

Migrate FDM to cdFMC Using FMT within CDO

Contents

[Introduction](#)

[Prerequisites](#)

[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

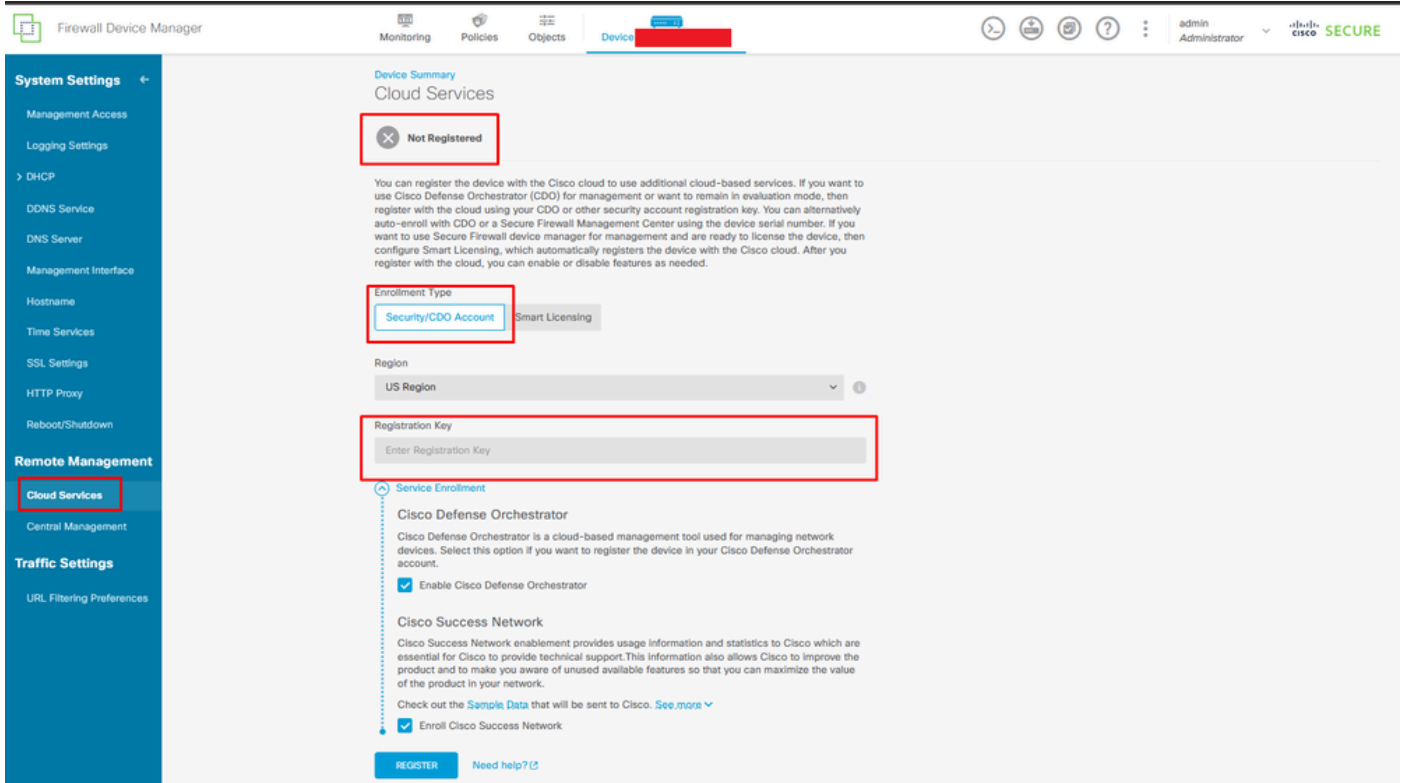
To begin the migration, it is necessary to have the FDM device with no pending deployments and register to

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

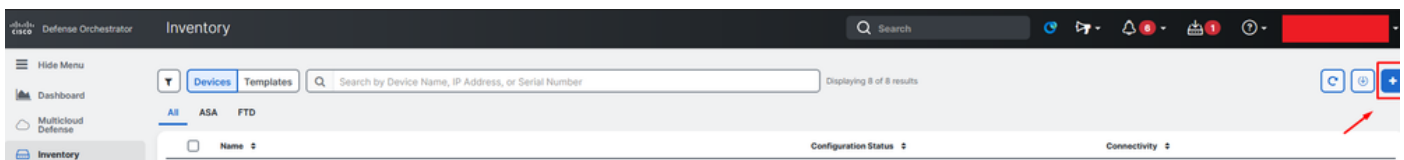
Over Cloud Services it is shown that is not registered. Select the CDO Account enrollment type and provide the Registration Key from CDO.



