

FDM naar CDFMC migreren met FMT binnen CDO

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[Verifiëren](#)

Inleiding

In dit document wordt beschreven hoe u een Firepower Device Manager (FDM) kunt migreren naar een cloudbeheerd FMC (cdFMC) met de Firepower Migration Tool (FMT) in CDO.

Voorwaarden

Vereisten

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

Gebruikte componenten

Dit document is opgesteld op basis van de bovengenoemde vereisten.

- Firepower Device Manager (FDM) in versie 7.4.1
- Cloud-geleverd Firewall Management Center (cdFMC)
- Cloud Defense Orchestrator (CDO)

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Gebruikers van CDO Admin kunnen migraties van hun apparaten naar CDFMC uitvoeren wanneer

de apparaten in versie 7.2 of hoger staan. In de migratie die in dit document wordt beschreven, is cdFMC al ingeschakeld op CDO-huurder.

Configureren

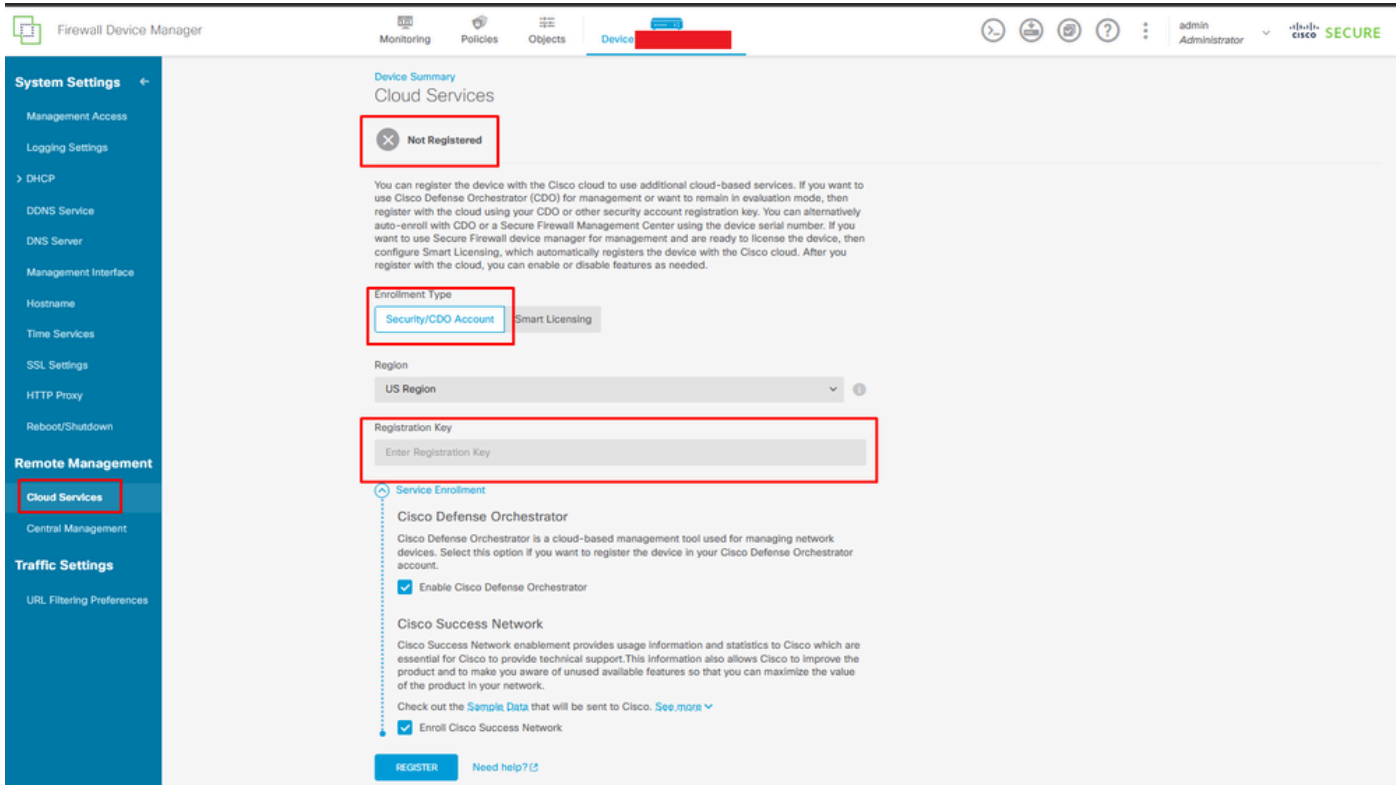
1.- Cisco Cloud-services inschakelen op FDM

Om met de migratie te beginnen, is het nodig om het FDM-apparaat te hebben zonder implementaties die in behandeling zijn en om zich te registreren bij Cloud Services. Om te registreren bij Cloud Services navigeren naar System Settings > See More > Cloud Services.

In het gedeelte Cloud Services vindt u dat het apparaat niet is geregistreerd. Daarom is het noodzakelijk om de inschrijving uit te voeren met het type Security/CDO-account. U moet een registratiesleutel configureren en vervolgens Registreren.

Cloud-services voor registratie

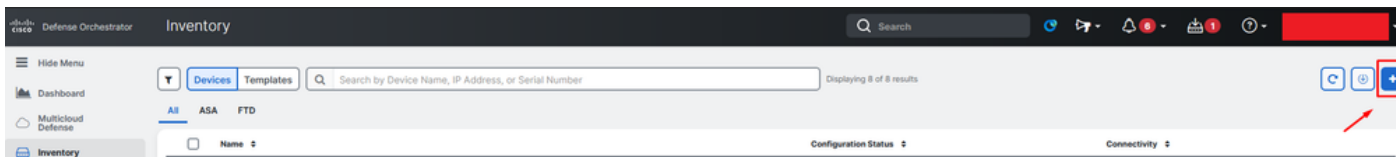
Over Cloud Services is aangetoond dat dit niet is geregistreerd. Selecteer het inschrijvingstype CDO-account en geef de registratiesleutel op via CDO.



