Migrate FDM to cdFMC Using FMT within CDO

Contents

Introduction	
<u>Prerequisites</u>	
Requirements	
Components Used	
Background Information	
Configure	
Verify	

Introduction

This document describes how to migrate a Firepower Device Manager (FDM) to Cloud-Delivered FMC (cdFMC) using Firepower Migration Tool (FMT) in CDO.

Prerequisites

Requirements

- Firepower Device Manager (FDM) 7.2+
- Cloud-delivered Firewall Management Center (cdFMC)
- Firepower Migration Tool (FMT) included in CDO

Components Used

This document was created based on the aforementioned requirements.

- Firepower Device Manager (FDM) on version 7.4.1
- Cloud-delivered Firewall Management Center (cdFMC)
- Cloud Defense Orchestrator (CDO)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

CDO admin users can perform migrations of their devices to cdFMC when the devices are on version 7.2 or higher. In the migration described in this document, cdFMC is already enabled on CDO Tenant.

Configure

1.- Enable Cisco Cloud Services on FDM

To begin the migration, it is necessary to have the FDM device with no pending deployments and register to

Cloud Services. In order to register to Cloud Services navigate to **System Settings > See More > Cloud Services**.

Within the **Cloud Services** section, you find device is not registered, therefore, it is necessary to perform the enrollment with the type **Security/CDO Account**. You must configure a Registration Key, then Register.



Registration Cloud Services

Over Cloud Services it is shown that is not registered. Select the CDO Account enrollment type and provide the Registration Key from CDO.



Registration to Cloud Services

The registration key can be found inside CDO. Navigate to CDO, go to Inventory > Add symbol.

A menu appears to select the type of device you have. Select the FTD option. You must have the FDM option enabled; otherwise, the corresponding migration cannot be performed. The type of registration uses **Use Registration Key**. In this option, the Registration Key appears in step number 3, which we must copy and paste into the FDM.

diade Defense Orchestrator	Inventory	Q Search	॰ १४ - ०० - २०० छ	•
Hide Menu	Templates Q Search by Device Name, IP Address, or Serial Number	Displaying 8 of 8 results		C () +
Multicloud Defense	All ASA FTD			/
inventory	Name \$	Configuration Status \$	Connectivity \$	

Onboard FDM, add option

A menu appears to Select a Device or Service Type.



Select Device or Service Type

For this document, Select Registration Key has been selected.



Here, it shows the Registration Key needed on the previous step.

Fil Mi	rewall Threat Defense anagement Mode:) FTD () () FDM () ecommended)	▲ Important: This method of onboarding allows for local co-management of the firewall via FDM. To manage your device with delivered Firewall Management System, click the FTD button instead. Learn more Composition of the device using a registration Key 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)	ith cloud-
1	Device Name		
2	Database Updates	Enabled	
3	Create Registration Key	7a53c	
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	

Registration Process

Once the **Registration Key** has been obtained, copy and paste it into the FDM and click **Register**. After registering the FDM within Cloud Services, it is displayed as **Enabled** as shown in the image.

The Smart License has been skipped as the device is going to be registered once the device is up and running.

Monitoring	Policies	 Objects	Device: joroa-fdm-tech
Device Summa Cloud Se Not Reg	ry Prvices Istered		
You can register use Cisco Defe register with th auto-enroll with want to use Se configure Smar register with th	er the device w ense Orchestra e cloud using h CDO or a Se cure Firewall o rt Licensing, w e cloud, you c	with the Cisco clo ator (CDO) for ma your CDO or oth ocure Firewall Ma device manager which automatical 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 Ily registers the device with the Cisco cloud. After you able features as needed.
Enrollment Typ	e		
Security/CD0	O Account	Smart Licensing	1
Region US Region			~ 6
Registration Ke	У		
7a53c2t			
Service En	rollment		
Cisco D	efense Orc	hestrator	
Cisco Defe devices. S account.	ense Orchestra elect this option	ator is a cloud-b on if you want to	ased management tool used for managing network register the device in your Cisco Defense Orchestrator
🔽 Enabl	e Cisco Defen	se Orchestrator	
Cisco S	uccess Net	work	
Cisco Suc essential f product ar of the prod	cess Network or Cisco to pro nd to make you duct in your ne	enablement pro- ovide technical s u aware of unuse etwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ad available features so that you can maximize the value
Check out	the Sample D	ata that will be s	ent to Cisco. See more 🗸
🚦 🔽 Enroll	Cisco Succes	s Network	
REGISTER	Need he	lp? 🖸	

FDM Registration

When registering FDM, it shows the Tenancy, Cloud services connected, and Registered.