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.



Onboard FDM, add option

A menu appears to Select a Device or Service Type.

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

Meraki Security Appliance



Integrations

Enable basic CDO functionality for
integrations



VPC

AWS VPC

Amazon Virtual Private Cloud



Duo Admin

Duo Admin Panel

Umbrella

Umbrella Organization

View Umbrella Organization Policies
from CDO



Import

Import configuration for offline
management

Select Device or Service Type

For this document, Select Registration Key has been selected.

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.

Registration Type

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

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 [input field] +

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.

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

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?](#)

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

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 [re-register](#) 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 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 to be displayed as Synced and Online.

Inventory | Displaying 9 of 9 results

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	-	Syncing	Online
[Redacted] FTD	-	-	Online
[Redacted] FTD	-	-	Online
[Redacted] FTD	-	Not Synced	Unreachable

Device Details

Model: Cisco Firepower Threat Defense for Azure

Serial: [Redacted]

Version: 7.4.1-172

Onboarding Method: Registration Key

Smart Version: 3.15.3.100-56

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

Device Actions
API Tool, Workflows, Manage Backups, Remove

Management
Notes, Changelog, Executive Report

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

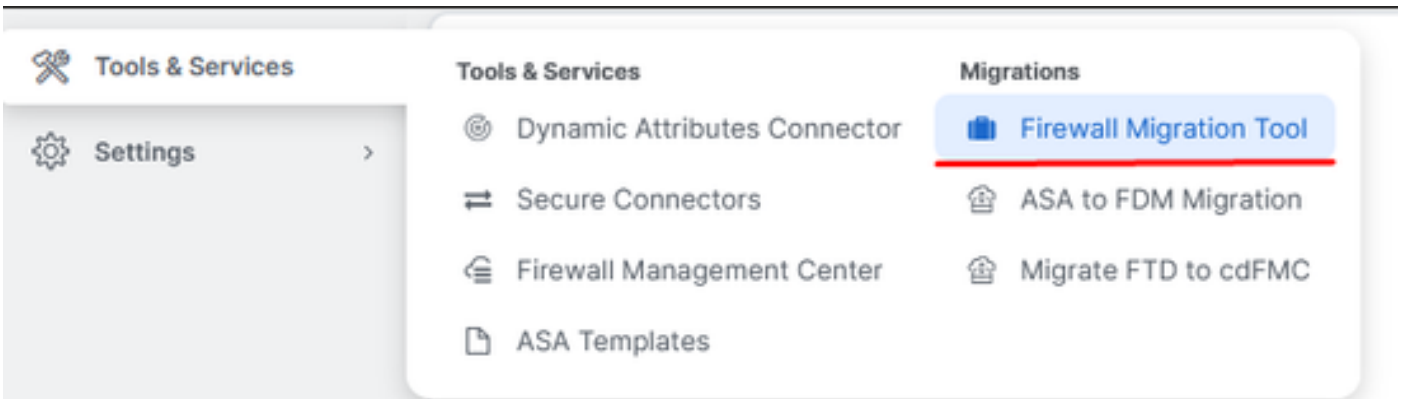
Label Groups and Labels
Add Labels

CDO Inventory FDM Onboarded

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

[Checked] [Redacted] **fdm** FDM | Synced | Online

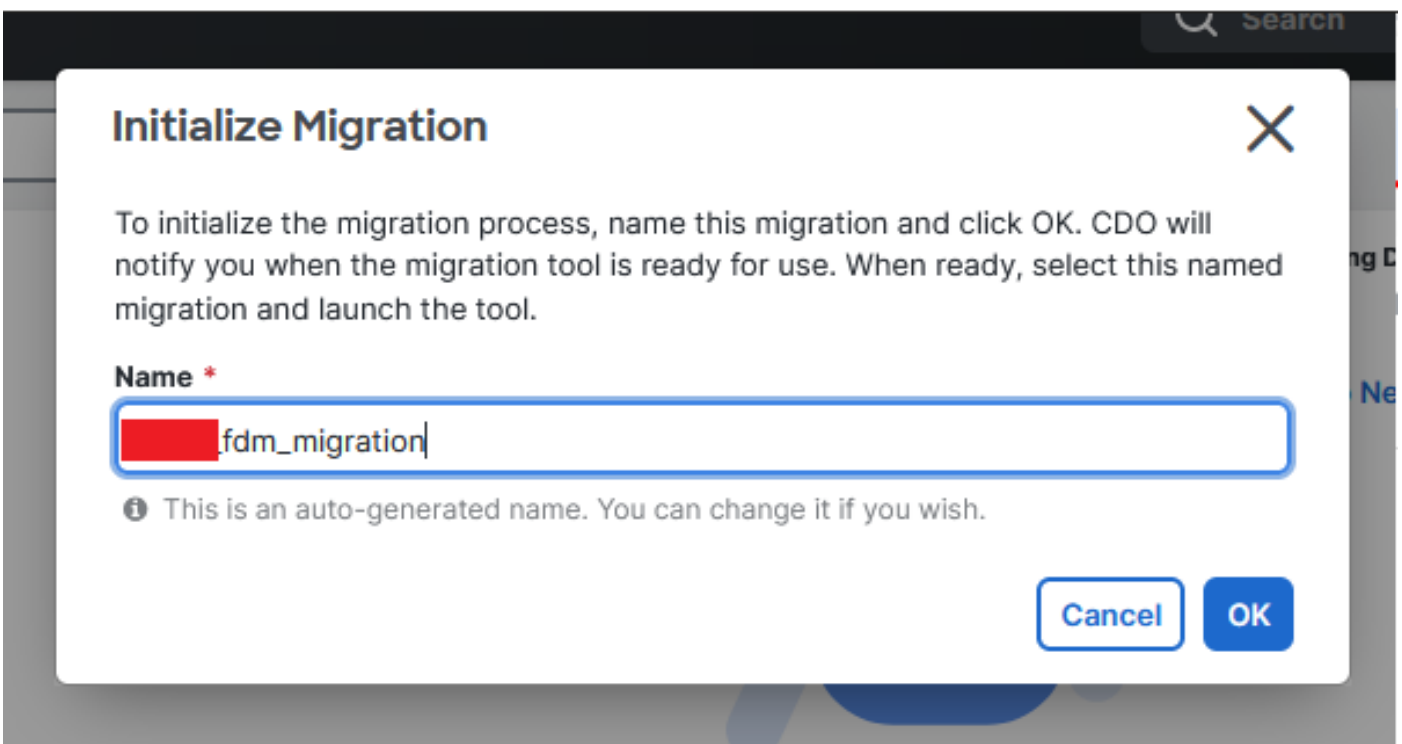
When the FDM has been successfully on-boarded to CDO, we must log out of the FDM. After logging out of the FDM, navigate within CDO to **Tools & Services > Migration > Firewall Migration Tool**.



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



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



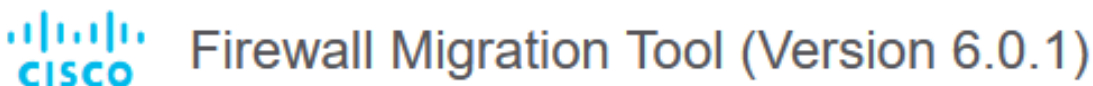
Initialize Migration

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

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

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.



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.

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) v

- 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 policies 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 :

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

████████_fdm_████████ - Available

Connect



FDM Device Selection

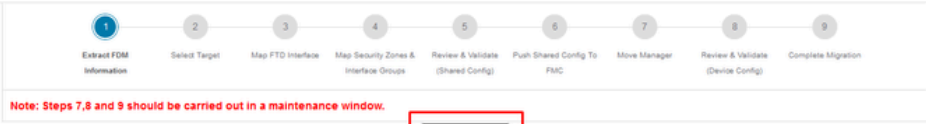
FDM device config extraction successful



100% Complete

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.



Extract Cisco Secure Firewall Device Manager (7.2+) Information

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

Extraction Methods

FDM IP Address:

