

Migración de FDM a cdFMC mediante FMT en CDO

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Verificación](#)

Introducción

Este documento describe cómo migrar un administrador de dispositivos Firepower (FDM) a un FMC distribuido en la nube (cdFMC) mediante la herramienta de migración de Firepower (FMT) en CDO.

Prerequisites

Requirements

- Firepower Device Manager (FDM) 7.2+
- Centro de gestión de firewall en la nube (cdFMC)
- Herramienta de migración de Firepower (FMT) incluida en CDO

Componentes Utilizados

Este documento fue creado sobre la base de los requisitos mencionados.

- Firepower Device Manager (FDM) en la versión 7.4.1
- Centro de gestión de firewall en la nube (cdFMC)
- Orquestador de defensa de la nube (CDO)

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Los usuarios administradores de CDO pueden realizar migraciones de sus dispositivos a cdFMC cuando los dispositivos están en la versión 7.2 o superior. En la migración descrita en este documento, cdFMC ya está habilitado en el arrendatario CDO.

Configurar

1.- Habilitar servicios en la nube de Cisco en FDM

Para comenzar la migración, es necesario tener el dispositivo FDM sin implementaciones pendientes y registrarse en Cloud Services. Para registrarse en Cloud Services, navegue hasta System Settings > See More > Cloud Services.

Dentro de la sección Servicios en la nube, usted encuentra que el dispositivo no está registrado, por lo tanto, es necesario realizar la inscripción con el tipo de cuenta de seguridad/CDO. Debe configurar una clave de registro y, a continuación, Registrar.

The screenshot displays the Cisco FDM web interface. At the top, there are navigation tabs: Monitoring, Policies, Objects, and Device. The 'Device' tab is active, showing a summary for a Cisco Firepower Threat Defense for Azure device. Key details include: Model (Cisco Firepower Threat Defense for Azure), Software (7.4.1-172), VDB (376.0), and Intrusion Rule Update (20231011-1536). The Cloud Services status is 'Connected | SEC TAC', and High Availability is 'Not Configured'. A 'CONFIGURE' button is visible.

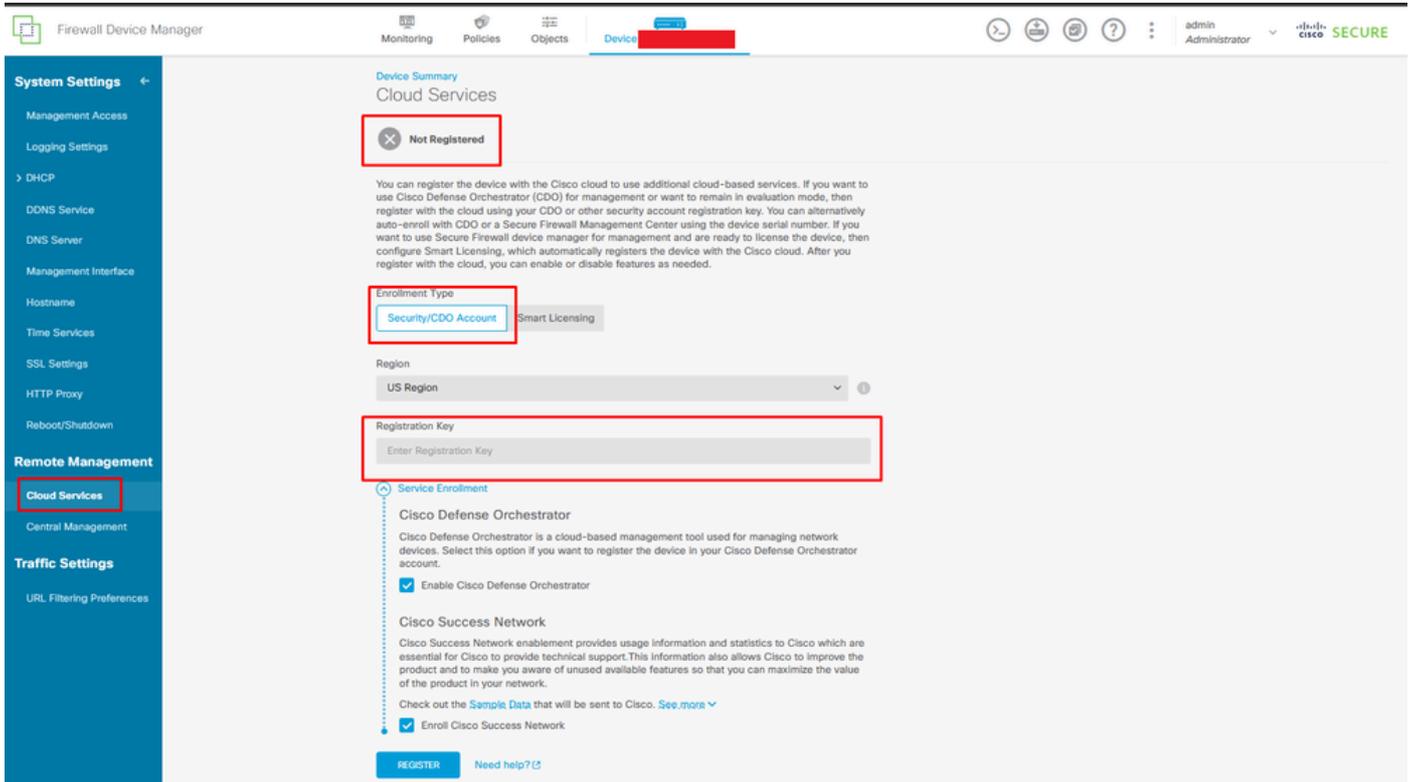
Below the summary is a network diagram showing the device connected to an 'Inside Network' and an 'ISP/WAN/Gateway'. The device has ports labeled O/1 and O/0. To the right, there are icons for Internet, DNS Server, NTP Server, and Smart License.