Registratie naar cloudservices

De registratiesleutel kan worden gevonden binnen CDO. Navigeer naar CDO, ga naar Inventaris > Toevoegen symbool.

Er verschijnt een menu om het type apparaat te selecteren dat u hebt. Selecteer de FTD-optie. U moet de FDM-optie ingeschakeld hebben; anders kan de corresponderende migratie niet worden uitgevoerd. Het registratietype gebruikt Registratiesleutel gebruiken. In deze optie, verschijnt de Sleutel van de Registratie in stap 3, die wij moeten kopiëren en in FDM klevan.



Aan boord van FDM, voeg optie toe

Er verschijnt een menu om een apparaat- of servicetype te selecteren.

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

Selecteer apparaat- of servicetype

Voor dit document is een registratiesleutel geselecteerd.

Follow the steps below

[Cancel](#)



Firewall Threat Defense

Management Mode:

FTD
(Recommended)

FDM

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.

Registratietype

Hier ziet u de registratiesleutel die u bij de vorige stap nodig hebt.

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

Registratieproces

Nadat de registratiesleutel is verkregen, kopieert en plakt u deze in de FDM en klikt u op Registreren. Na registratie van de FDM binnen Cloud Services wordt deze weergegeven als Ingeschakeld zoals in de afbeelding.

De slimme licentie is overgeslagen, aangezien het apparaat wordt geregistreerd zodra het apparaat in bedrijf is.

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?](#)

FDM-registratie

Bij het registreren van FDM, toont het de Huurdienst, de Cloud-diensten verbonden en geregistreerd.

Device Summary
Cloud Services

Connected Registered
Enrollment Type: Security/CDO Account
Region: US Region
Tenancy: [redacted]

Cisco Defense Orchestrator DISABLE
Enabled

Cisco Success Network DISABLE
Enabled

Send Events to the Cisco Cloud ENABLE
Disabled

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with CDO. Please [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.

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-registratie voltooid

Binnen CDO, in het menu Inventaris, kan FDM in het proces worden gevonden om te worden on-boarded en synchroniseren. De voortgang en het verloop van deze synchronisatie kunnen worden bekeken in het gedeelte Workflows.

Wanneer dit proces is voltooid, wordt het weergegeven als Synced en Online.

Inventory

Displaying 9 of 9 results

Name	Configuration Status	Connectivity
[redacted]	-	Unreachable
[redacted]	-	Serial Number Mismatch
[redacted]	Not Synced	Pending Setup
[redacted]	-	Pending Setup
[redacted]	-	Pending Setup
fdm	Syncing	Online
[redacted]	-	Online
[redacted]	-	Online
[redacted]	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: 3.15.3100-56

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

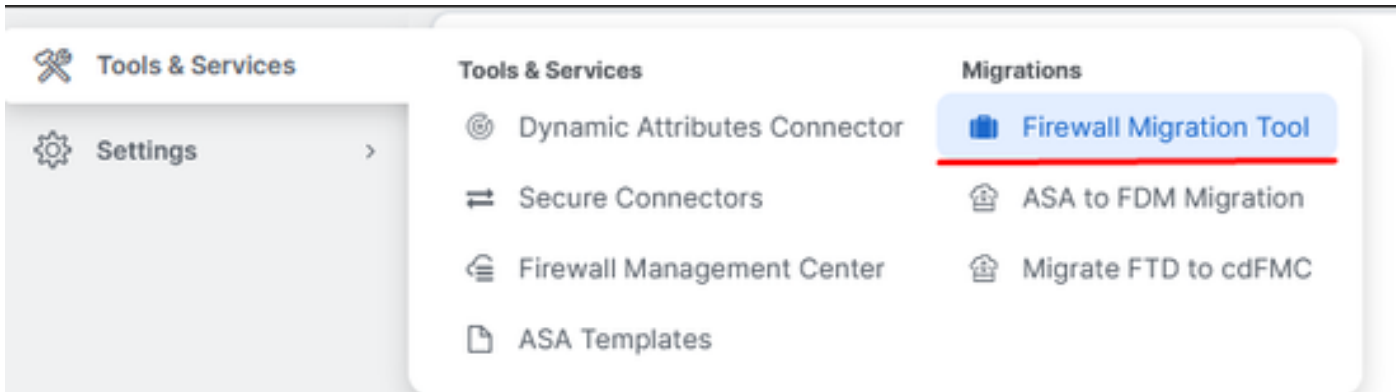
CDO-inventaris FDM onboarded

Wanneer de apparaten zijn gesynchroniseerd, toont het zoals Online en Synced.