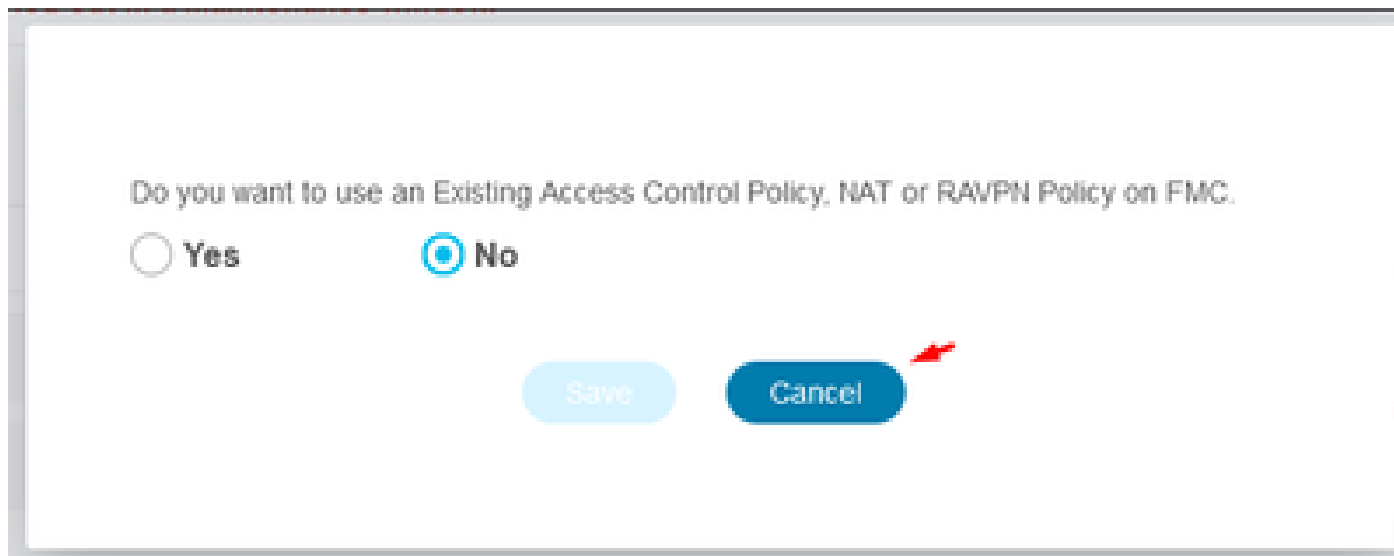
Parsed Summary

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPNEIGRP)	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	0

Back Next

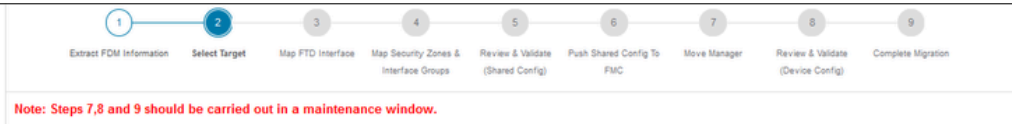
Steps for Migration Process

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?"



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**.



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 ⓘ

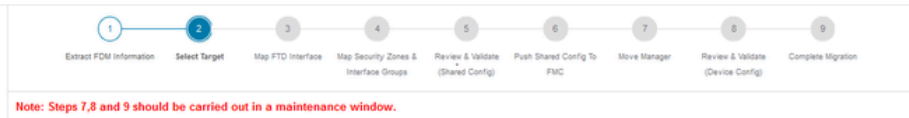
Proceed ➔

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

Features to be selected

Then **Start Conversion**.

Firewall Migration Tool (Version 6.0.1)



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 ➤

Start conversion.

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

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

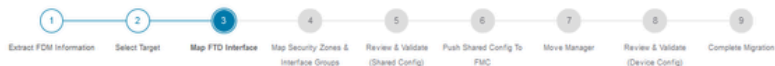
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPI/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	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)			

Back

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**.



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

Refresh

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!

Back

Next

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.

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

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 name if as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

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.

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.

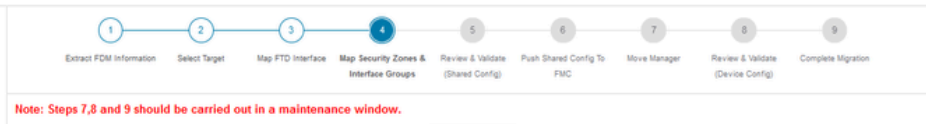
Select the objects that you want to map to FDM interfaces

Security Zones Interface Groups

Cancel Auto-Create

Auto-Create Option.

Then select **Next**.



Map Security Zones and Interface Groups

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

[Add SZ & IG](#) [Auto-Create](#)

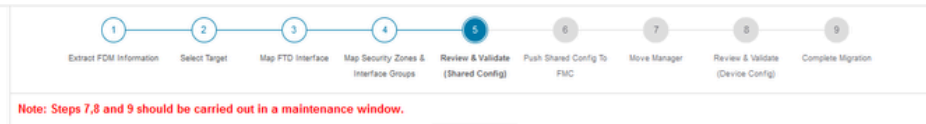
FDM Logical Interface N...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A)
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_ig (A)

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

[Back](#) [Next](#)

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.



