center/ agement	e the device manager Data Interface Select Data Interface	to manage it.

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。

ewall Migration Too	ol (Versio	on 6.0.1)				
		Detract FDM Information Select Target	3 4 5 Map FTD Interface Map Security Zones & Review & Va Interface Oroups (Shared Co	6 7 Idate Push Shared Config To Move Manager Review J Ifg) FMC (Device	9 Validate Complete Migration Config)	
		Note: Steps 7,8 and 9 should be carrie	d out in a maintenance window.			
Opti	imize, R	Review and Validate Device Co	nfiguration Page 0		Source: Cisco Secure Firewall Devic Selected Migration: Includes Device a	e Manager (7.2+ nd Shared Confi
		Objects NAT Interfaces Routes Site-t	o-Site VPN Tunnels 🔵 Remote Access VPN	SNMP DHCP	-	
Sta	atic PPPoE	E)				
S	elect all 2 ent	tries Selected: 0 / 2			Q Search	+
•		Interface Q	Zone Q	IP Address Q	State	
	1	GigabitEthernet0/0	outside_zone		Enabled	
0	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
1 to 2 of 2  ∢ ∢ Page [	1_ of 1_1	► H			Validate	

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。

	$\odot$	Successfully Validated		
alidation Summary (Pre-pu	ish)			
		2	1	1
		Logical Interfaces	Routes	DHCP
			(Static Routes, ECMP)	(Server, Relay, DDNS)
	0	0		
	Platform Settings	Malware & File Policy		
	(snmp,http)			

驗證狀態-推送配置。

具有百分比推入配置的彈出窗口。

Firewall Migrati	on Tool (Version 6.	0.1)				
		Extract FDM Information Note: Steps 7,8 and 9 should I	2 3 Select Target Map FTD	PUSHING 10% Complete Push to Cloud-delivered FMC is In progress. Please wait for entire rush process to complete the micration	7)	O     Revers & Validate     Complete lifegration     (Device Config)
ſ	Complete Migra Migration Status	tion				Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Conlig
	Interfaces	0				
	Routes					
	Policy Assignment					
	Please download the Post-	Push migration report for a detailed	summary. Download R			

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。

	J.1)			
	1     2 Extract FDM Information Select Target	3 4 Map FTD Interface Map Security Zones & Review Interface Groups (Shared	5 6 7 6 Valdate Push Shared Config To Move Manager Rev I Config) PMC (De	Complete Migration vice Config:
	Note: Steps 7,8 and 9 should be carried	d out in a maintenance window.		
Complete Migra	tion	_		Source: Cisco Secure Firewall Device Manage Selected Migration: Includes Device and Shared
Migration Status				
Migration is comp Next Step - Login	lete, policy is pushed to FMC. to FMC to deploy the policy to FTD.			
Live Connect:				
Selected Context: Single	Context Mode			
Migration Summary (Pos	Push)			
3		ration 4		3
		Natural Objects		Annual Control Public Objects
Access Control List L	nes Access List Object	cts Network Objects		Access Control Policy Objects
Access Control List L	Access List Obje (Standard, Extended used RAVPINEIORP)	cts Network Objects		(Geo, Application, URL, objects and https://on.Rule.Group)
Access Control List L Not selected for migr	tion Access List Obje	In BOW	Post Objects	(Geo, Application, URL, objects and Infrusion Rule Group)
Access Control List L Not selected for migr Dynamic-Roote Obj	tion 2 Network Address Tran	slation Logical Interfaces	Port Objects 1 Routes	(Geo, Application, URL objects and Herbusion Rule Group)