FDM onboarded

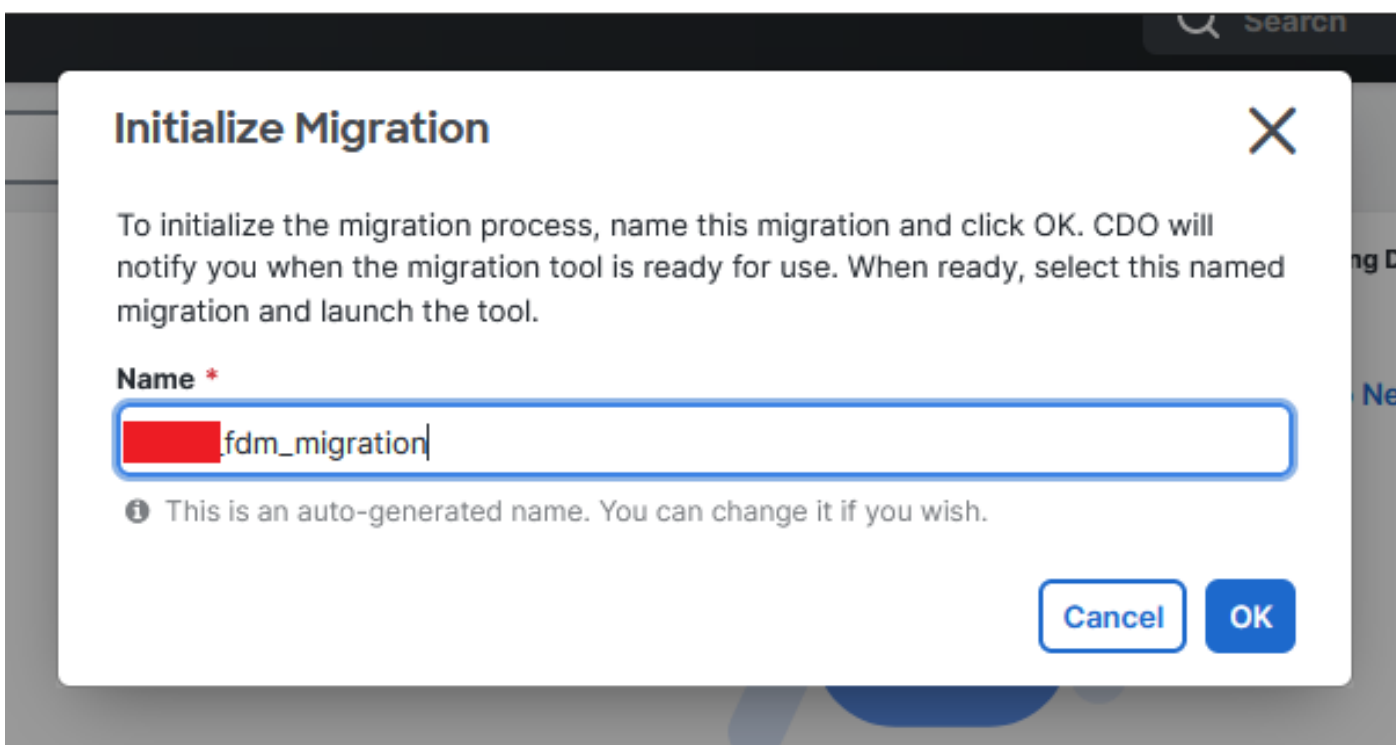
Wanneer de FDM met succes op-boarded aan CDO is geweest, moeten wij uit FDM afloggen. Na het uitloggen van de FDM, navigeer binnen CDO naar Tools & Services > Migratie > Firewall Migration Tool.



Klik op het symbool Toevoegen en er verschijnt een willekeurige naam die aangeeft dat de naam moet worden gewijzigd om het migratieproces te starten.

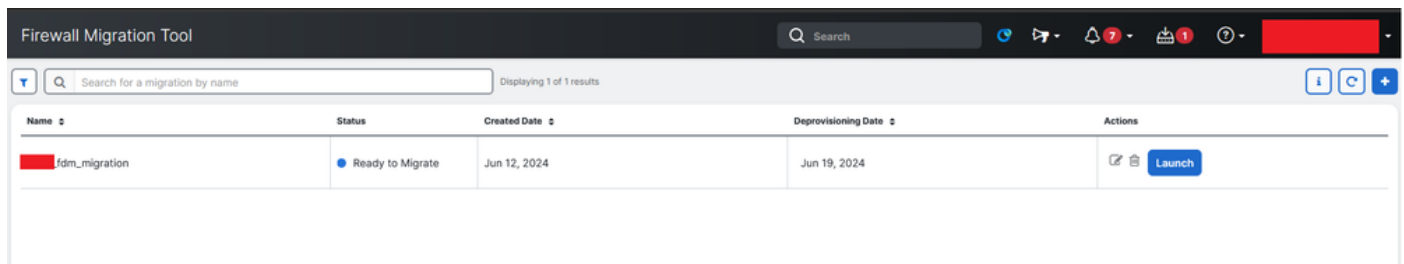


Klik na het hernoemen op Start om de migratie te starten.



Migratie initialiseren

Klik op Start om de migratieconfiguratie te starten.



The screenshot shows the Firewall Migration Tool interface. At the top, there is a search bar and a navigation menu. Below that, a table displays migration details. The table has columns for Name, Status, Created Date, Deprovisioning Date, and Actions. One migration entry is visible with the name 'fdm_migration', status 'Ready to Migrate', created date 'Jun 12, 2024', and deprovisioning date 'Jun 19, 2024'. An action button labeled 'Launch' is present in the Actions column.

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

Start van migratie

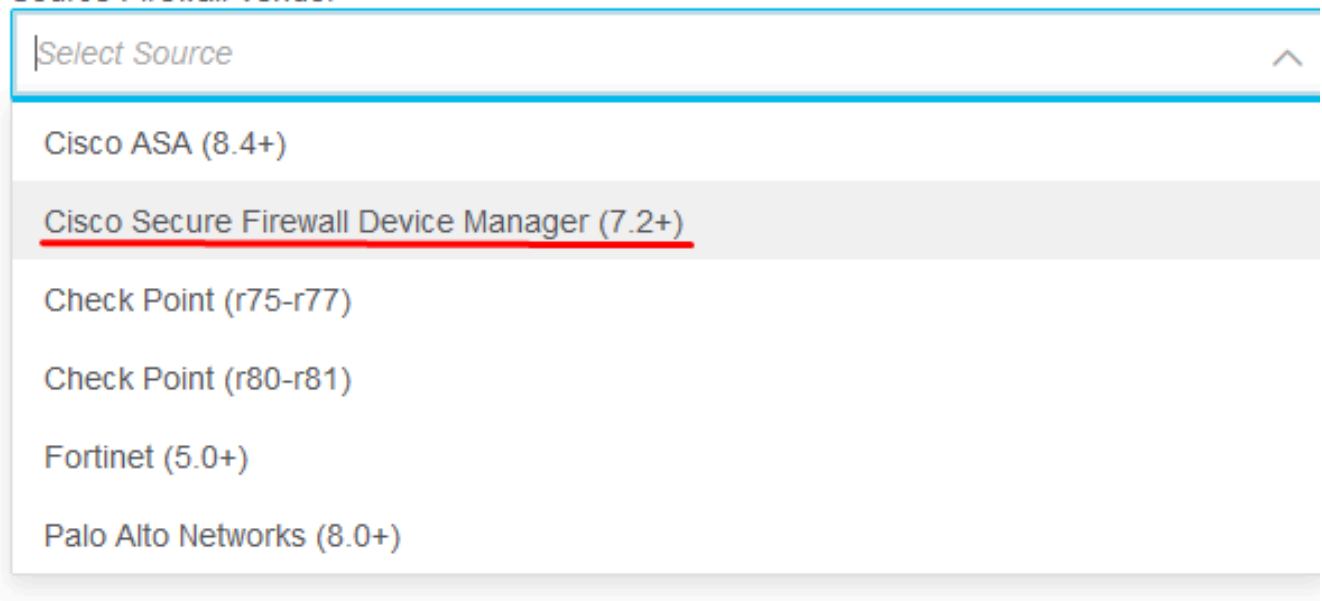
Nadat u op Start hebt geklikt, wordt er een venster geopend voor het migratieproces waarin de optie Cisco Secure Firewall Device Manager (7.2+) is geselecteerd. Zoals eerder vermeld, is deze optie ingeschakeld vanaf versie 7.2.