FDM Registration Complete

Within CDO, in the Inventory menu, the FDM can be found in the process of being on-boarded and synchronizing. The progress and flow of this synchronization can be reviewed within the **Workflows** section.

Once this process is completed, it appears be displayed as Synced and Online.

estee Defense Orchestrator	Inventory			Q Search	<mark>ଓ</mark> ⊳r-	۵0-	₫1	<u>۰</u>
Hide Menu	T Devices Templates Q S	earch by Device Name, IP Address, or Serial Number		Displaying 9 of 9 results	C 🛛 🕇	> Fom Devic	ce Details	2
Configuration	Name =		Configuration Status	Connectivity \$		Se Ve	odel trial	Cisco Firepower Threat Defense for Azure
 Policies Objects 	C FDM			Serial Number Mismatch		or M Sr	nboarding ethod sort Version	Registration Key 3.1.53.100-56
-& VPN >	C FTD		Ø Not Synced	Pending Setup		ຈິ S ງ ແ	yncing 00 is communicat a moment.	ing with your device. Please check back
√r Analytics →	O FTD			Pending Setup		Devi	API Tool	
(+) Jobs	O FTD			Pending Setup		3	Workflows Manage Back Remove	ups
Settings >	FDM		Syncing	Online		Man	agement	
				Online		6	Notes Changelog Executive Rep	port
	O FTD		O Not Synced	A Unreachable		i≟ c	onflict Detecti heck every:	Disabled • Tenant default (24 hours) •
						Labe	el Groups and L	abels



When the devices have been synchronized, it shows like Online and Synced.



When the FDM has been successfully on-boarded to CDO, we must log out of the FDM. After logging out of the FDM, navigate within CDO to **Tools & Services > Migration > Firewall Migration Tool**.

😤 Tools & Services		Tools & Services	Migrations
δ} Settings	>	Ø Dynamic Attributes Connector	Firewall Migration Tool
			會 ASA to FDM Migration
		😑 Firewall Management Center	畲 Migrate FTD to cdFMC
		ASA Templates	

Click the **Add** symbol, and a random name appears, indicating that the name needs to be renamed to initiate the migration process.

•	g Search for a migration by name	Displaying 0 of 0 results			10
Nerve	J Status	Created Data: 0	Deprovisioning Data a	Actions	1
	No migratio	ons found. Begin migrating ASA, FDM, Checkpoint, Fortine	, or Palo Alto Networks firewalls to FTD.		

After renaming, click on **Launch** to begin the migration.

		C Search
	Initialize Migration	×
	To initialize the migration process, name this migration and click OK. CD notify you when the migration tool is ready for use. When ready, select to migration and launch the tool.	0 will this named
	Name *	
I	.fdm_migration	
l	This is an auto-generated name. You can change it if you wish.	
	Cano	OK

Initialize Migration

Click **Launch** to start the migration configuration.

	Q Search	<u>७</u> फ़ा• ∆ 0- ⇔1	· ·
Displaying 1 of 1 results			i C +
tus Created Date ©	Deprovisioning Date ©	Actions	
Ready to Migrate Jun 12, 2024	Jun 19, 2024	C 🔒 Launch	
R	Displaying 1 of 1 results as Created Date 2 leady to Migrate Jun 12, 2024	Created Date © Deprovisioning Date © Jun 12, 2024 Jun 19, 2024	Q Search S Pr A D Displaying 1 of 1 results xs Created Date 2 Actions leady to Migrate Jun 12, 2024 Jun 19, 2024 If a conch

Migration Launch process

After clicking **Launch**, a window is going to open for the migration process where the option Cisco Secure Firewall Device Manager (7.2+) is selected. As previously mentioned, this option is enabled starting from version 7.2.

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 Select Source Configuration

Once selected, three different migration options are presented: Shared Configuration Only, Includes Device & Shared Configurations, and Includes Device & Shared Configurations to FTD New Hardware.

For this instance, the second option, Migrate Firepower Device Manager (Includes Device & Shared Configuration), is performed.

) 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
	 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.	

Migration Options

Once the migration method has been selected, proceed to select the device from the list provided.

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
fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_
Connect

FDM Device Selection



Config Extraction Completed

It is recommended to open the tab located at the top to review and understand at which step we are when the device has been selected.