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。

-11-11- CISCO	Defense Orchestrate	or	Serv	vices					Q Search		<b>ଓ</b> ⊳ <b>7</b> ∙	ł	۵- ط	1	•	-
≡	Hide Menu											>	Cloud-D	elivere	d FMC	
in.	Dashboard		Q	Search by Device Name, IP Addres	us, or Serial N	imber							Version	20240	0514	
0	Multicloud Defense		FMC	Secure Connectors									Actions			
	Inventory		-										O Cher	k For Cha	anges	
Con	Iguration		i	"Auto onboard On-Prem FMCs from S	ecureX tenant*	setting is not enabled. Click here to e	enable settin	g.					d Depl	oyment	inges	
۲	Policies	>											Upda     Work	tes flows		
¢	Objects	>		Name		Version	Devices	Туре	Status	Last Heartbeat	_		O APIE	xplorer		
-&-	VPN	>		Cloud-Delivered FMC		20240514	⊜3	Cloud-Delivered FMC	O Active	06/12/2024, 12:42:21			Manageme	nt		
Ever	ts & Monitoring					7.2.7-build 500	⊜0	On-Prem FMC	A Unreachable				🖨 Devi	ces		
st.	Analytics	>											<ul> <li>Polic</li> <li>Obje</li> </ul>	les cts		
٩	Change Log												C NAT			
(	Jobs												-> Site	o site VPI pte Acces	N IS VPN	
*	Tools & Services		Tools 8	& Services	Migrations								Platf	orm Settin	igs	
ø	Settings	>	6 0	Dynamic Attributes Connector	Firewall	Migration Tool							System			
			≓ s	Secure Connectors	ASA to F	DM Migration							O Conf	Iguration		
				SA Templates	22 migrate	TD to cormo							Smar O AMP	t Licenser Managen	is ment	
				terriphere a									+ Devi	ze Health		
													Cisc	D Cloud Ev	vents	

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。

Defense Orchestrator FMC / Devices / Secure Firewall Device Sum	mmary Analysis Policies De	vices Objects Integration	*> F	Return Home Deploy Q 💿 🍘 🗭	~ dudu SECURE
-fdm-Azure			Deployments	Upgrades Health OTasks	🛨   🌑 Show Notifications
Cisco Firepower Threat Defense for Azure			20+ total 0	waiting 0 running 0 retrying 6 success 20+ failures	Q, Filter
Device Interfaces Inline Sets Routin	Ig DHCP VTEP		Policy Deployme	ent	
		-	Policy Deploy	ment to -fdm-Azure. Applied successfully	1m 54s 🗙
General	∕±∓	License			
Name:	-fdm-Azure	Performance Tier :	FTI Health Policy		
Transfer Packets:	No	Essentials:	Apply Initial_H Health Policy ap	Health_Policy 2023-06-29 17:28:08 to fdm-Azure plied successfully	1m 40s ×
Troubleshoot:	Logs CLI Download	Export-Controlled Features:			
Mode:	Routed	Malware Defense:	<ul> <li>Discovery</li> </ul>		
Compliance Mode:	None	IPS:	fdm-Azur	e - Discovery from the device is successful.	2m 10s 🗙
Performance Profile:	Default	Carrier:	<ul> <li>SETional</li> </ul>		
TLS Crypto Acceleration:	Disabled	URL:	-1dm-Azur	e - SFTunnel connection established successfully.	- X
		Secure Client Premier:			
Device Configuration:	Import Export Download	Secure Client Advantage:	Register		
OnBoarding Method:	Registration Key	Secure Client VPN Only:	_	Remove completed tasks	
Inspection Engine		Health		Management	/ 🔍
Inspection Engine:	Snort 3	Status:	0	Remote Host Address:	NO-IP
Revent to Snort 2		Policy: Initial_Health_Policy 20	23-06-29 17:28:08	Secondary Address:	
		Excluded:	None	Status:	0
				Manager Access Interface:	Management Interface
Inventory Details	c	Applied Policies	1	Advanced Settings	/
X III 🖙 + 1					

cdFMC註冊任務已完成。

裝置位於cdFMC > Device > Device Management中。

Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices Objects	Integration		•> Return Home	Deploy Q	२ ॰ 🌮 🌣 🛛	~	disdo SECURE
View By: Group  All (3)  Error (0)  Warning (0)	Offline (0)	Normal (3)	Deployment Pendi	ing (3) • Upgrade (0)	<ul> <li>Snort 3 (3)</li> </ul>				Migrate   Deplo	yment History
Collapse All									Download	Device List Report
Name			Model	Version	Chassis	Licenses	,	Access Control Policy	Auto RollBack	
Ungrouped (3)										
Original Short 3     N/A - Routed			FTDv for Azure	7.4.1	N/A	Essentials	N	lone	4(3)	11

