

Migrer FDM vers cdFMC en utilisant FMT dans CDO

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Configurer](#)

[Vérifier](#)

Introduction

Ce document décrit comment migrer un Firepower Device Manager (FDM) vers le Cloud-Delivered FMC (cdFMC) à l'aide de l'outil de migration Firepower (FMT) dans CDO.

Conditions préalables

Exigences

- Firepower Device Manager (FDM) 7.2+
- Centre de gestion des pare-feu (cdFMC) fourni dans le cloud
- Outil de migration Firepower (FMT) inclus dans CDO

Composants utilisés

Ce document a été créé sur la base des exigences mentionnées ci-dessus.

- Firepower Device Manager (FDM) version 7.4.1
- Centre de gestion des pare-feu (cdFMC) fourni dans le cloud
- 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Les utilisateurs CDO admin peuvent effectuer des migrations de leurs périphériques vers cdFMC lorsque les périphériques sont sur la version 7.2 ou ultérieure. Dans la migration décrite dans ce

document, cdFMC est déjà activé sur le locataire CDO.

Configurer

1.- Activer les services cloud Cisco sur FDM

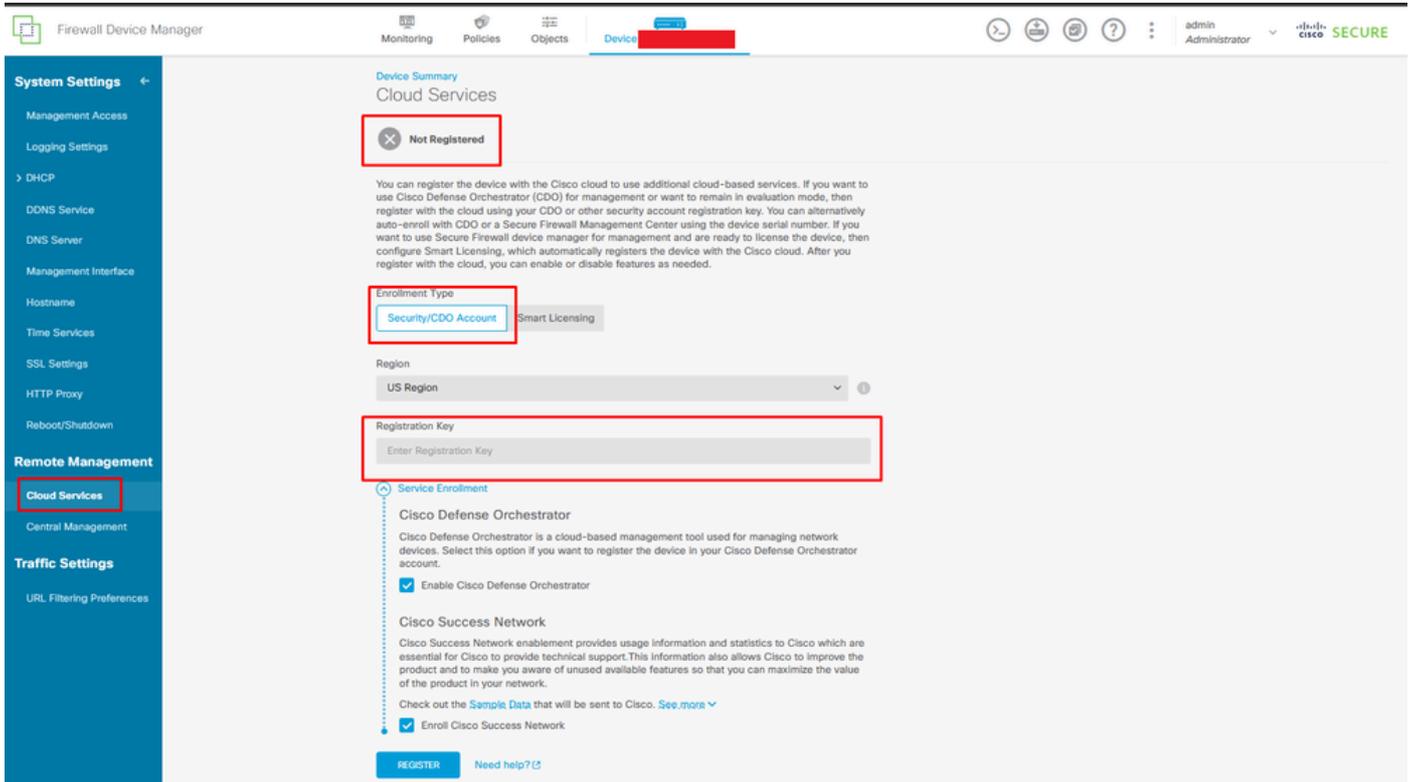
Pour commencer la migration, il est nécessaire d'avoir le périphérique FDM sans déploiements en attente et de s'inscrire aux services cloud. Pour vous inscrire aux services cloud, accédez à Paramètres système > En savoir plus > Services cloud.

Dans la section Cloud Services, vous trouvez que le périphérique n'est pas enregistré, par conséquent, il est nécessaire d'effectuer l'inscription avec le type Security/CDO Account. Vous devez configurer une clé d'enregistrement, puis vous inscrire.

The screenshot displays the Cisco FDM configuration interface. At the top, there are navigation tabs: Monitoring, Policies, Objects, and Device. The 'Device' tab is active, showing a network diagram with an 'Inside Network' connected to a 'Cisco Firepower Threat Defense for Azure' device. The device has interfaces 0/0, 0/1, and MGMT. To the right, there is an 'ISP/WAN/Gateway' connected to an 'Internet' cloud, which includes services like DNS Server, NTP Server, and Smart License. Below the diagram, there are several configuration panels: Interfaces (Management: Unmerged, Enabled 2 of 2), Routing (1 static route), Updates (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), System Settings (Management Access, Logging Settings), Smart License (Registered, Tier: FTDv20 - 3 Gbps), Backup and Restore, Troubleshoot (No files created yet), 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), and Device Administration (Audit Events, Deployment History, Download Configuration). A dropdown menu is open over the System Settings panel, listing options: Management Server / Host, SSL Settings, Cloud Services (highlighted), Service, HTTP Proxy, Reboot/Shutdown of Interface, Central Management, and URL Filtering Preferences.