Steps for Migration Process

Being a new migration, select **Cancel** when prompted with the option "*Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC?*"

Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.	
🔿 Yes 💿 No	
Save Cancel	

Cancel option for Existing Configuration

Afterwards, there are going to be options to select the Features to be migrated as shown in the image. Click **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 should	d be carried o	ut in a maintena	nce window.						
Select Target 🗿					^			Sele	ource: Cisco Secure Fi cted Migration: Includ	rewall Device Manager (7.2+) es Device and Shared Config
Firewall Management - C	Cloud-delivered FMC									>
Select Features										~
Device Configuration		SI	ared Configura	tion			0	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 (Cry	pto Map)		Time based Obi	ects (no data)						
Route Based (VTI	9		Remote Access	VPN						
Platform Settings			File and Malware	Policy						
- DHCP										
Server										
Relay										
DDNS										
Proceed										
Note:Platform settings an	d file and malware policy migrat	ion is supporte	d in FMC 7.4 and I	ater versions.						



Then Start Conversion.

Firewall Migration To	ool (Version 6.0	.1)									
		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 sho	Id be carried o	ut in a maintena	nce window.		_				
Se	elect Target 🕠					^			Sciences	ource: Cisco Secure Firew cted Migration: Includes [all Device Manager (7.2+) Device and Shared Config
FI	irewall Management - C	loud-delivered FMC									>
Se	elect Features										>
R	ule Conversion/ Proces	ss Config									~
C	Start Conversion										

Start conversion.

Once the parsing process has concluded, two options can be used: **Download** the document and continue with the migration by clicking **Next**.



Download Report.

The device interfaces are set to be displayed. As a best practice, it is advisable to click **Refresh** to update the interfaces. Once validated, you can proceed by clicking **Next.**

Map FTD Interface O Interface Name FDM Interface Name FTD Interface Name Ggabitthemetion Ggabitthemetion
Map FTD Interface Image: (7.2*) Compatible meetio Ogabitithemeetio Ogabitithemeetio Ogabitithemeetio
FDM Interface Name FDD Interface Name OgabetEnerret00 OgabetEnerret00 OgabetEnerret01 OgabetEnerret01
OgaabEthernet00 OgaabEthernet00 OgaabEthernet011 OgaabEthernet011
Ggab#ElhernetD1 Ggab#ElhernetD1

Interfaces Displayed

Navigate to the **Security Zones** and **Interface Groups** section, where you need to add manually with Add SZ & IG. For this example, **Auto-Create** has been chosen. This helps to automatically generate the interfaces within the FMC to which you are migrating. After finish, click on the **Next** button.

Firewall Migration Tool (Version 6.0.1)

	Extract FDM Information	2 3 Select Target Map FTD Interface	5 Map Security Zones 8. Review & Validat Interface Groups (Shared Config)	6 Push Shared Config To FMC	7 Move Manager Review (Device	8 9 & Validate Complete Mgration e Config)	
	Note: Steps 7,8 and 9 should	d be carried out in a maintena	ance window.	_			
Map Security Zone	es and Interface Group	ps 🕡	^	Add Si	Z & IG Auto-Crea	Source: Cisco Se Selected Option	cure Firewall Device Manager (7.2+) Includes Device and Shared Config
FDM Logical Interface	FDM Security Zones	s FTD Interface	FMC Security	Zones FI	IC Interface Groups		
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	Sele	ct interface Groups	~	
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Sele	ct Interface Groups	~	

Security Zones and Interface Groups

Auto-Create option maps FDM interfaces to existing FTD Security Zones and interfaces groups in FMC that have the same name.

		C
FTD		Group
Gigabit	Auto-Create	ups
Gigabit	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.	ups
	Select the objects that you want to map to FDM interfaces	
	🤜 Security Zones 🔽 Interface Groups	
	Cancel Auto-Create	

Auto-Create Option.

Then select Next.