#### 訪問控制策略在策略>訪問控制下遷移。

_																	
٢	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis Po	licies De	evices	Objects	Integration		+> Return Home	Deploy	Q	•	e	° 0		Ŷ	cisco	SECURE
								Object Ma	nagement	Intr	usion	Net	work An	alysis Policy	DNS	Import	t/Export
																Ne	w Policy
	Access Control Policy		Status				Last Modified		Lock 5	Status							
	Default Access Control Policy Default Access Control Policy with default action block		Targeting	0 devices			2024-05-11 22:28:19 Modified by "Firepower System"									ъ р	/1
	FTD-Mig-ACP-1718216278		Targeting Up-to-date	1 devices e on all target	ted devices		2024-06-12 12:18:00 Modified by 1									% B	11

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		Add Network	▼ Q, Fil	ter	
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	Sh	ow Unused Ot	ijects s. and so on.
		,			, and as an
Name	Value		Туре	Override	
any	0.0.0.0/0 ::/0		Group		唱く言め
any-ipv4	0.0.0.0/0		Network		¶a q ≣ #
any-ipv6	::/0		Host		<b>₽</b> < <b>∂</b> &
Banned	103.104.73.155		Host	0	有人资格
Gw_test01	172.22.2.1		Host		┗/〒め
Inside_Network_IP	192.168.192.10		Host	0	┗/〒め
IPv4-Benchmark-Tests	198.18.0.0/15		Network		<b>₽</b> < <b>∂</b> &
IPv4-Link-Local	169.254.0.0/16		Network		¶∎ Q ⊕ #
IPv4-Multicast	224.0.0.0/4		Network		■ Q 〒 88
IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶∎ Q ⊕ #
IPv4-Private-172.16.0.0-12	172.16.0.0/12		Network		¶∎ Q ≣ #
IPv4-Private-192.168.0.0-16	192.168.0.0/16		Network		¶∎ Q ≣ #
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		¶∎ Q ≣ &
IPv6-IPv4-Mapped	::##:0.0.0.0/96		Network		¶∎ Q ≣ #
					B & - H

從FDM移轉至cdFMC的物件

#### 已遷移對象管理介面。

FMC / Objects / Object Mar	tor nagement	Analysis	Policies	Devices	Objects	Integration		*> Return	Home	Deploy	۹	•	¢ 😜	0		~	cisco SECURI
AAA Server     Access List     Address Pools     Annication Ethner	Inte	rface	nt your networ	k to help you n	nanage and c	lassify traffic flow. An i	nterface object simply groups interfaces. These	e groups may span m	ultiple de	Add	can also	configu	re multipl	• interf	Q, Filter	on a single	e device.
AS Path BFD Template Cipher Suite List	Nam V 🛔	e 🔺					Type Interface Group		Routed	се Туре							/ 1 4
Community List     DHCP IPv6 Pool     Distinguished Name     DNS Server Group	> 4	inside_zone	•				Security Zone		Routed								/ .
<ul> <li>External Attributes</li> <li>File List</li> <li>FlexConfig</li> </ul>	> ~ #	outside_ig	•				Interface Group		Routed								/ ¥ M
Geolocation Interface Key Chain	~ #	outside_zone	-				Security Zone		Routed								/18
> PKI	-	-Fidm-Azuro	-														

已遷移對象管理介面。

#### 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)。