Services cloud d'inscription

Sur les services cloud, il est indiqué que n'est pas enregistré. Sélectionnez le type d'inscription Compte CDO et fournissez la clé d'inscription de CDO.



Inscription aux services cloud

La clé d'enregistrement se trouve à l'intérieur de CDO. Accédez à CDO, accédez à Inventory > Add symbol.

Un menu apparaît pour sélectionner le type de périphérique dont vous disposez. Sélectionnez l'option FTD. L'option FDM doit être activée ; sinon, la migration correspondante ne peut pas être effectuée. Le type d'enregistrement utilise Utiliser la clé d'enregistrement. Dans cette option, la clé d'enregistrement apparaît à l'étape 3, que nous devons copier et coller dans le FDM.



FDM intégré, ajouter une option

Un menu s'affiche pour sélectionner un périphérique ou un type de service.

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

Sélectionner un périphérique ou un type de service

Pour ce document, l'option Sélectionner la clé d'enregistrement a été sélectionnée.

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.

Type d'enregistrement

Ici, il affiche la clé d'enregistrement nécessaire à l'étape précédente.

Firewall Threat Defense
Management Mode:
 FTD FDM (Recommended)

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

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

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

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

1 Device Name [REDACTED]

2 Database Updates **Enabled**

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

4 Smart License **(Skipped)**

5 Done
Your device is now onboarding.
ⓘ This may take a long time to finish. You can check the status of the device on the Devices and Services page.

Add Labels ⓘ
Add label groups and labels +

Go to Inventory

Processus d'enregistrement

Une fois la clé d'enregistrement obtenue, copiez-la et collez-la dans le FDM, puis cliquez sur Register. Après l'enregistrement du FDM dans les services cloud, il s'affiche comme Enabled comme indiqué dans l'image.

La licence Smart a été ignorée car le périphérique va être enregistré une fois qu'il sera opérationnel.

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

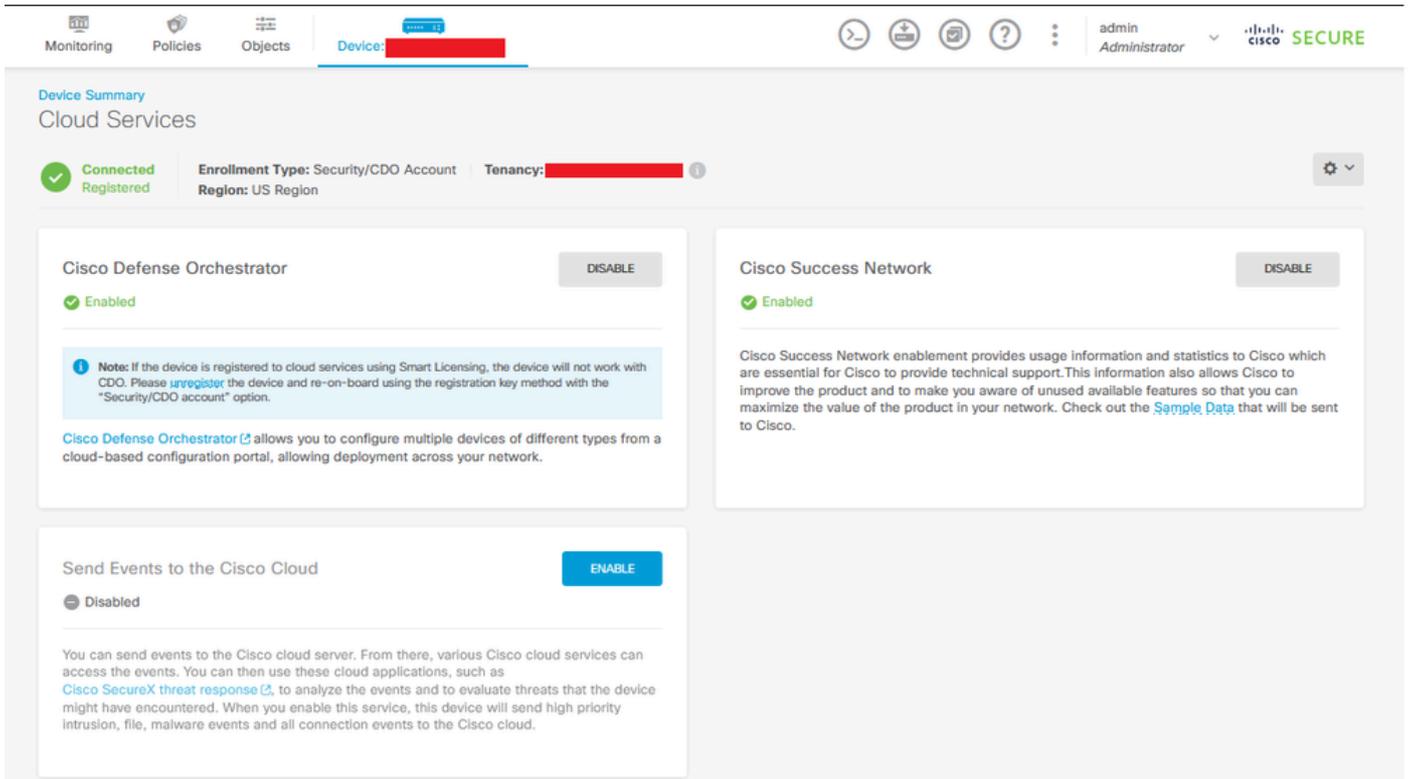
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product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

Check out the [Sample Data](#) that will be sent to Cisco. [See more](#)