Firewall Migration Tool (Version 6.0.1)

Select Source Configuration (i)

Source Firewall Vendor



The screenshot shows a dropdown menu for selecting the source firewall vendor. The menu is titled 'Source Firewall Vendor' and contains a search bar with the placeholder text 'Select Source'. Below the search bar, a list of vendors is displayed, with 'Cisco Secure Firewall Device Manager (7.2+)' highlighted in red.

- 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-bronconfiguratie selecteren

Na selectie worden drie verschillende migratieopties gepresenteerd: Alleen gedeelde configuratie, inclusief apparaat- en gedeelde configuraties en inclusief apparaat- en gedeelde configuraties voor FTD New Hardware.

In dit geval wordt de tweede optie, Migrate Firepower Device Manager (inclusief apparaat en gedeelde configuratie), uitgevoerd.

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 :

Migratieopties

Nadat de migratiemethode is geselecteerd, gaat u verder met het selecteren van het apparaat uit de geboden lijst.

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-apparaatselectie

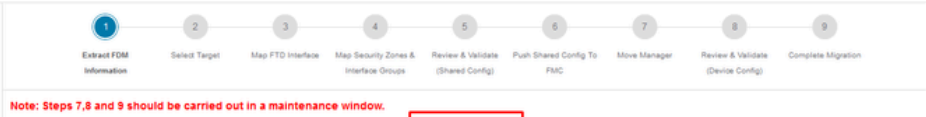
FDM device config extraction successful



100% Complete

Config-extractie voltooid

Het is aan te raden om het tabblad bovenaan te openen om te bekijken en te begrijpen in welke stap we staan wanneer het apparaat is geselecteerd.



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:

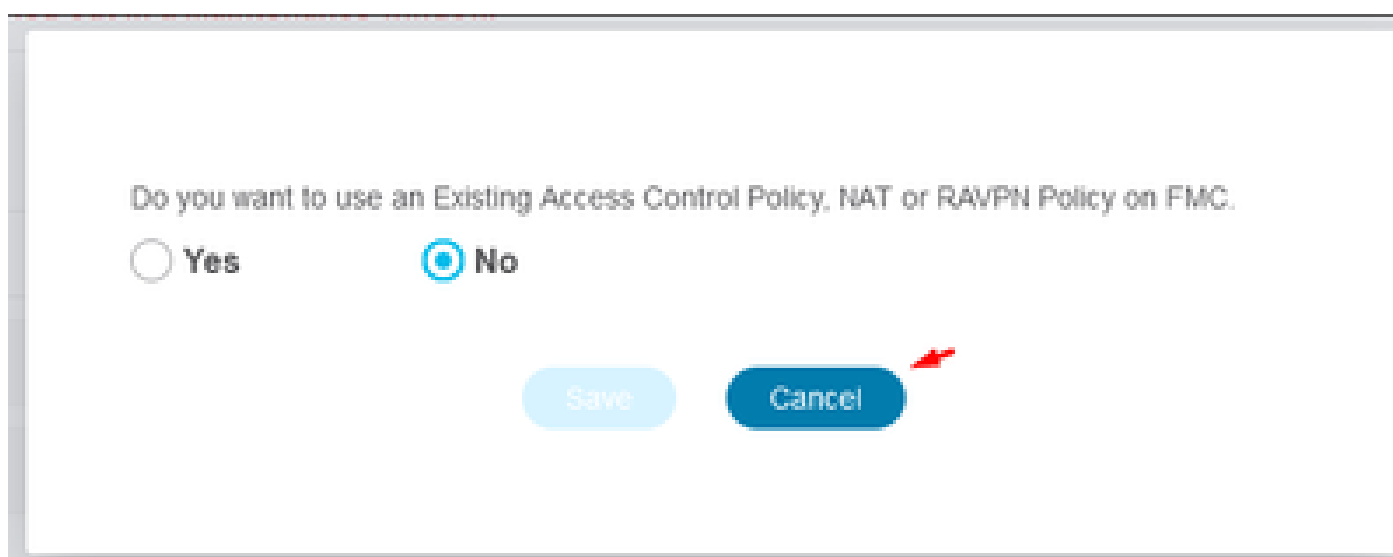
Parsed Summary

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

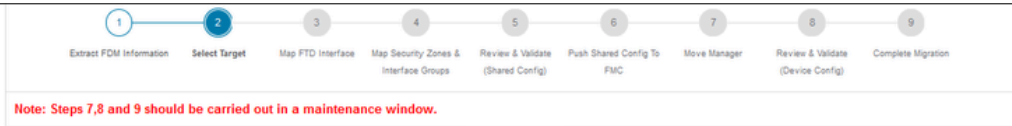
Stappen voor het migratieproces

Aangezien het een nieuwe migratie betreft, selecteert u Annuleren wanneer u hierom wordt gevraagd met de optie "Wilt u een bestaand toegangscontrolebeleid, NAT- of RAVPN-beleid op FMC gebruiken?"



Optie voor bestaande configuratie annuleren

Daarna zullen er opties zijn om de te migreren functies te selecteren zoals in de afbeelding. Klik op Doorgaan.