Image: training into traininto traininto training into traininto training into trai	Firewall Migration Tool (Version 6.0.	.1)						
Item:: tem:: tem:: <t< th=""><th></th><th>Extract FDM Information Select Targe</th><th>3 4 Map FTD Interface Map Security Zone Interface Group</th><th>5 es & Review & Validate Push Share is (Shared Confg) Fi</th><th>6 7 d Config To Move Manager MC</th><th>8 Review & Validate (Device Config)</th><th>9 Complete Migration</th><th></th></t<>		Extract FDM Information Select Targe	3 4 Map FTD Interface Map Security Zone Interface Group	5 es & Review & Validate Push Share is (Shared Confg) Fi	6 7 d Config To Move Manager MC	8 Review & Validate (Device Config)	9 Complete Migration	
Image: Security Zones and Interface Groups () Image: Society Zones FID Interface Image: Society Zones FID Image: Society Zones <t< td=""><td></td><td>Note: Steps 7,8 and 9 should be carrie</td><td>ed out in a maintenance window.</td><td></td><td></td><td></td><td></td><td></td></t<>		Note: Steps 7,8 and 9 should be carrie	ed out in a maintenance window.					
FDM Logical Interface N FDM Security Zones FD Interface FMC Security Zones FMC Interface Groups viside usble_zone GgaddEthernet50 usble_zone (A) usble_g (A) v made usble_zone GgaddEthernet51 node_zone (A) usble_g (A) v Mode_Zone GgaddEthernet51 node_zone (A) usble_g (A) v Mode_Zone GgaddEthernet51 node_zone (A) usble_g (A) v Mode_Zone GgaddEthernet51 node_zone (A) usble_g (A) v	Map Security Zones	s and Interface Groups 🕕					Source: Cisco Secure Firew Selected Option: Includes I	all Device Manager (7.2+) Device and Shared Config
FDM Logical Interface N FDM Security Zones FDD Interface FMC: Security Zones FMC: Security Zones FMC: Security Zones FMC: Security Zones extade outside_zone Orgatititemention outside_zone (A) outside_g(A) v extade issde_zone Orgatititemention issde_zone (A) issde_g(A) v extade issde_zone Orgatititemention issde_zone (A) issde_g(A) v extade issde_zone Orgatititemention issde_zone (A) issde_zone (A) issde_g(A) v					Add SZ & IG	uto-Create		
outside outside_zone Ogsbitthermethth outside_zone (A) outside_y(A) v nade nade_zone Ogsbitthermethth nade_zone (A) nade_g(A) v Nade_Click on Auto-Create button to auto map the FDM namef as the name of the FMC interface objects and security zones. Click on next button to proceed ahead. 10 PR-9287 2 q = Page 1 of 1 > b]	FDM Logical Interface N	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface G	oups		
made made_zone GigateEthemetD1 made_zone (A) made_ug (A) v Image: Second Action 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. Image: Second Action 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. Image: Second Action 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.	outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_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.	inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)	÷		
10 v pet,page 2 4 4 Page 1 of 1 ▶ ▶	<u>Note:</u> Click on Auto-Create bu	itton to auto map the FDM nameif as the r	name of the FMC interface objects and	d security zones. Click on next	; button to proceed ahead.			
	10 v per.pege 2 [4	∢ Page 1 of 1 ⊨ ►						

After Auto-Creation option.

In step 5, as shown in the top bar, take the time to examine the Access Control Policies (ACP), Objects, and NAT rules. Continue by carefully reviewing each item and then click on **Validate** to confirm that there are no issues with names or configurations.

Firewall Migration	Tool	(Versio	n 6.0.1)					
			1 2 Extract FDM Information Select Target	3 4 S Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Bhared Config)	6 7 Push Shared Config To Move Manager FMC	8 Review & Validate Com (Device Confg)	9 piete Migration	
			Note: Steps 7,8 and 9 should be carried of	out in a maintenance window.				
	Opti	mize, R	eview and Validate Shared Con	figuration Only 💿	,	Sourc Selected	e: Cisco Secure Firewal Migration: Includes De	Device Manager (7.2+) vice and Shared Config
	Access	Control	Dbjects NAT Interfaces Routes Site-to-S	Site VPN Tunnels 🜒 Remote Access VPN SI				
	Acc	ess List Obje	cts Network Objects Port Objects Access Co	ontrol Policy Objects VPN Objects Dynamic-Rout	e Objects			
	Sel	lect all 3 entri	ies Selected: 0/3 Actions - Save				Q Search	+
	•	*	Name Q	Validation State	Туре Q		/alue 2	
	0	1	OutsidelPv4Gateway	Validation pending	Network Object	172	2.18.1.1	
	0	2	OutsideIPv4DefautRoute	Validation pending	Network Object	0.0	0.0/0	
		3	Banned	Validation pending	Network Object	103	3.104.73.155	
rpage 1 to 3 of 3 4 4	Page	1_ of 1 ≽	И			Val	lidate	

Access Control, Objects and NAT Configurations

Then Push Shared Configuration Only



Push Shared Configuration Only

The percentage of completion and the specific task being worked on can be observed.

Firewall Migratio	on Tool (Version 6.0.1)			
	Push Shared Config to I	FMC	PUSHING	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 migration	n report for a detailed summary.		

Pushing Percentage

After completion of step 5, proceed to step 6, as displayed in the top bar, where the **Push Shared Configuration to FMC** takes place. At this, select the **Next** button to advance.