Enroll Cisco Success Network

REGISTER

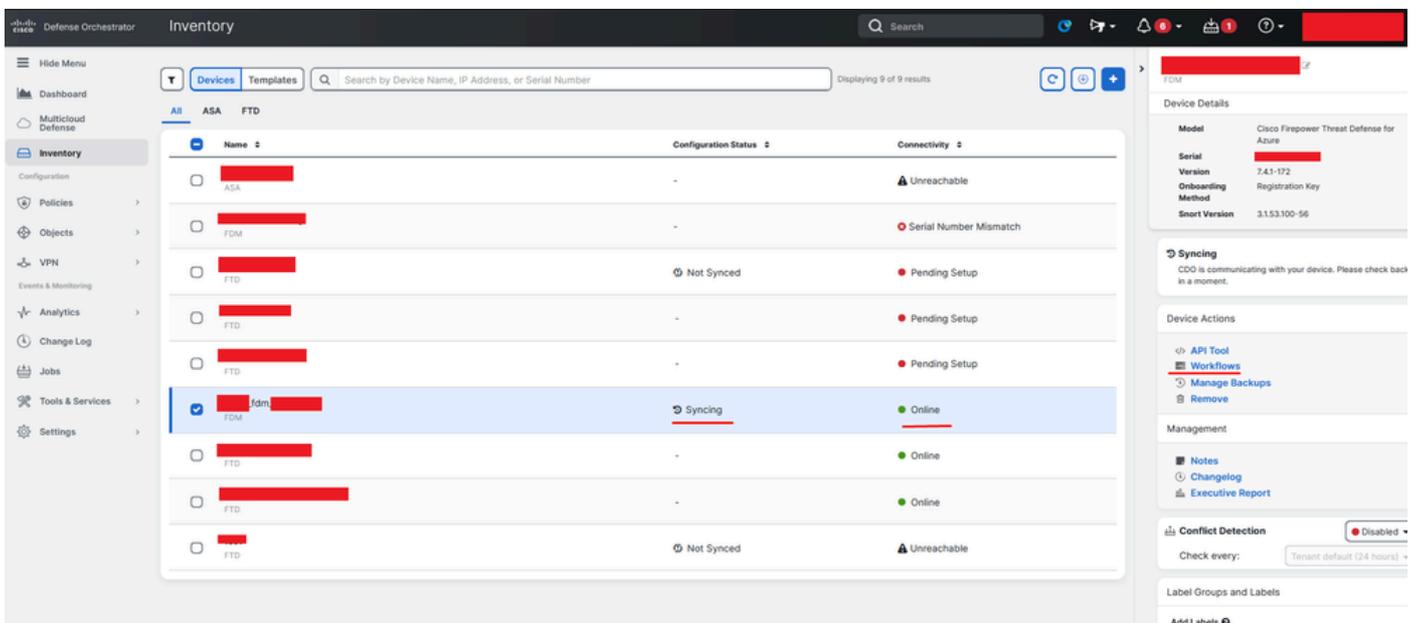
[Need help?](#)



Enregistrement FDM terminé

Dans CDO, dans le menu Inventaire, le FDM est en cours d'intégration et de synchronisation. La progression et le flux de cette synchronisation peuvent être examinés dans la section Workflows.

Une fois ce processus terminé, il s'affiche sous la forme Synchronisé et En ligne.



Inventaire CDO FDM intégré

Lorsque les périphériques ont été synchronisés, ils s'affichent comme Online (En ligne) et Synchronized (Synchronisé).



FDM intégré

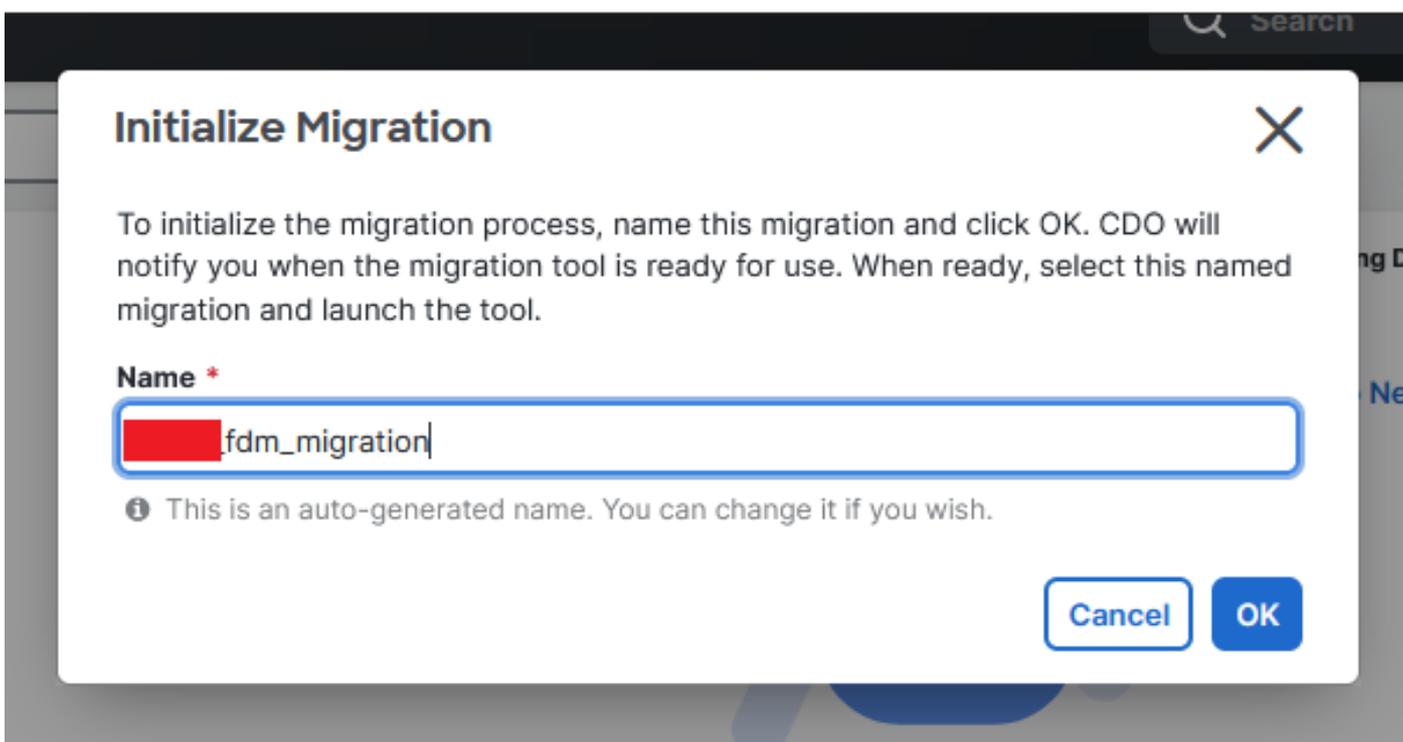
Lorsque le FDM a été correctement intégré à CDO, nous devons nous déconnecter du FDM. Après vous être déconnecté de FDM, naviguez dans CDO vers Tools & Services > Migration > Firewall Migration Tool.