Optimize, Review and Validate Shared Configuration Only

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

Access Control **Objects** NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN SNMP DHCP

[Access List Objects](#) [Network Objects](#) [Port Objects](#) [Access Control Policy Objects](#) [VPN Objects](#) [Dynamic-Route Objects](#)

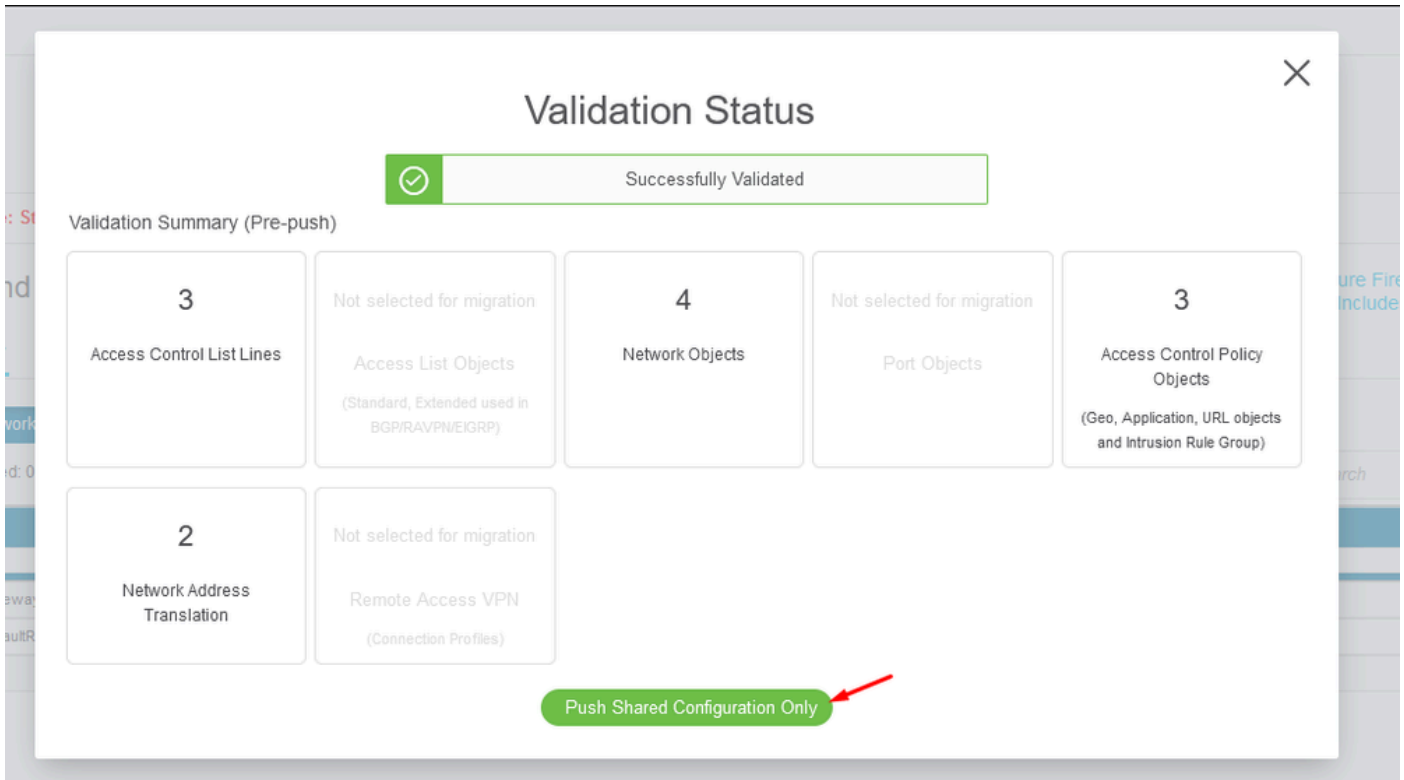
Select all 3 entries Selected: 0/3 [Actions](#) [Save](#)

#	Name	Validation State	Type	Value
1	OutsidePv4Gateway	Validation pending	Network Object	172.18.1.1
2	OutsidePv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
3	Banned	Validation pending	Network Object	103.104.73.155

[Validate](#)