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 ⓘ

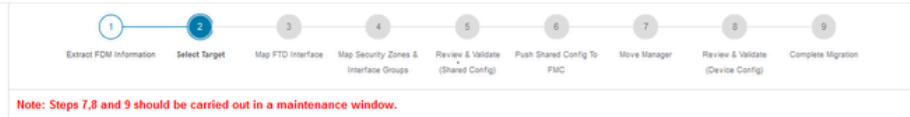
Proceed ➔

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

Te selecteren functies

Start vervolgens de conversie.

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 de conversie.

Nadat het parseren is voltooid, kunnen twee opties worden gebruikt: Download het document en ga door met de migratie door op Volgende te klikken.

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

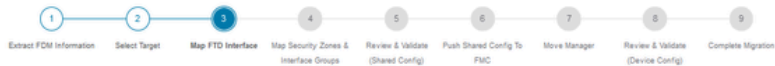
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPM/EGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)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

Rapport downloaden.

De apparaatinterfaces zijn ingesteld om te worden weergegeven. Als beste praktijk, is het raadzaam om te klikken verfrissen om de interfaces bij te werken. Nadat u deze optie hebt gevalideerd, kunt u op Volgende klikken.



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

Weergegeven interfaces

Navigeer naar het gedeelte Security Zones en interfacegroepen, waar u handmatig moet

toevoegen met Add SZ & IG. Voor dit voorbeeld is Auto-Create gekozen. Dit helpt om automatisch de interfaces te genereren binnen het VCC waarnaar u migreert. Klik na het voltooiën op de knop Volgende.

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.

Security zones en interfacegroepen

Auto-Create optie brengt FDM-interfaces in kaart aan bestaande FTD Security Zones en interfacegroepen in FMC die dezelfde naam hebben.

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

Optie automatisch maken

Selecteer vervolgens Volgende.

Firewall Migration Tool (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 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 page 2 Page 1 of 1

Back Next

Na de optie Automatisch maken.

In stap 5, zoals in de bovenste balk, neemt u de tijd om het toegangscontrolebeleid (ACS), de objecten en de NAT-regels te onderzoeken. Ga verder door elk item zorgvuldig te bekijken en klik vervolgens op Valideren om te bevestigen dat er geen problemen zijn met namen of configuraties.

Firewall Migration Tool (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 should be carried out in a maintenance window.

Optimize, Review and Validate Shared Configuration Only

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

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

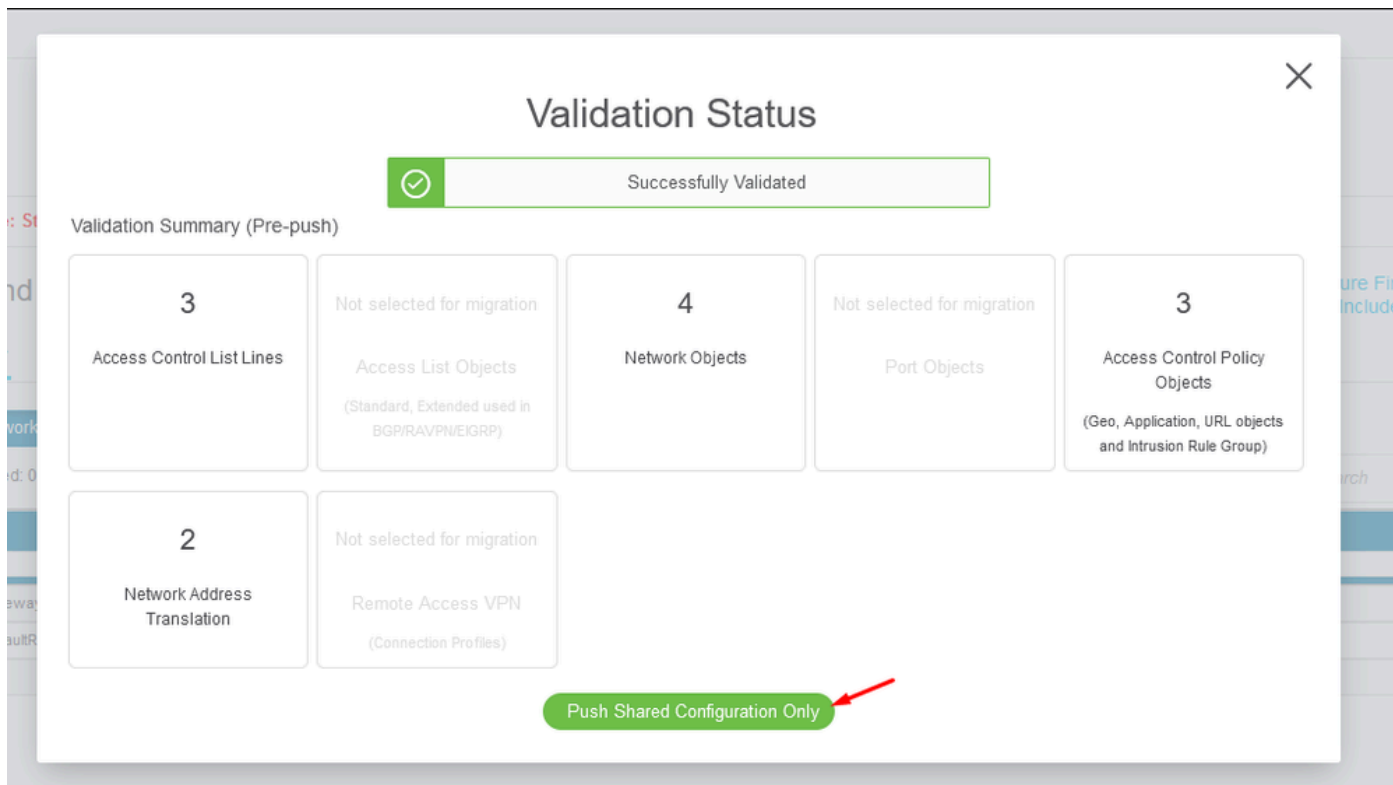
Select all 3 entries Selected: 0/3 Actions Save Search