Cliquez sur le symbole Add, et un nom aléatoire apparaît, indiquant que le nom doit être renommé pour lancer le processus de migration.

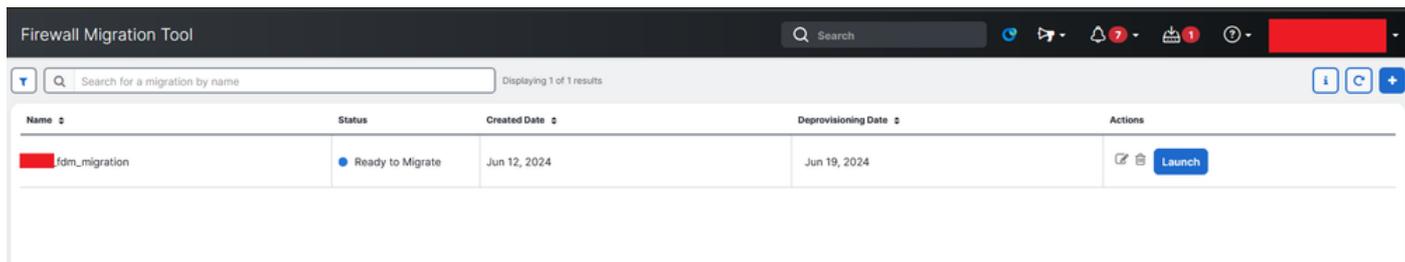


Après avoir renommé, cliquez sur Launch pour commencer la migration.



Initialiser la migration

Cliquez sur Launch pour démarrer la configuration de la migration.



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

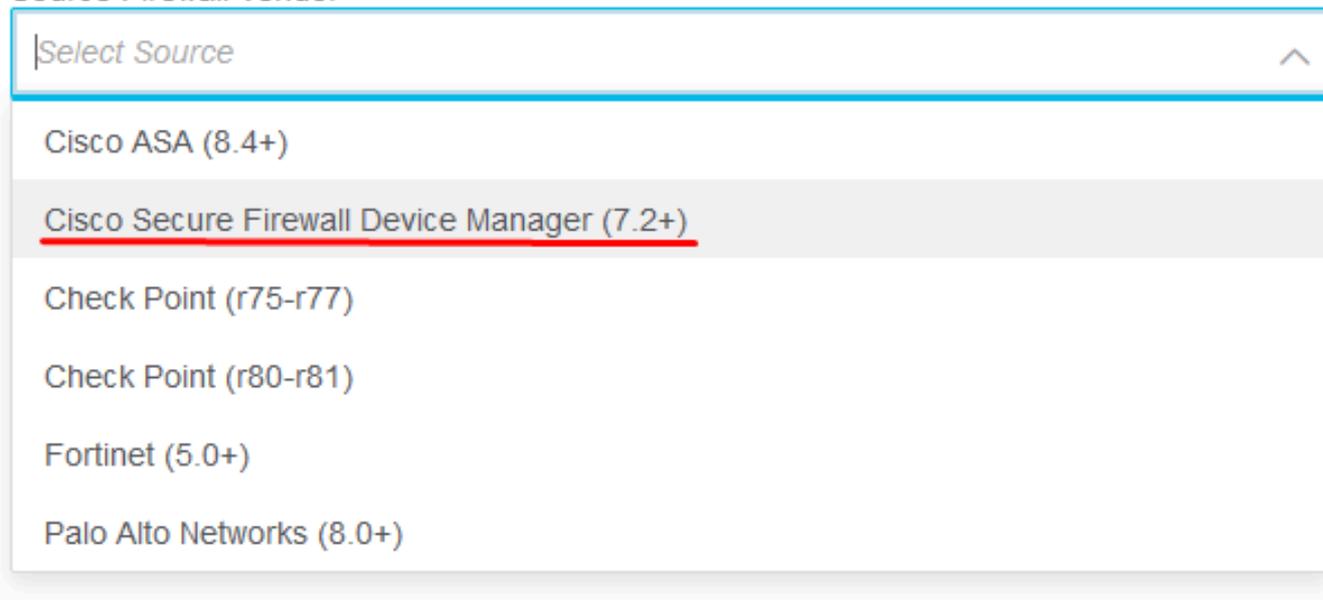
Processus de lancement de la migration

Après avoir cliqué sur Launch, une fenêtre s'ouvre pour le processus de migration où l'option Cisco Secure Firewall Device Manager (7.2+) est sélectionnée. Comme mentionné précédemment, cette option est activée à partir de la 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+)

Configuration source de sélection FMT

Une fois sélectionnées, trois options de migration différentes sont présentées : Configuration partagée uniquement, Inclut les configurations de périphériques et partagées, et Inclut les configurations de périphériques et partagées vers le nouveau matériel FTD.

Dans ce cas, la deuxième option, Migrate Firepower Device Manager (Inclut le périphérique et la configuration partagée), est exécutée.

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 :

Options de migration

Une fois la méthode de migration sélectionnée, sélectionnez le périphérique dans la liste fournie.

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 - Available

Connect

Sélection du périphérique FDM

FDM device config extraction successful

100% Complete

Extraction de la configuration terminée

Il est recommandé d'ouvrir l'onglet situé en haut de la page pour vérifier et comprendre à quelle étape nous sommes lorsque le périphérique a été sélectionné.