The main content area is a grid of configuration cards:

- Interfaces:** Management: Unmerged, Enabled 2 of 2. View All Interfaces.
- Smart License:** Registered, Tier: FTDv20 - 3 Gbps. View Configuration.
- Site-to-Site VPN:** There are no connections yet. View Configuration.
- Routing:** 1 static route. View Configuration.
- Backup and Restore:** View Configuration.
- Remote Access VPN:** Requires Secure Client License, No connections | 1 Group Policy. Configure.
- Updates:** Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds. View Configuration.
- Troubleshoot:** No files created yet. REQUEST FILE TO BE CREATED.
- Advanced Configuration:** Includes: FlexConfig, Smart CLI. View Configuration.
- System Settings:** Management Access, Logging Settings, **Cloud Services** (highlighted), HTTP Proxy, Reboot/Shutdown Interface, Central Management, URL Filtering Preferences. See more.
- Device Administration:** Audit Events, Deployment History, Download Configuration. View Configuration.

Registro Servicios en la nube

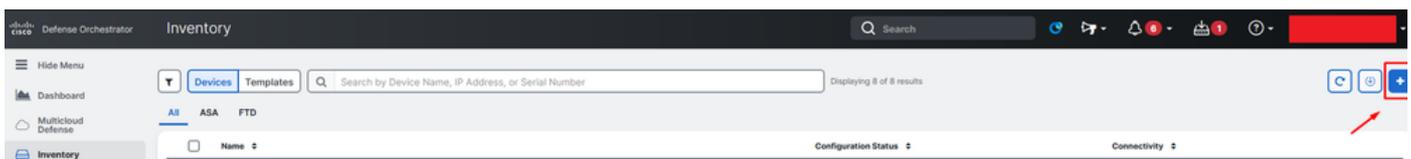
A través de los servicios en la nube se muestra que no está registrado. Seleccione el tipo de inscripción de cuenta CDO y proporcione la clave de registro de CDO.



Registro en servicios en la nube

La clave de registro se puede encontrar dentro de CDO. Vaya a CDO, vaya a Inventario > Agregar símbolo.

Aparece un menú para seleccionar el tipo de dispositivo que tiene. Seleccione la opción FTD. Debe tener activada la opción FDM; de lo contrario, no se podrá realizar la migración correspondiente. El tipo de registro utiliza Use Registration Key. En esta opción, la clave de registro aparece en el paso número 3, que debemos copiar y pegar en FDM.



FDM integrado, añadir opción

Aparecerá un menú para seleccionar un tipo de dispositivo o servicio.

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

Seleccione el tipo de dispositivo o servicio

Para este documento, se ha seleccionado Select Registration Key .

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.

Tipo de registro

Aquí se muestra la clave de registro necesaria en el paso anterior.