#	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

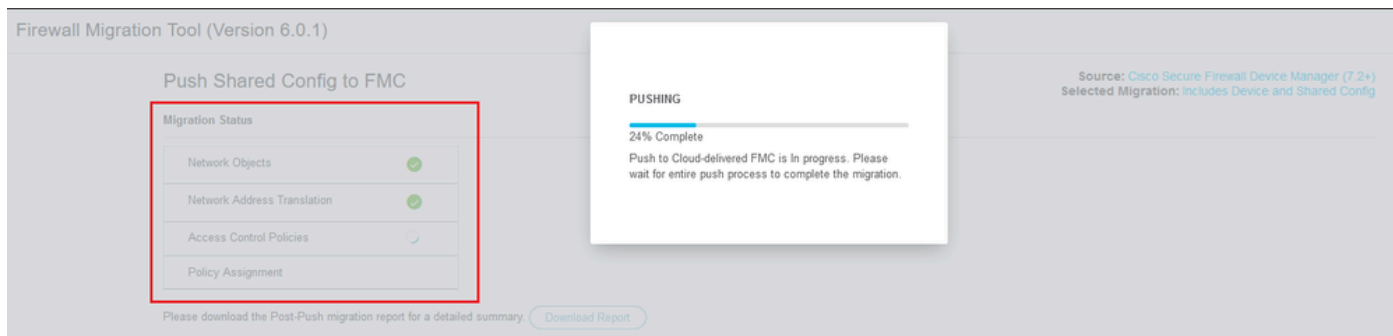
Validate

Alleen gedeelde configuratie in-/uitschakelen



Alleen gedeelde configuratie onder druk

Het voltooiingspercentage en de specifieke taak waaraan gewerkt wordt, zijn zichtbaar.



Percentage duwen

Na voltooiing van stap 5 gaat u verder met stap 6, zoals weergegeven in de bovenbalk, waar de Push Shared Configuration naar FMC plaatsvindt. Selecteer nu de knop Volgende om verder te gaan.



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

Duw gedeelde configuratie naar VCC voltooid

Deze optie brengt een bevestigingsbericht teweeg, verwijzend naar de voortzetting van de manager migratie.

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.

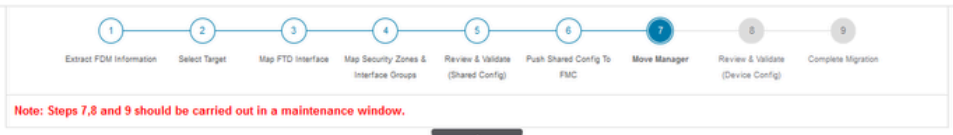
I acknowledge all the steps mentioned above have been completed.

Proceed

Cancel

Verplaatsingsbeheer bevestigen

Voor het doorlopen van de migratie van managers is het nodig dat het Management Center ID en NAT ID bij de hand zijn, wat essentieel is. Deze ID's kunnen worden hersteld door Details bijwerken te selecteren. Deze actie initieert een pop-up venster waar de gewenste naam voor de FDM vertegenwoordiging binnen CDFMC wordt ingevoerd, gevolgd door het opslaan van de wijzigingen.



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

Move Manager

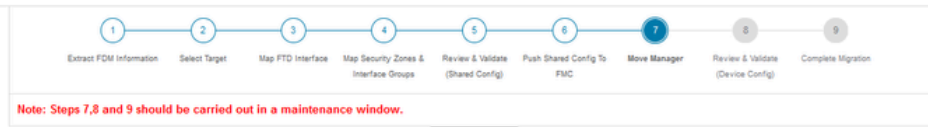
Manager Center-id en NAT-id

Apparaatnaam voor registratie bijwerken.

Na deze actie worden de ID's voor de bovengenoemde velden weergegeven.



Waarschuwing: breng geen wijzigingen aan in de Management Center-interface. Standaard wordt de beheeroptie geselecteerd. Laat deze optie als de standaardinstelling staan.



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	26PMT	fdm-Azure	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management Select Data interface

Save

Move Manager

ID van beheercentrum en NAT-id.

Nadat u de optie Details bijwerken hebt gekozen, wordt het apparaat gesynchroniseerd.

on Tool (Version 6.0.1)

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

SYNCING the FDM Device

9% Complete

FDM-apparaat synchroniseren

Nadat de migratie is voltooid, is de volgende stap om de interfaces, routes en DHCP-instellingen te onderzoeken die in de FDM zijn geconfigureerd door Validate te selecteren.



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

#	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



FDM-instellingen valideren

Na bevestiging, kies Push Configuration om het configuratie duwproces te initiëren, dat gaat verder tot de migratie eindigt. Daarnaast is het mogelijk om de taken die worden uitgevoerd te controleren.

Validation Status

✔ Successfully Validated

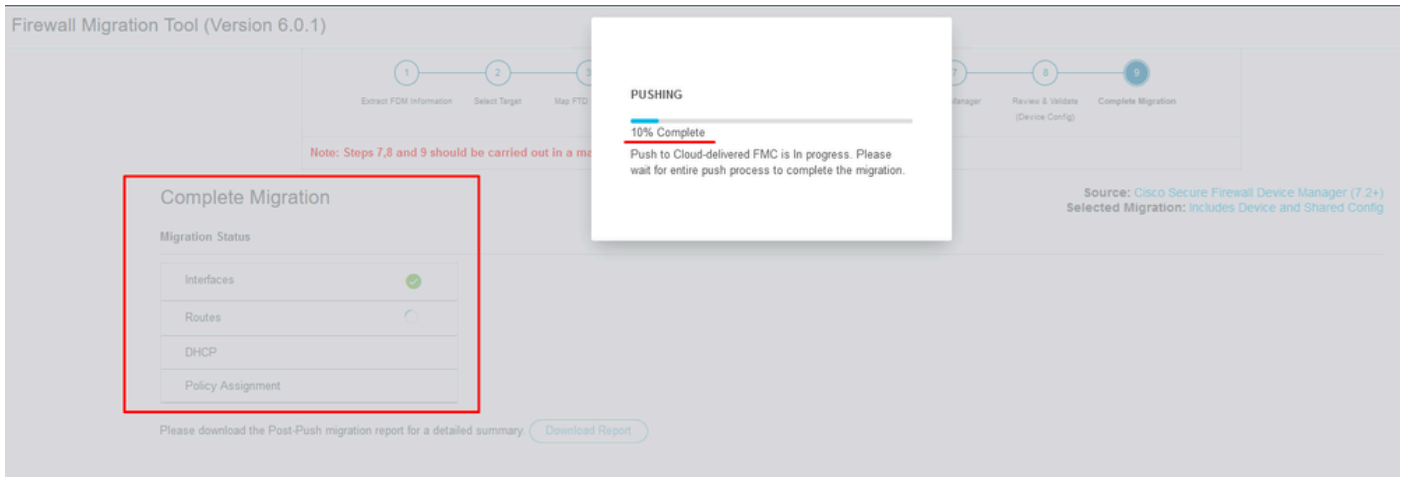
Validation Summary (Pre-push)