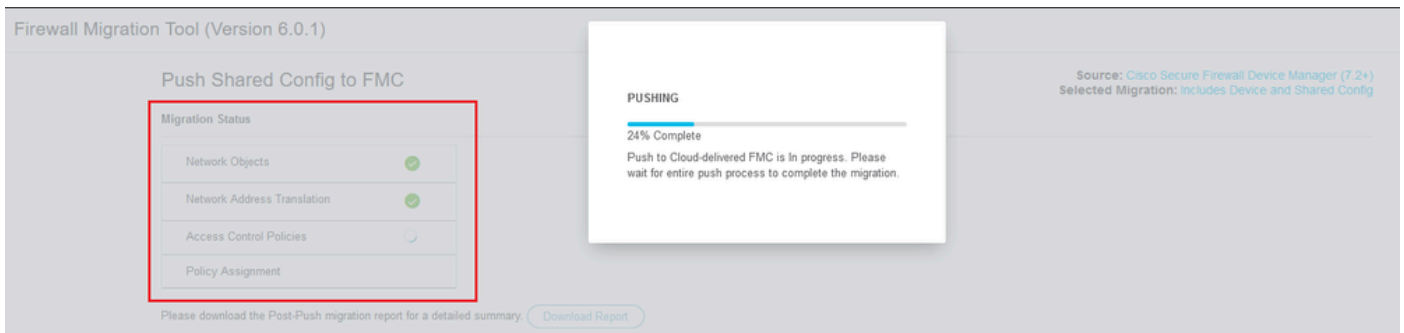
Access Control, Objects and NAT Configurations

Then **Push Shared Configuration Only**



Push Shared Configuration Only

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



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.



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

Next

Push Shared Config to FMC Completed

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

Confirm Move Manager

Requires maintenance window to be scheduled

FDM manager will be moved to be managed in FMC.

The steps outlined below should be performed in a maintenance 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.

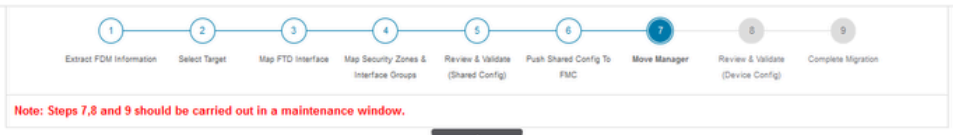
I acknowledge all the steps mentioned above have been completed.

Proceed

Cancel

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.



Move Manager

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

Update Details

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	cdc			cloudapp.ni	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management	Select Data Interface

Move Manager

Manager Center ID & NAT ID

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco-mex-ngfw-tac.app.us.cdc...			proa-fdm-techno.internal.cloudapp.ni	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management	Select Data Interface

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.

Firewall Migration Tool (Version 6.0.1)



Move Manager

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

[Update Details](#)

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... 1	NAT ID 2	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco	us.cdo...	ogp	166GW/104v	3aPMI	fdm-Azure	CiscoUmbrellaDNSServerGroup
					<input checked="" type="radio"/> Data <input type="radio"/> Management	Select Data Interface