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

Proceso de registro

Una vez obtenida la clave de registro, cópiela y péguela en FDM y haga clic en Register (Registrar). Después de registrar el FDM en los servicios en la nube, se muestra como Habilitado, como se muestra en la imagen.

Se ha omitido la licencia inteligente, ya que el dispositivo se va a registrar una vez que esté en funcionamiento.

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

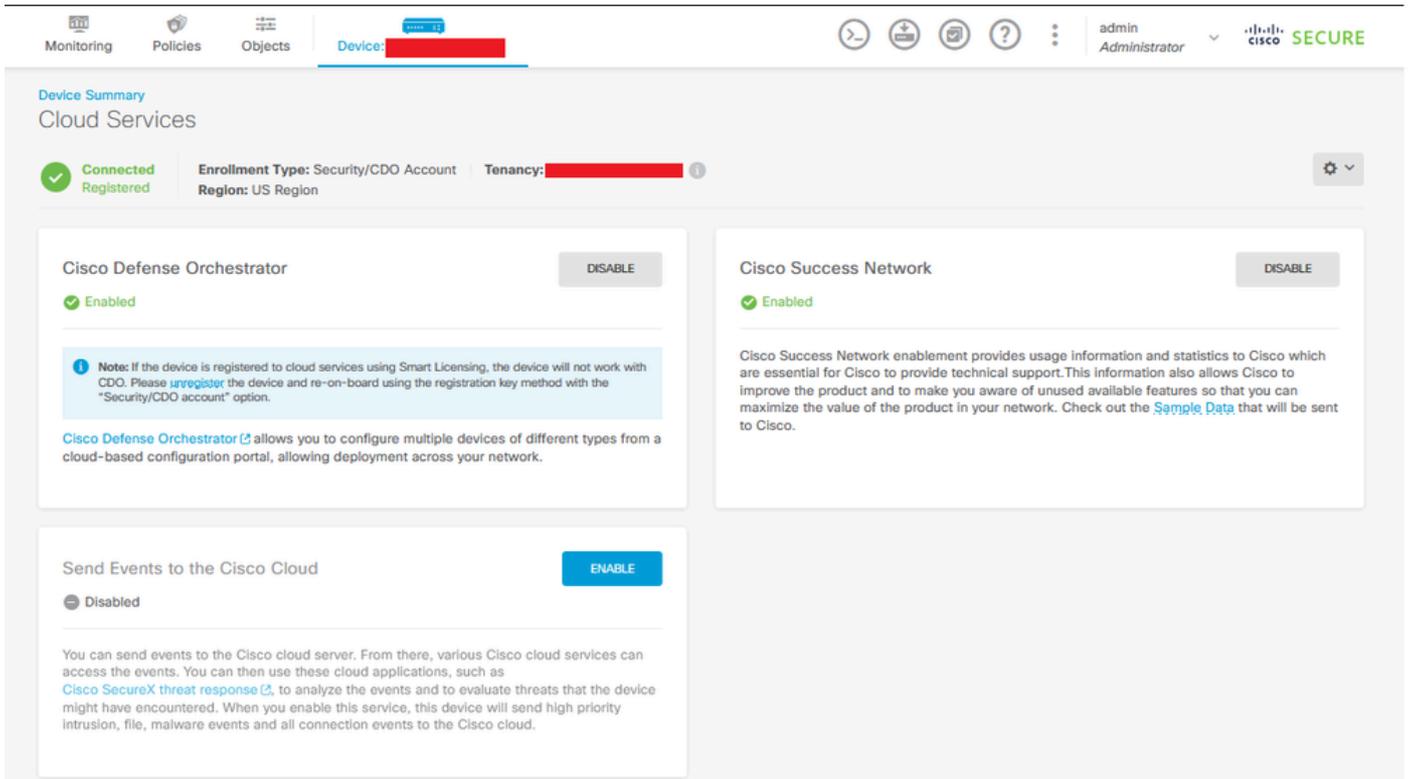
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product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