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

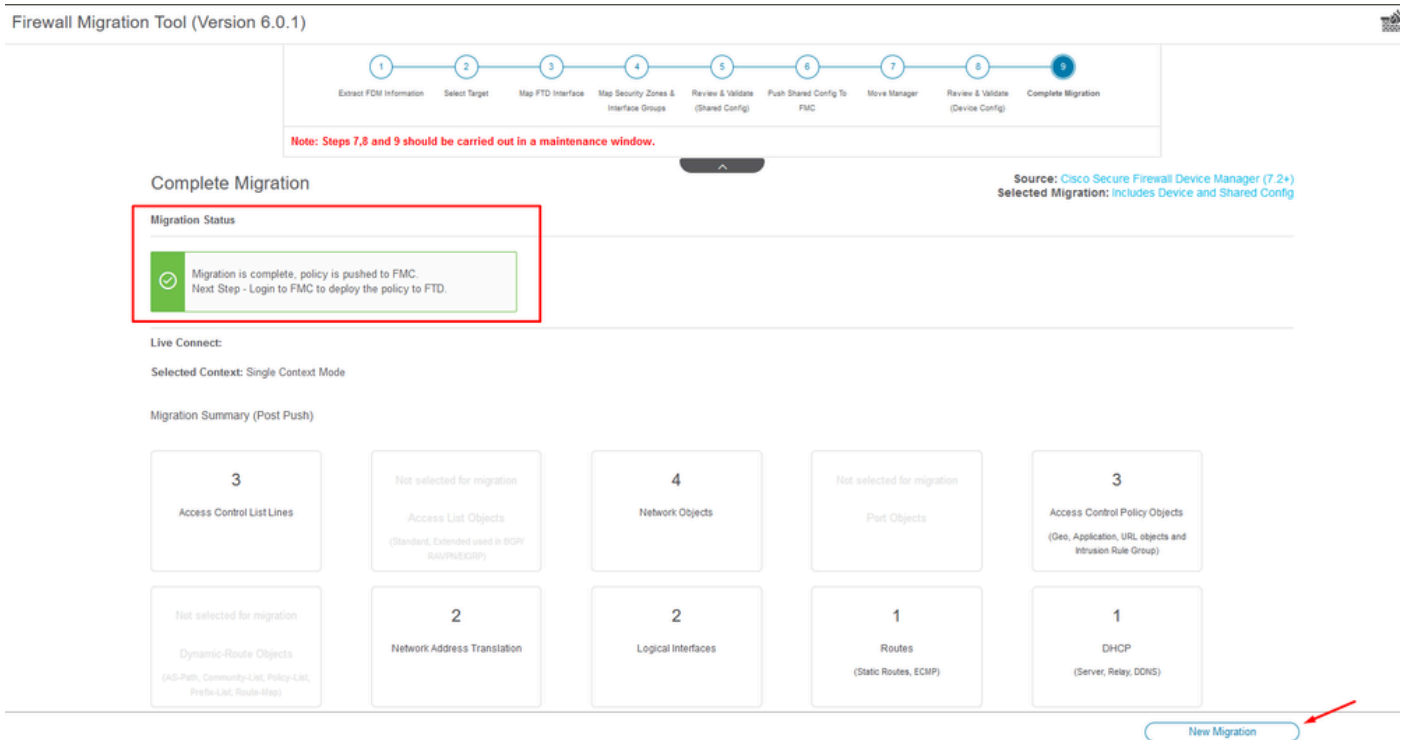
Validatiestatus - Push Configuration.

Pop-up venster met de percentage het duwen configuratie.



Percentage omlaag drukken voltooid

Na voltooiing wordt een optie voor het initiëren van een nieuwe migratie gepresenteerd, waarmee het einde van het migratieproces van FDM naar CDFMC wordt gemarkeerd.