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

Extract Cisco Secure Firewall Device Manager (7.2+) Information

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

Extraction Methods >

FDM IP Address:

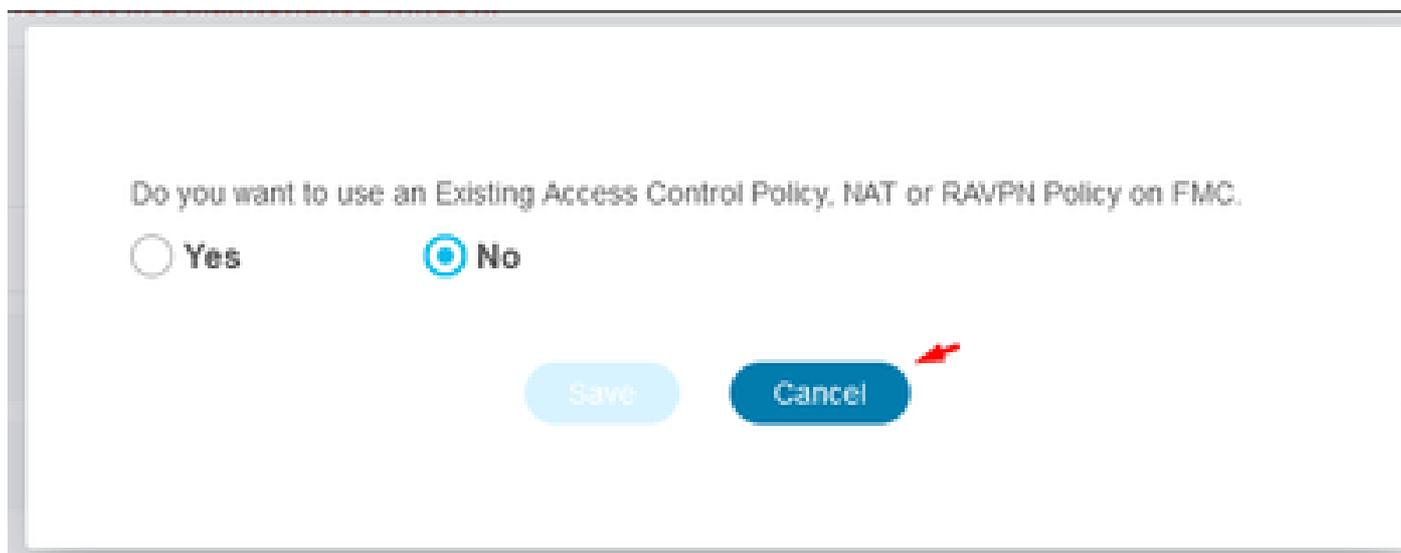
Parsed Summary

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	

Back Next

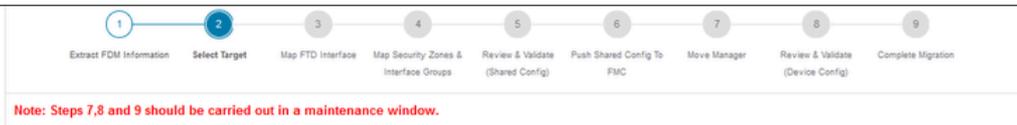
Étapes du processus de migration

En tant que nouvelle migration, sélectionnez Annuler lorsque vous y êtes invité avec l'option « Voulez-vous utiliser une politique de contrôle d'accès, une politique NAT ou RAVPN existante sur FMC ? »



Annuler l'option de configuration existante

Par la suite, il y aura des options pour sélectionner les fonctionnalités à migrer comme indiqué dans l'image. Cliquez sur Continuer.



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.

Fonctionnalités à sélectionner

Puis Lancez La 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

Commencez la conversion.

Une fois le processus d'analyse terminé, deux options peuvent être utilisées : Téléchargez le document et poursuivez la migration en cliquant sur Suivant.

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

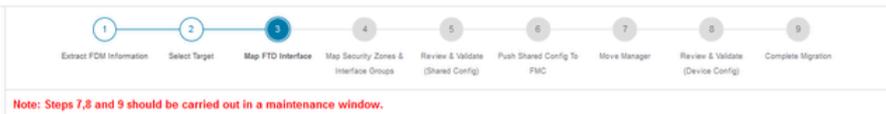
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPI/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)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

Back

Next

Télécharger le rapport.

Les interfaces des périphériques sont définies pour être affichées. Il est conseillé de cliquer sur Refresh pour mettre à jour les interfaces. Une fois la validation effectuée, vous pouvez continuer en cliquant sur Next (Suivant).



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 affichées

Accédez à la section Zones de sécurité et groupes d'interfaces, où vous devez ajouter

manuellement avec Add SZ & IG. Pour cet exemple, Auto-Create a été choisi. Cela permet de générer automatiquement les interfaces au sein du FMC vers lequel vous effectuez la migration. Une fois terminé, cliquez sur le bouton Next (Suivant).

Firewall Migration Tool (Version 6.0.1)

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

Map Security Zones and Interface Groups

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

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

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

Zones de sécurité et groupes d'interfaces

L'option Auto-Create mappe les interfaces FDM aux zones de sécurité FTD existantes et aux groupes d'interfaces dans FMC qui ont le même nom.

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

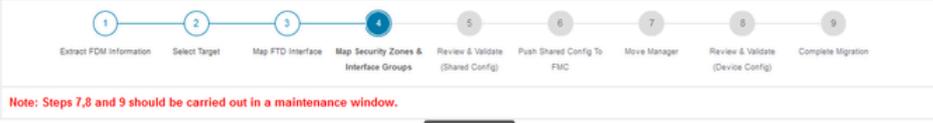
Security Zones Interface Groups

Cancel Auto-Create

Option de création automatique.

Sélectionnez ensuite Suivant.

Firewall Migration Tool (Version 6.0.1)



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

Map Security Zones and Interface Groups 

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

[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) 

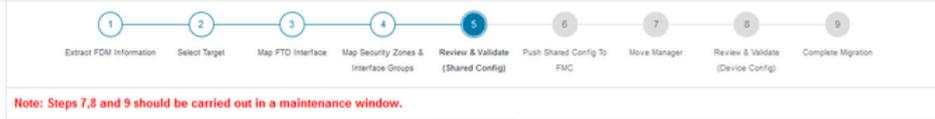
Note: Click on Auto-Create button to auto map the FDM name as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

10  def.p93# 2 |< < Page 1 of 1 > >|

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

Option Après la création automatique.