	1 Extract FDM Informat	2 ion Select Target	3 Map FTD Interface	4 Map Security Zones & Interface Groups	5 Review & Validate (Shared Config)	Push Shared Config To FMC	7 Move Manager	8 Review & Validate (Device Config)	9 Complete Migration	
	Note: Steps 7,8 and 9 sh	ould be carried out	t in a maintena	nce window.						
Push Shared Co	nfig to FMC				^			Solution	Source: Cisco Secure Fire	vall Device Manager
Migration Status								aen	ected migration. Includes	Device and Shared
Live Connect:										
Selected Context: Single C Migration Summary (Post F	untext Mode									
Selected Context: Single C Migration Summary (Post F	ontext Mode			4					3	
Selected Context: Single C Migration Summary (Post F 3 Access Control List Line	suntext Mode tush) s			4 Network (76jects				3 Access Control Policy O (Gee, Application, URL obje Intrusion Rule Group)	bjects (ts and)
Selected Context: Single C Migration Summary (Post F 3 Access Control List Line Not selected for migrab	sentext Mode sush) s (Slane) m	selected for migration iccreas List Objects text, Extended used in BC RAVINEZCRIP)		4 Network C	Dbjects or migration				3 Access Control Policy O (Geo, Application, URL obje Intrusion Rule Group) Not selected for migro	bjects cts and)

Push Shared Config to FMC Completed

This option triggers a confirmation message, prompting the continuation of the manager migration.

Confirm Move Manager

Requires maintainence window to be scheduled FDM manager will be moved to be managed in FMC.



Confirm Move Manager

Proceeding with the manager migration requires having the Management Center ID and NAT ID at hand, which is essential. These IDs are retrievable by selecting **Update Details.** This action initiates a pop-up window where the desired name for the FDM representation within the cdFMC is entered, followed by saving the alterations.

Firewall Migration Tool (Version 6.0	0.1)									
	1		-0-		6	•	8	9		
	Extract FDM Information	Select Target Map FTD Interface	Map Security Zones & Interface Oroups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration		
	Note: Steps 7,8 and 9 should	be carried out in a maintena	nce window.							
Move Manager				^			Selec	ource: Cisco Se ted Migration:	cure Firewall Device Includes Device and	e Manager (7.2+) d Shared Config
Update Deta	alls									
This step is mandatory an	nd should be performed during	a downtime window. After yo	ou register the dev	vice with the m	anagement center	or Cloud-delive	ered FMC, you ca	in no longer use	the device manage	er to manage it.
Management Cent	Management Cente 🕒	NAT ID 🕟	Threat De	efense Hostn	DNS Server	Group	Manageme	nt Center/	Data Interface	
cisco edi	o		1	Leloude	app.n CiscoUmbrellaDN	SServerGroup 🗸	💿 Data 🕥 Ma	inagement	Select Data Interface	v

Manager Center ID & NAT ID

Firewall Migration Tool (Version 6.0	Extract FEM Information Sel Note: Steps 7,8 and 9 should be	2 Up	date Device Name for I	X	Berier & Valdas Complete Higuiton (Davies Contg)		
Move Manager Uptate Data This step is mandatory ar	dt	downtime	Cancel Sam		Source: Cisco Se Selected Migration: d FMC, you can no longer use	cure Firewall Device Ma Includes Device and Sh the device manager to	nager (7.2+) ared Config
Management Cent	Management Cente 💿	NAT ID 🕕	Threat Defense Hostn	DNS Server Group	Management Center/	Data Interface	
cisco-mex-ngfw-tac.app.us.cd	D		joroa-fdm-techzone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup ~	💿 Data 🕥 Management	Select Data Interface	v .

Update Device Name for Registration.

After this action, the IDs for the aforementioned fields are shown.



Warning: Do not make any changes to the Management Center Interface. By default, the Management option is selected, leave this option as the default setting.