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

Enroll Cisco Success Network

REGISTER

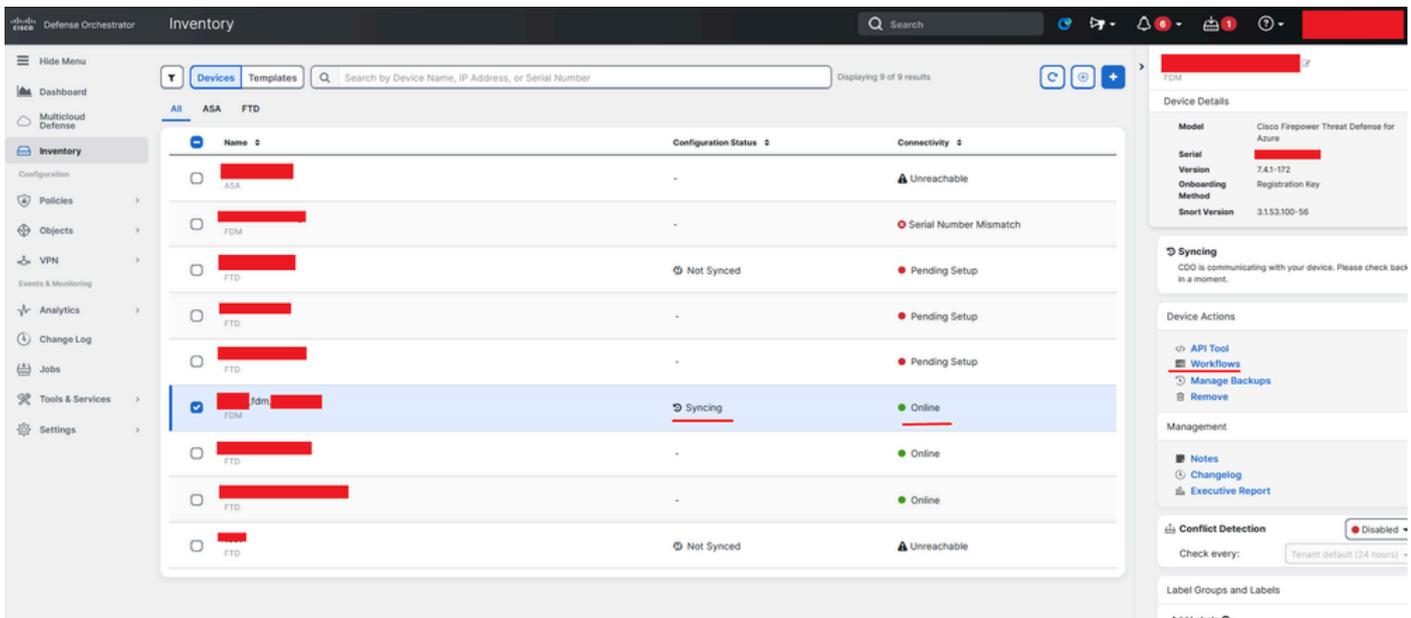
[Need help?](#)



Registro de FDM finalizado

En CDO, en el menú Inventory (Inventario), se puede encontrar FDM en proceso de incorporación y sincronización. El progreso y el flujo de esta sincronización se pueden revisar en la sección Flujos de trabajo.

Una vez finalizado este proceso, aparece como Sincronizado y En línea.



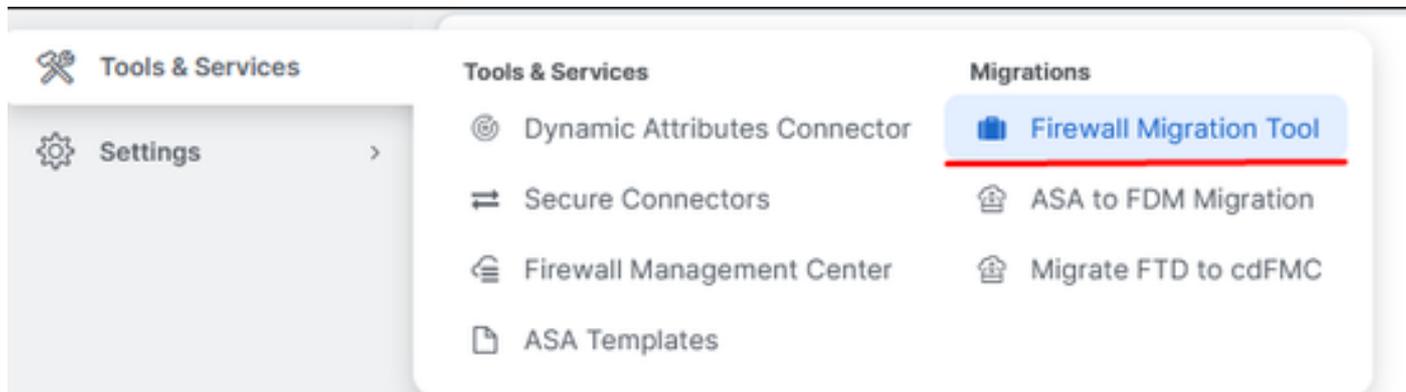
Inventario de CDO FDM incorporado

Cuando los dispositivos se han sincronizado, se muestra como En línea y Sincronizado.