À l'étape 5, comme indiqué dans la barre supérieure, prenez le temps d'examiner les règles ACP (Access Control Policies), les objets et la NAT. Continuez en examinant attentivement chaque élément, puis cliquez sur Valider pour confirmer qu'il n'y a aucun problème avec les noms ou les 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

Search

#	Name	Validation State	Type	Value
1	OutsidePv4Gateway	Validation pending	Network Object	172.16.1.1
2	OutsidePv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
3	Banned	Validation pending	Network Object	103.104.73.155

Page 1 to 3 of 3 | Page 1 of 1



Contrôle d'accès, objets et configurations NAT

Puis Push Shared Configuration Only

Validation Status

✔ Successfully Validated

Validation Summary (Pre-push)

<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="font-size: 24px; margin: 0;">3</p> <p style="margin: 0;">Access Control List Lines</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="margin: 0;">Not selected for migration</p> <p style="margin: 0;">Access List Objects <small>(Standard, Extended used in BGP/RAVPNEIGRP)</small></p> </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="font-size: 24px; margin: 0;">4</p> <p style="margin: 0;">Network Objects</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="margin: 0;">Not selected for migration</p> <p style="margin: 0;">Port Objects</p> </div>
<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="font-size: 24px; margin: 0;">2</p> <p style="margin: 0;">Network Address Translation</p> </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="margin: 0;">Not selected for migration</p> <p style="margin: 0;">Remote Access VPN <small>(Connection Profiles)</small></p> </div>	<div style="border: 1px solid #ccc; padding: 5px; width: 80%; margin: 0 auto;"> <p style="font-size: 24px; margin: 0;">3</p> <p style="margin: 0;">Access Control Policy Objects <small>(Geo, Application, URL objects and Intrusion Rule Group)</small></p> </div>	

Push Shared Configuration Only

Diffuser la configuration partagée uniquement

Le pourcentage d'achèvement et la tâche spécifique en cours d'exécution peuvent être observés.

Firewall Migration Tool (Version 6.0.1)

Push Shared Config to FMC

Migration Status

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

Please download the Post-Push migration report for a detailed summary. [Download Report](#)

PUSHING

24% Complete

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

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

Pourcentage de poussée

Une fois l'étape 5 terminée, passez à l'étape 6, comme indiqué dans la barre supérieure, où la configuration partagée Push to FMC a lieu. À ce stade, sélectionnez le bouton Next pour avancer.

Firewall Migration Tool (Version 6.0.1)

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

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

Push Shared Config to FMC

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

Migration Status

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

3 Access Control List Lines	Not selected for migration Access List Objects <small>(Standard, Extended used in SDP, SAU/PN/EGRP)</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](#)

Diffusion de la configuration partagée vers FMC terminée

Cette option déclenche un message de confirmation, invitant à poursuivre la migration du manager.

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

Confirmer le gestionnaire de déplacement

La migration du gestionnaire nécessite la présence de l'ID Management Center et de l'ID NAT, ce qui est essentiel. Ces ID peuvent être récupérés en sélectionnant Mettre à jour les détails. Cette action lance une fenêtre contextuelle dans laquelle le nom souhaité pour la représentation FDM dans cdFMC est entré, puis enregistre les modifications.



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

Move Manager

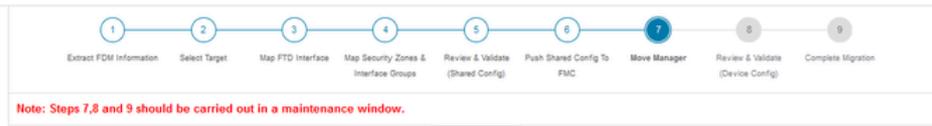
ID du centre de gestion et ID NAT

Mettre à jour le nom du périphérique pour enregistrement.

Après cette action, les ID des champs susmentionnés sont affichés.



Avertissement : n'apportez aucune modification à l'interface Management Center. Par défaut, l'option Management (Gestion) est sélectionnée. Conservez cette option comme paramètre par défaut.



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	us.cdo... ego	856GW 104v	26PM	fdm-Azure	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management Select Data interface

Save

Move Manager

ID du centre de gestion et ID NAT.

Après avoir choisi l'option Update Details, le périphérique qu'il va commencer à synchroniser.

Synchronisation du périphérique FDM

Une fois la migration finalisée, l'étape suivante consiste à examiner les interfaces, les routes et les paramètres DHCP configurés dans le FDM en sélectionnant Valider.



Optimize, Review and Validate Device Configuration Page

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

Static PPPoE

Select all 2 entries Selected: 0 / 2

Search

#	Interface	Zone	IP Address	State
1	GigabitEthernet0/0	outside_zone		Enabled
2	GigabitEthernet0/1	inside_zone	15.1	Enabled

Page 1 to 2 of 2 Page 1 of 1

Validate

Valider les paramètres de configuration FDM

Après la validation, choisissez Push Configuration pour lancer le processus de transmission de la configuration, qui va se poursuivre jusqu'à la fin de la migration. En outre, il est possible de surveiller les tâches en cours d'exécution.