Save

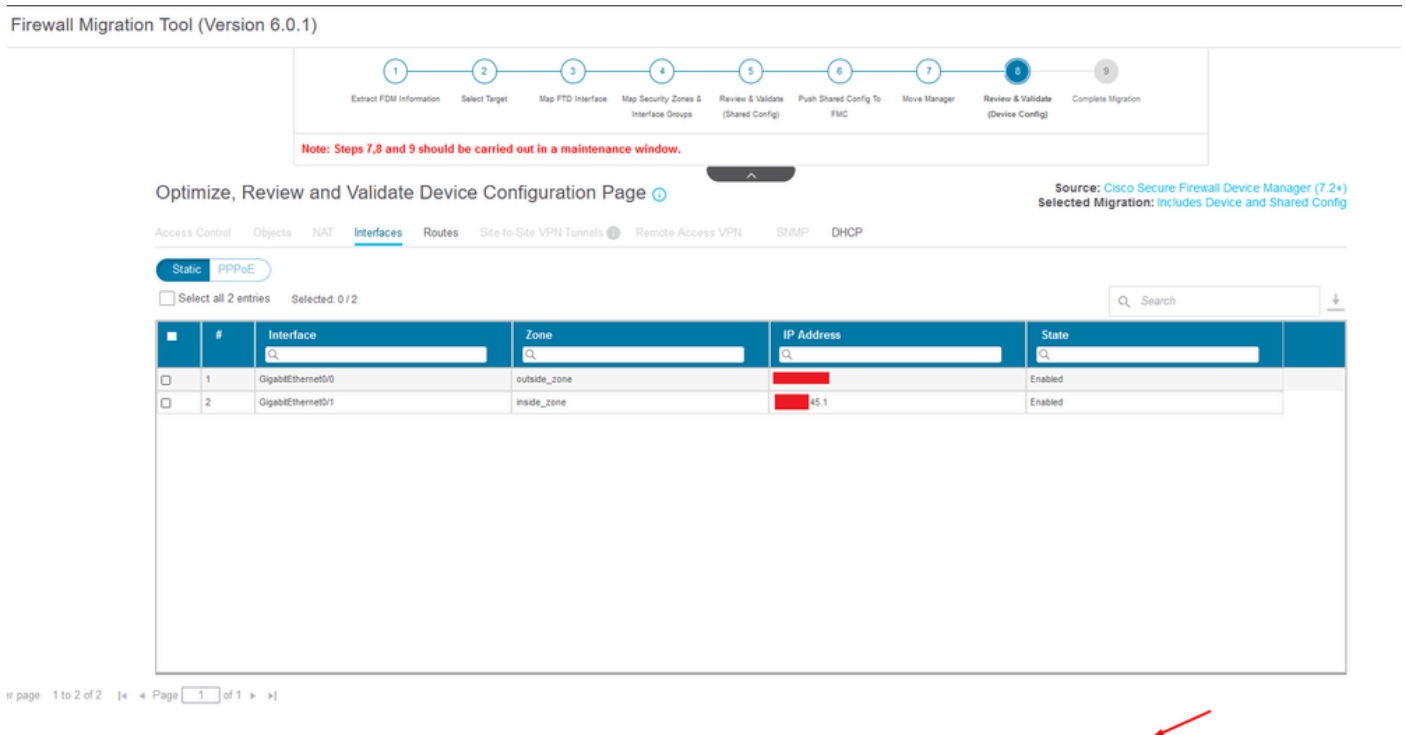
Move Manager

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



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**.



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.

Validation Status

✔ Successfully Validated

Validation Summary (Pre-push)

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

Push Configuration

Validation Status - Push Configuration.

Pop-up window with the percentage pushing configuration.

Firewall Migration Tool (Version 6.0.1)

Complete Migration

Migration Status

Interfaces	✔
Routes	⌚
DHCP	⌚
Policy Assignment	⌚

PUSHING

10% 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. [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.



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

New Migration

Complete Migration

Verify

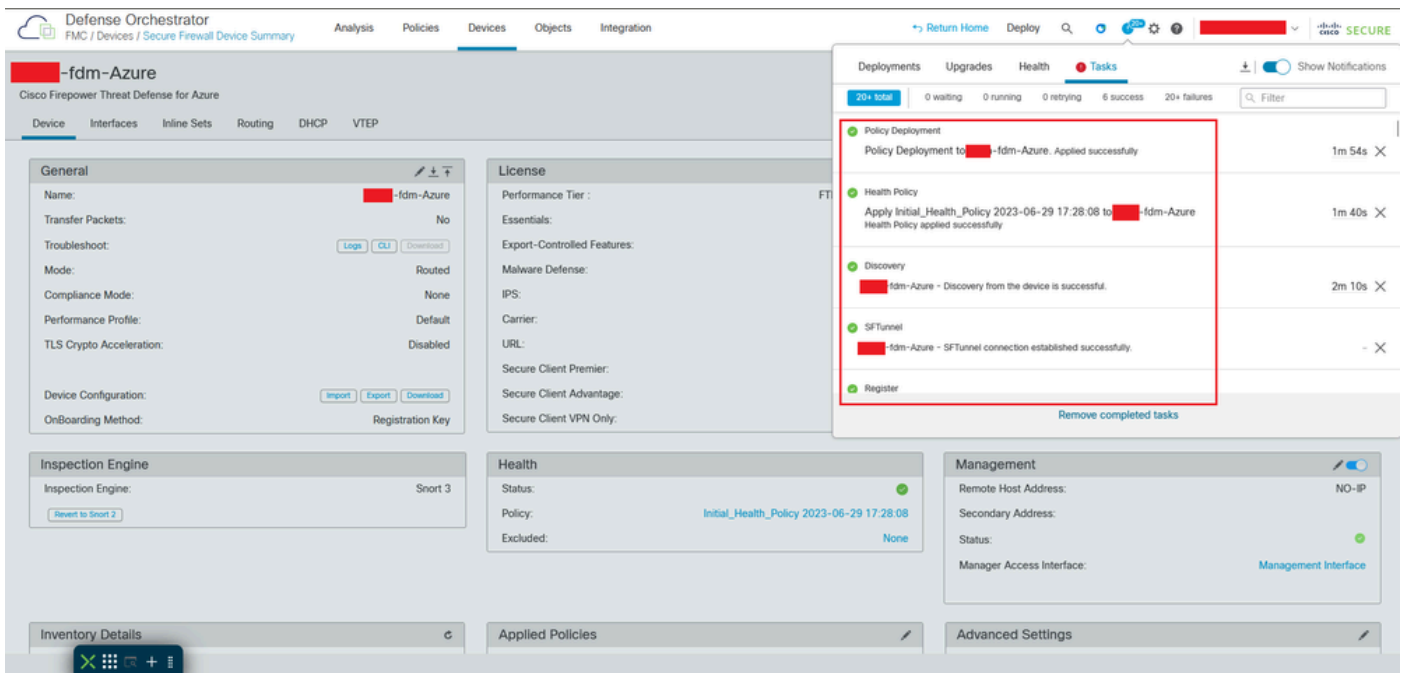
To verify that the FDM has been successfully migrated to the cdFMC.