		()	2			-(5)		-0-	8	9	
	Extract	t 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	,8 and 9 should b	be carried out	in a maintena	nce window.						
Move Man	ger				(^)		So	urce: Cisco Sec ted Migration:	cure Firewall Device Ma Includes Device and Si
Move Mana	ger				,				So Select	urce: Cisco Sec ted Migration:	cure Firewall Device Ma Includes Device and SI
Move Mana	ger te Details tory and <u>should be per</u>	rformed during a	a downtime wi	indow. After yo	<u>ou regi</u> ster the dev	vice with the ma	inagement center	or Cloud-delive	So Select re <u>d FMC, you ca</u>	urce: Cisco Sec ted Migration: n no longer use	cure Firewall Device Ma Includes Device and Si the device manager to
Move Mana Up This step is mand Management	GEF te Details tory and <u>should be perf</u> ent Manageme	rformed during a ent Cente 🕡	a downtime wi	indow. After yo	ou register the dev Threat De	vice with the ma	DNS Server	or Cloud-delive Group	So Select red FMC, you ca Managemen	urce: Cisco Set ted Migration: n no longer use t Center/	the device manager to Data Interface
Move Mana Up This step is mand Management of casce	ger te Details tory and should be performed ant Management us.coto ogu	rformed during a ent Cente i	a downtime wi NAT ID (GW 104V	indow. After yo	Du register the dev Threat De BaPMi dm-Azu	vice with the ma efense Hostn	DNS Server CiscoUmbrellaDN	or Cloud-delive Group SServerGroup ~	So Select Management	urce: Cisco Set led Migration: n no longer use t Conter/	cure Firewall Device Mil Includes Device and SI the device manager to Data Interface Select Data Interface

Move Manager

After choosing **Update Details** option, the device it is going to start syncing.

Tool (Version 6.	0.1)									
	1 Extract FDM Information	2 Select Target Ma	3 4 4	es & Review & Validate ps (Shared Config)	B Push Shared Config To FMC	T Move Manager	8 Review & Validate (Device Config)	9 Complete Migration		
	Note: Steps 7,8 and 9 should	d be carried out in	a maintenance window.							
Move Manager							Soi Select	urce: Cisco Sec ed Migration: I		
Update Det	ails	g a downtime wind	dow.	SYNCING the FDM D	evice	ıd-delive	red FMC, you car	n no longer use	the device manager to	o manage it.
Update Det This step is mandatory a Management Cent	nd should be performed durin Management Cente	g a downtime wind	:	SYNCING the FDM D	evice	ıd-delive	red FMC, you car Management	n no longer use t Center/	the device manager to Data Interface	o manage it.
Update Det This step is mandatory a Management Cent Cisco us.co	ails nd should be performed durin Management Cente	g a downtime wind NAT ID • 666W 104	dow.	SYNCING the FDM Do 9% Complete	evice CiscoUmbrelaDNS	id-delive ServerGroup ∨	red FMC, you car Management	n no longer use t Center/	the device manager to Data Interface Select Data Interface	o manage it. V

Syncing FDM Device

After the migration is finalized, the next step is to examine the interfaces, routes, and DHCP settings configured in the FDM by selecting **Validate**.

wall Migration	Tool (Versi	on 6.0.1)	2 3 4 ext Target Map FTD Interface Map Security Zones & I	5 6 7	9 Review & Validate Complete Mgration	
		Note: Steps 7,8 and 9 should be	carried out in a maintenance window.	(shared Config) PMC	(Device Config)	
c	Optimize, I	Review and Validate Device	e Configuration Page 🕦	^	Source: Cisco Se Selected Migration	cure Firewall Device Manager (7.2+)
		Objects NAT Interfaces Routes	Site-to-Site VPN Tunnels 🔵 Remote Access V	/PN SNMP DHCP	selected migration	. Includes bevice and shared coming
	Static PPPo	E				
0	Select all 2 er	ntries Selected: 0 / 2			Q S	earch 🛓
	•	Interface Q	Zone Q	IP Address	State	
0	0 1	GigabitEthernet0/0	outside_zone		Enabled	
0	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
to 2 of 2 4 4 Pa	age 1 of 1	> >]				

Validate FDM configuration Settings

After validation, choose **Push Configuration** to initiate the configuration push process, which is going to continue until the migration concludes. Additionally, it is possible to monitor the tasks that are being executed.

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

Validation Status - Push Configuration.

Pop-up window with the percentage pushing configuration.

Firewall Migration Tool (Version	6.0.1)					
	Ensut FDM Information Select	2 Theyar Map PTD PUSHING arried out in a ma Push to Clouded way for entire au	ivered FMC is In progress. Please	7 8 Aanager Review & Validas (Device Config)	Complete Migration	
Complete Mi Migration Status	gration			s	Source: Cisco Secure Firew elected Migration: includes (
Interfaces	0					
Routes	0					
DHCP						
Policy Assignme	nt					
Please download the l	Post-Push migration report for a detailed sur	nmary. Download Report				

Pushing Percentage Completed

Upon completion, an option to initiate a new migration is presented, marking the end of the migration process from FDM to cdFMC.