Validation Status

✔ Successfully Validated

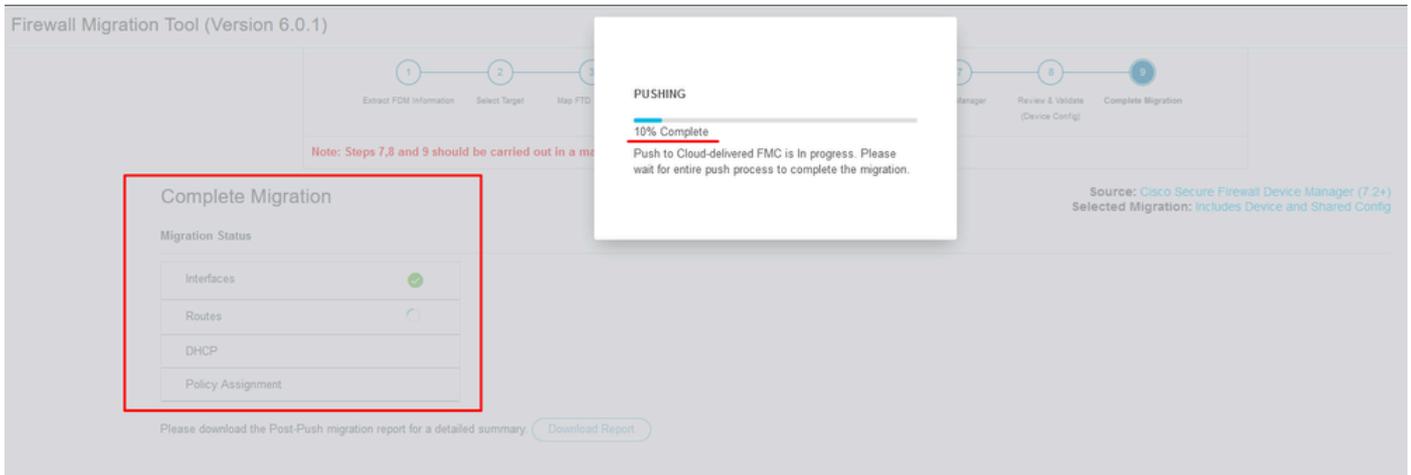
Validation Summary (Pre-push)

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

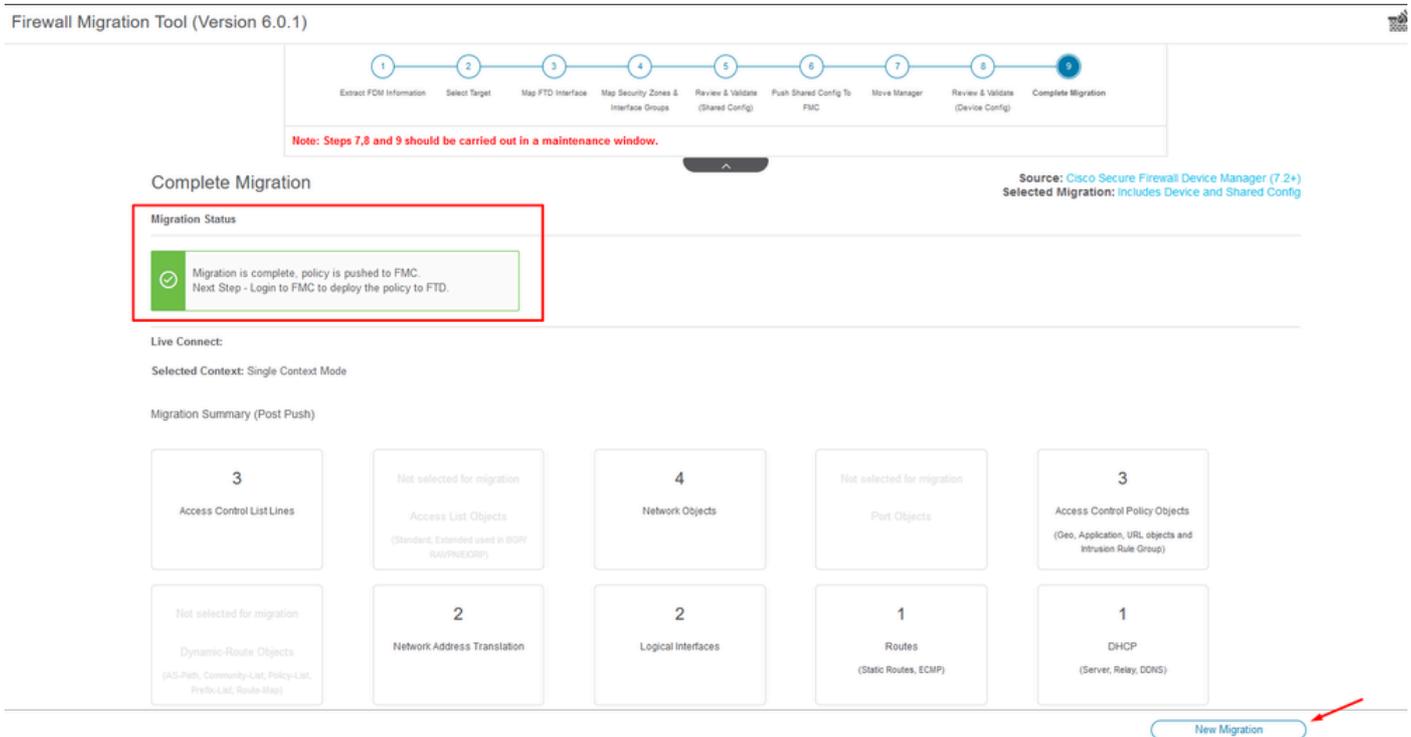
Statut de validation - Configuration push.

Fenêtre contextuelle contenant la configuration de diffusion en pourcentage.



Pourcentage de transmission terminé

Une fois terminé, une option permettant d'initier une nouvelle migration est présentée, marquant la fin du processus de migration de FDM à cdFMC.