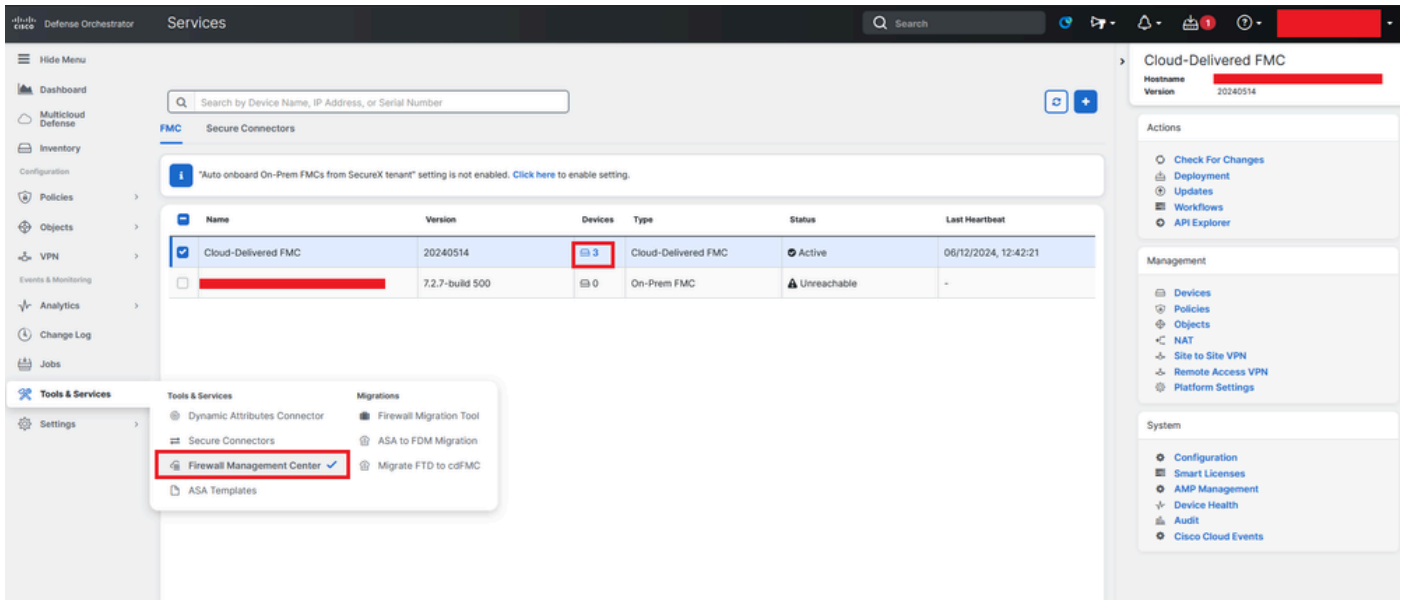


Volledige migratie

Verifiëren

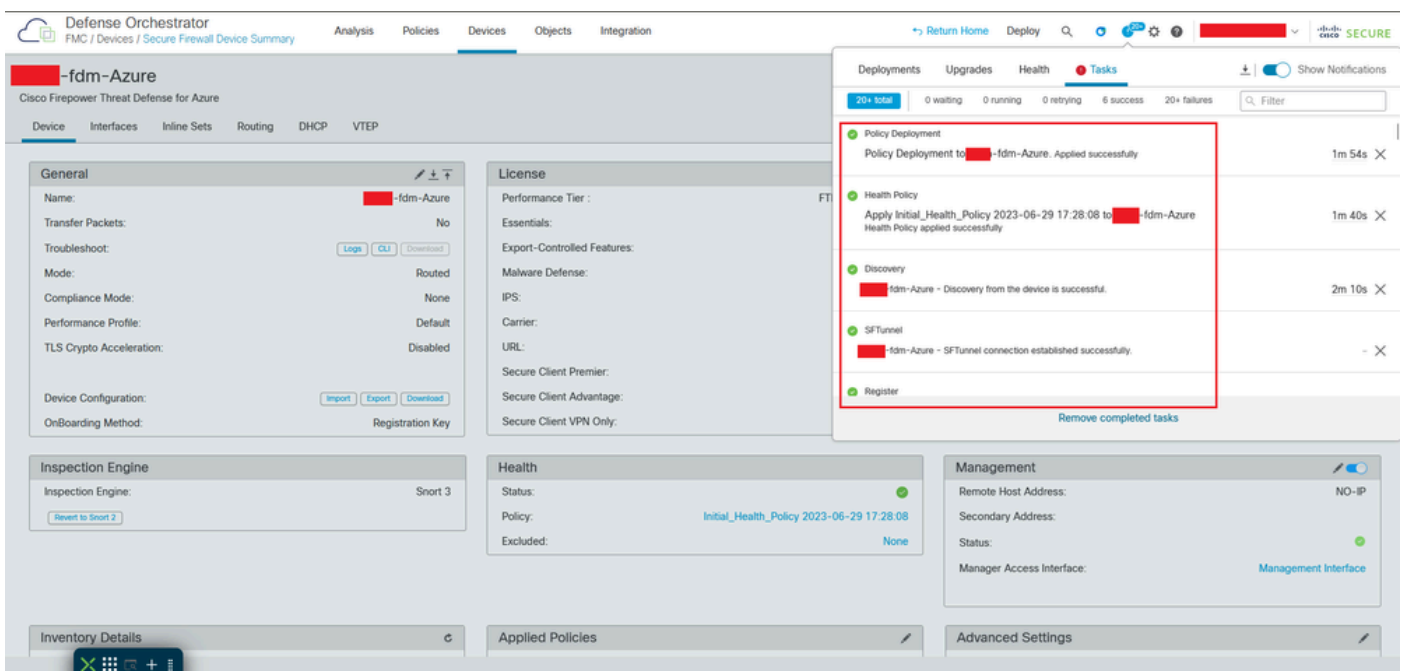
Om te verifiëren dat de FDM met succes naar de CVT is gemigreerd.

Ga naar CDO > Tools & Services > Firepower Management Center. Daar ziet u dat het aantal geregistreerde apparaten is toegenomen.



CDFMC-geregistreerde apparaten

Controleer het apparaat in Apparaten > Apparaatbeheer. Bovendien kunt u binnen de taken van het VCC vinden wanneer het apparaat met succes is geregistreerd en de eerste inzet met succes is voltooid.



Registratietaak voor cdFMC voltooid.

Het apparaat staat op CDFMC > Apparaat > Apparaatbeheer.

Defense Orchestrator
FMC / Devices / Device Management

Analysis Policies Devices Objects Integration

Return Home Deploy Search

View By: Group

All (3) Error (0) Warning (0) Offline (0) Normal (3) Deployment Pending (3) Upgrade (0) Short 3 (3)

Search Device Add

Download Device List Report

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	

Apparaat geregistreerd op CDFMC

Toegangsbeheer Beleid gemigreerd onder Beleid > Toegangsbeheer.

Defense Orchestrator
FMC / Policies / Access Control / Access Control

Analysis Policies Devices Objects Integration

Return Home Deploy Search

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

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

Migratiebeleid

Op dezelfde manier kunt u de in de FDM gemaakte objecten die correct naar de cdFMC zijn gemigreerd, bekijken.

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	

Objecten gemigreerd van FDM naar CDFMC

Objectbeheerinterfaces gemigreerd.

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_ig	Interface Group	Routed	
> fdm-Azure			
inside_zone	Security Zone	Routed	
> fdm-Azure			
outside_ig	Interface Group	Routed	
> fdm-Azure			
outside_zone	Security Zone	Routed	
> fdm-Azure			

Objectbeheerinterfaces gemigreerd.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.