igration root (version o	3.0.1)				
	(Extract F0	1 2 3 DM Information Select Target Map FTD I	Ap Security Zones & Review & Validante Interface Groups (Shared Config)	6 7 6 Push Shared Config To Move Manager Review & PMC (Device	3 Voldate Complete Migration Config)
	Note: Steps 7,8	and 9 should be carried out in a ma	intenance window.		
Complete Mig	ration				Source: Cisco Secure Firewall Device Manager (7. Selected Migration: Includes Device and Shared Co
Migration Status					
Migration is convext Step - Log	nplete, policy is pushe in to FMC to deploy th	d to FMC. e policy to FTD.			
Live Connect:					
Selected Context: Sin	gle Context Mode				
Migration Summary (P	ost Push)				
3			4		3
Access Control Lis	Lines		Network Objects		Access Control Policy Objects
					(Geo, Application, URL objects and Intrusion Rule Group)
		2	2	1	1
		2 Network Address Translation	2 Logical Interfaces	1 Routes	1 онср

Complete Migration

Verify

To verify that the FDM has been successfully migrated to the cdFMC.

Navigate to **CDO** > **Tools & Services** > **Firepower Management Center**. There, you find the number of registered devices has increased.

cisco Defense Orchestrator	Services				Q Search	उ व	, -	¢۰ ظ1 @۰ ۲
Hide Menu							>	Cloud-Delivered FMC
Dashboard	Q Search by Device Name IP Address or	Serial Number						Version 20240514
C Multicloud Defense	FMC Secure Connectors							Actions
Inventory								
Configuration	i "Auto onboard On-Prem FMCs from Secure"	K tenant" setting is not enabled. Click here	to enable settin	ıg.				Check For Changes Deployment Undetes
Policies >	(-) ·							Workflows
Objects >	Name	Version	Devices	Туре	Status	Last Heartbeat		API Explorer
"Å⊨ VPN →	Cloud-Delivered FMC	20240514	⊖ 3	Cloud-Delivered FMC	O Active	06/12/2024, 12:42:21		Management
Events & Monitoring	0	7.2.7-build 500	⊜0	On-Prem FMC	A Unreachable			
√r Analytics → ④ ChangeLog 실 Jobs								Policies Objects CNAT Site to Site VPN Remote Access VPN Platform Settings
Tools & Services	Tools & Services Migra	tions Firewall Migration Tool						
Settings >	Secure Connectors	ASA to EDM Migration						System
	 Firewall Management Center ASA Templates 	Migrate FTD to cdFMC						Configuration Smart Leenses ANP Management Device Health Aud Cisco Cloud Events



Check the device within **Devices > Device Management**. Additionally, within the tasks of the FMC, you can find when the device was successfully registered and the first deployment was completed successfully.

Defense Orchestrator Anal	lysis Policies D	evices Objects Integration	••	Return Home Deploy Q 💿 🌮 🌣 🕢 📕	 dude SECURE
-fdm-Azure			Deployments	Upgrades Health O Tasks	+ Show Notifications
Cisco Firepower Threat Defense for Azure			20+ total 0	0 waiting 0 running 0 retrying 6 success 20+ failures	Q, Filter
Device Interfaces Inline Sets Routing DHCP	VTEP		Policy Deploym	ent	
			Policy Deploy	ment to -fdm-Azure. Applied successfully	1m 54s 🗙
General	/±+	License			
Name:	-fdm-Azure	Performance Tier :	FTI O Health Policy		
Transfer Packets:	No	Essentials:	Apply Initial_ Health Policy ap	ppled successfully	1m 40s X
Troubleshoot:	gs CU Download	Export-Controlled Features:			
Mode:	Routed	Malware Defense:	 Discovery 		
Compliance Mode:	None	IPS:	-fdm-Azur	re - Discovery from the device is successful.	2m 10s 🗙
Performance Profile:	Default	Carrier:	 SETurnel 		
TLS Crypto Acceleration:	Disabled	URL:	-1dm-Azur	re - SFTunnel connection established successfully.	- ×
		Secure Client Premier:	-		
Device Configuration:	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:	•	Remote Host Address:	NO-IP
Revent to Smort 2		Policy: Initial_Health_Policy 202	3-06-29 17:28:08	Secondary Address:	
		Excluded:	None	Status:	•
				Manager Access Interface:	Management Interface
Inventory Details	¢	Applied Policies	1	Advanced Settings	1
X III 🛛 + I			,		,

cdFMC Registration Task Completed.