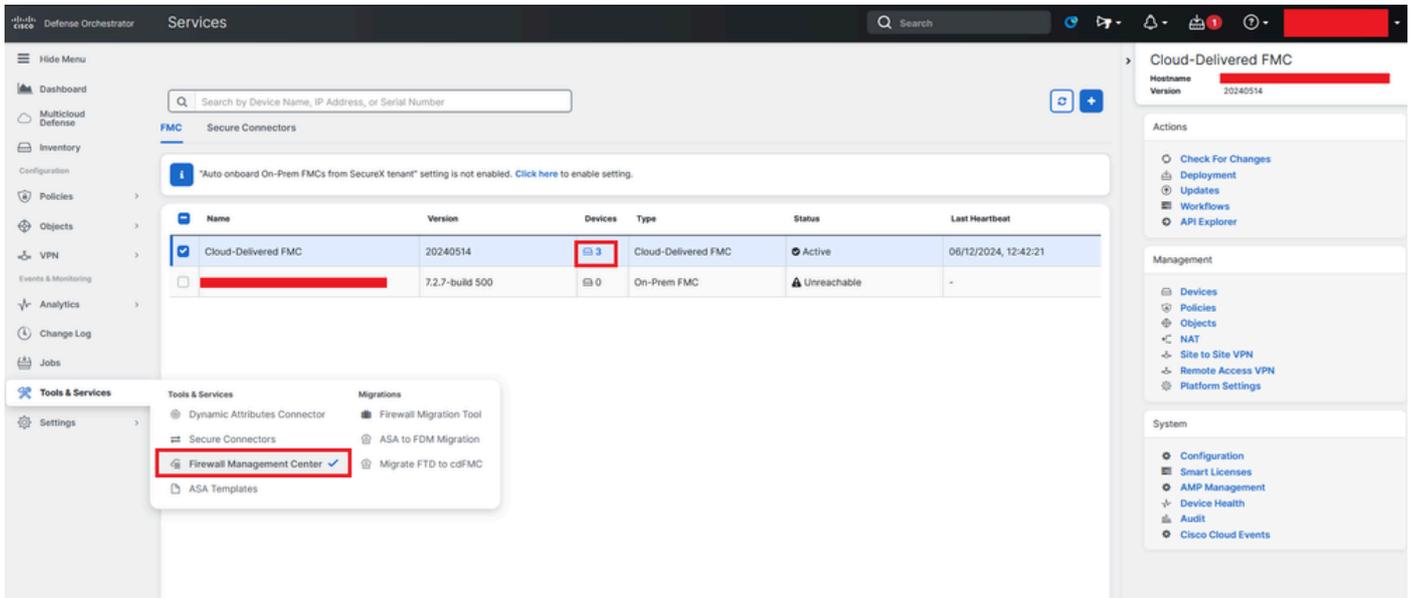


Migration complète

Vérifier

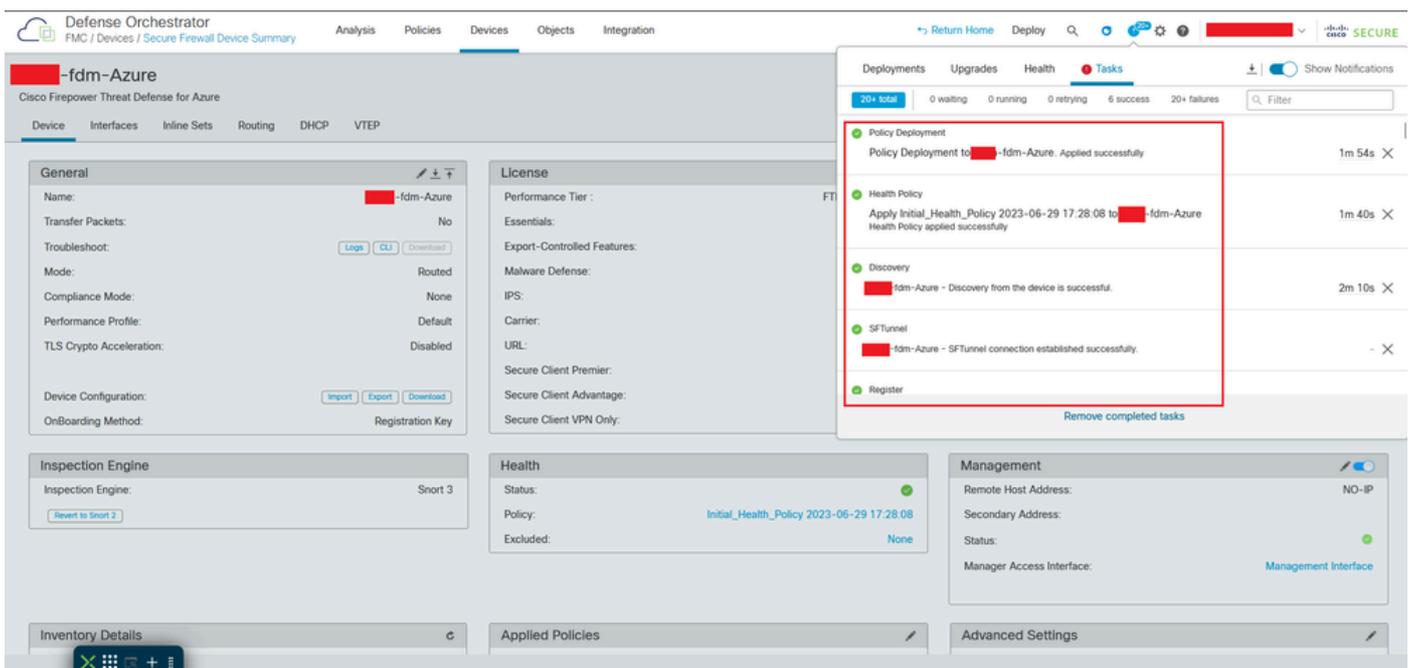
Pour vérifier que le FDM a été correctement migré vers le cdFMC.

Accédez à CDO > Tools & Services > Firepower Management Center. Là, vous constatez que le nombre de périphériques enregistrés a augmenté.



périphériques enregistrés cdFMC

Vérifiez le périphérique dans Périphériques > Gestion des périphériques. En outre, dans les tâches du FMC, vous pouvez trouver quand le périphérique a été correctement enregistré et quand le premier déploiement s'est terminé avec succès.



Tâche d'enregistrement cdFMC terminée.

Le périphérique se trouve sur cdFMC > Device > Device Management.

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

Périphérique enregistré sur cdFMC

Politique de contrôle d'accès migrée sous Politiques > Contrôle d'accès.

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

Politique migratoire

De même, vous pouvez revoir les objets créés dans FDM qui ont été correctement migrés vers cdFMC.

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	

Objets migrés de FDM vers cdFMC

Interfaces de gestion des objets migrées.

Defense Orchestrator
FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration

Return Home Deploy Q Filter

Interface

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

Name	Type	Interface Type	
inside_jg	Interface Group	Routed	
> fdm-Azure			
inside_zone	Security Zone	Routed	
> fdm-Azure			
outside_jg	Interface Group	Routed	
> fdm-Azure			
outside_zone	Security Zone	Routed	
> fdm-Azure			

Interfaces de gestion des objets migrées.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.