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

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	-

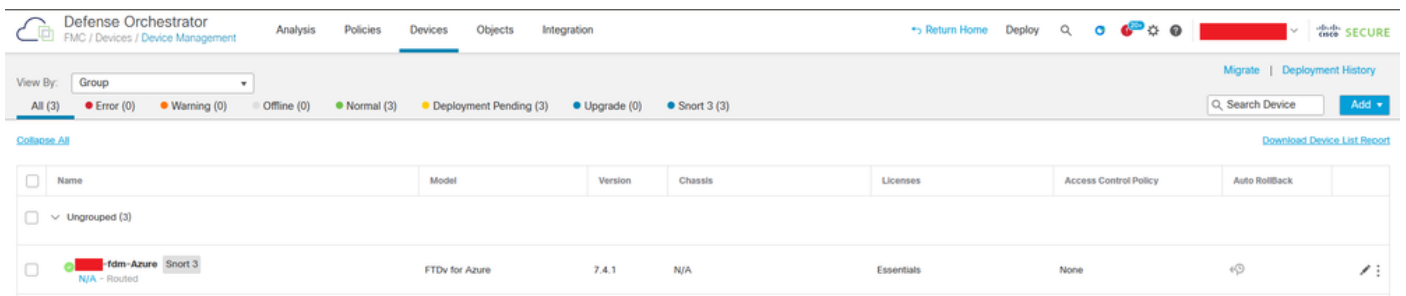
cdFMC Registered Devices

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.



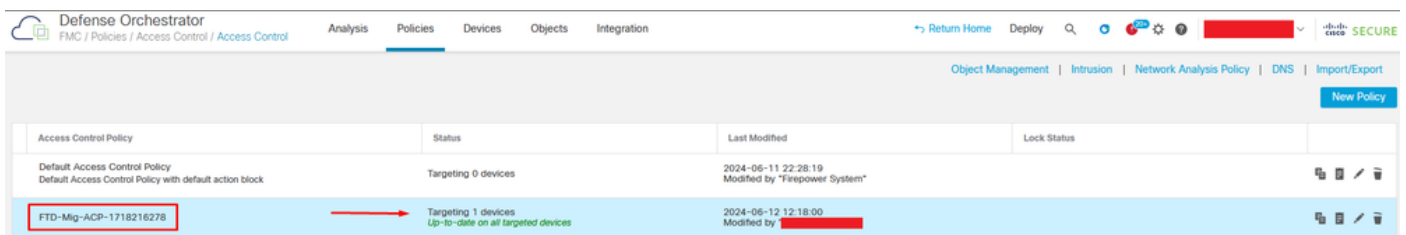
cdFMC Registration Task Completed.

Device is on cdFMC > Device > Device Management.



Device Registered on cdFMC

Access Control Policy migrated under Policies > Access Control.



Migration Policy

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

Network Add Network Filter
 Show Unused Objects

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		

Objects Migrated from FDM to cdFMC

Object Management interfaces Migrated.

Defense Orchestrator
 FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration Return Home Deploy Filter

Interface Add Filter

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	
inside_zone	Security Zone	Routed	
outside_ig	Interface Group	Routed	
outside_zone	Security Zone	Routed	

Object Management Interfaces Migrated.