Device is on **cdFMC > Device > Device Management.**

Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices Obje	cts Integratio	on		•> Return Home	Deploy	० o 🌮	° 0	~	disco SECURE
View By: Group All (3) Group View Group View By: Group Vi	Offline (0)	Normal (3)	Deployment P	ending (3)	Upgrade (0)	 Snort 3 (3) 				N Q 1	figrate Deplo	yment History
Collapse All											Download	Device List Report
Name			Model		Version	Chassis	Licenses		Access Control Pol	icy	Auto RollBack	
Ungrouped (3)												
- fdm-Azure Snort 3 N/A - Routed			FTDv for Azure		7.4.1	N/A	Essentials		None		۹۵	1

Device Registered on cdFMC

Access Control Policy migrated under **Policies > Access Control.**

٤	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis	Policies	Devices	Objects	Integration		+> Return Home	Deploy	۹	o	6 2 (× 0		v	-di-di- cisco	SECURE
								Object Ma	nagement	Intr	usion	Netw	ork An	alysis Policy	DNS	Import	t/Export
																Ne	w Policy
	Access Control Policy		s	Zatus			Last Modified		Lock 5	tatus							
	Access controlley						Salat mounted		Look								
	Default Access Control Policy Default Access Control Policy with default action block		Ta	rgeting 0 devices			2024-06-11 22:28:19 Modified by "Firepower System"									°6 🛙	/1
	FTD-Mig-ACP-1718216278		Ta Up	rgeting 1 devices	eted devices		2024-06-12 12:18:00 Modified by 1									% B	11

Migration Policy

Likewise, you can review the objects created in the FDM which were correctly migrated to the cdFMC.

Network		Add Network	•	Q, Filte	r		
A natural abiest concents and ar more ID addresses. Matural, abiests are used in unders alsoes, including assess partial reliairs, natural, abiests	minhlan interview when	dentitu nilas notuent dissources	nulae er	Show	w Unused Obj	ects	
A network object represents one or more in addresses. Network objects are used in various places, including access control policies, network to	vanables, intrusion rules,	dentity rules, network discovery	ruies, e	vent sea	renes, reports	, and so o	H1.
Nama	Value		Turne		Override		
PHILITY	0.0.0.0/0		1350		Cremine		
any	::/0		Group)		η Q Ι	8
any-ipv4	0.0.0.0/0		Netwo	ork		G Q	M
any-ipv6	::/0		Host			¶∎ ⊂ i	M
Banned	103.104.73.155		Host		•	9/i	N
Gw_test01	172.22.2.1		Host			6/1	8
Inside_Network_IP	192.168.192.10		Host		0	¶∕i	A
IPv4-Benchmark-Tests	198.18.0.0/15		Netwo	ark		n q i	8
IPv4-Link-Local	169.254.0.0/16		Netwo	ork		₽ Q	8
IPv4-Multicast	224.0.0.0/4		Netwo	ork		B Q	8
IPv4-Private-10.0.0.0-8	10.0.0/8		Netwo	ork		B Q	8
IPv4-Private-172.16.0.0-12	172.16.0.0/12		Netwo	ork		G Q	8
IPv4-Private-192.168.0.0-16	192.168.0.0/16		Netwo	ork		F1 Q 1	M
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group			F _1 Q i	M
IPv6-IPv4-Mapped	::fff:0.0.0.0/96		Netwo	ork		F1 Q 7	8

Objects Migrated from FDM to cdFMC

Object Management interfaces Migrated.

FMC / Objects / Object Ma	itor nagement	Analysis	Policies	Devices	Objects	Integration		•	Return Home	Deploy	Q	• 💞	° 0		Ý	cisco SECURE
> AAA Server	Interfa	ace								Add			*	Q, Filter		
Access List Address Pools	Interface of	objects segment	your network	to help you r	nanage and cl	assify traffic flow. An i	nterface object simply groups inte	erfaces. These groups may :	span multiple d	evices; you	an also c	configure i	nultiple inte	rface objects	on a single	device.
Application Finers AS Path BED Template	Name 🔺						Туре		Interf	се Туре						
Cipher Suite List	✓ ♣ insi	ide_ig					Interface Group		Route	đ						1 8
DHCP IPv6 Pool	> ===	-fdm-Azure	_				Security Zone		Route	1						
DNS Server Group	> #	-fdm-Azure														
File List	v 📥 out	side_ig					Interface Group		Route	t					,	1 W M
Geolocation	> 🖷	-fdm-Azure														
Key Chain	v de out	side_zone					Security Zone		Route	1						110
> PKI	> =	-tam-Azure														

Object Management Intefaces Migrated.