FDM incorporado

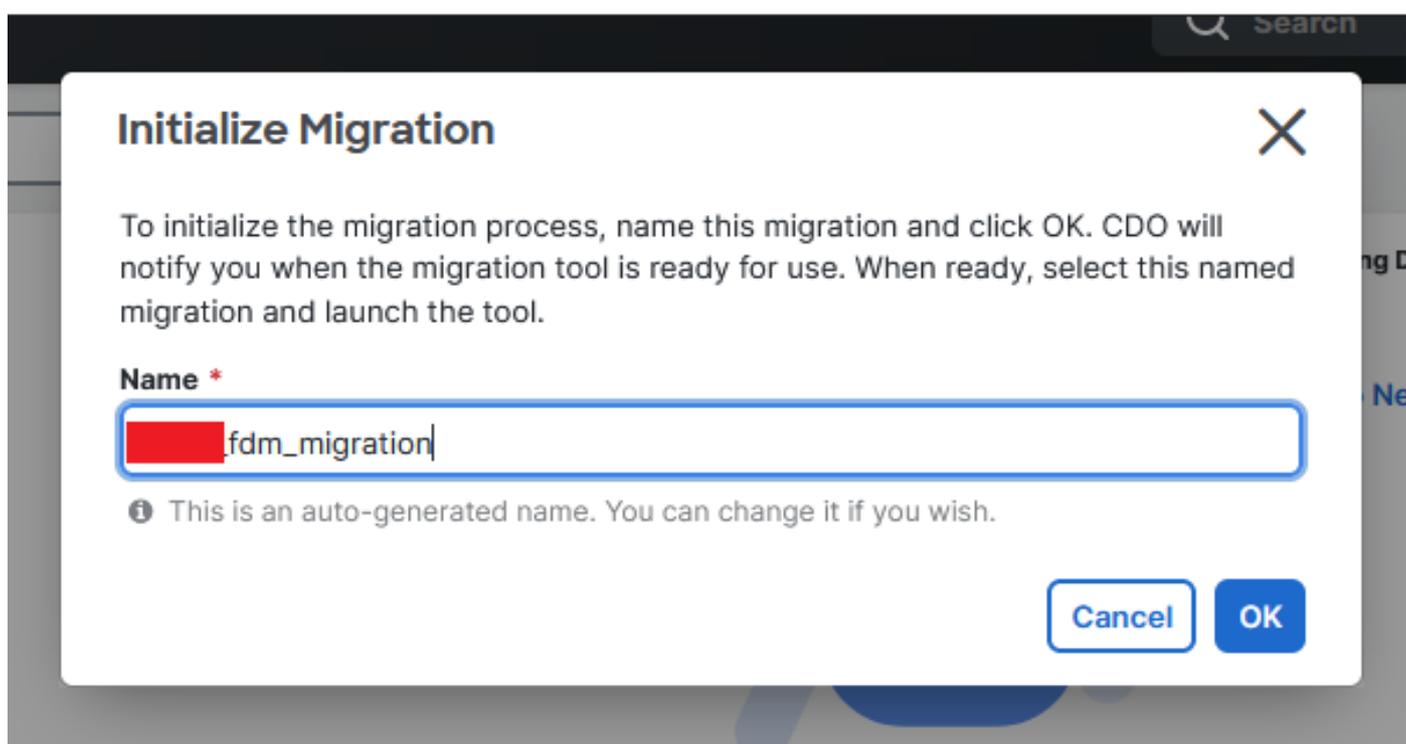
Una vez que FDM se haya integrado correctamente en CDO, debemos cerrar la sesión de FDM. Después de cerrar sesión en FDM, navegue dentro de CDO hasta Herramientas y servicios > Migración > Herramienta de migración de firewall.



Haga clic en el símbolo Add y aparecerá un nombre aleatorio que indica que es necesario cambiar el nombre para iniciar el proceso de migración.

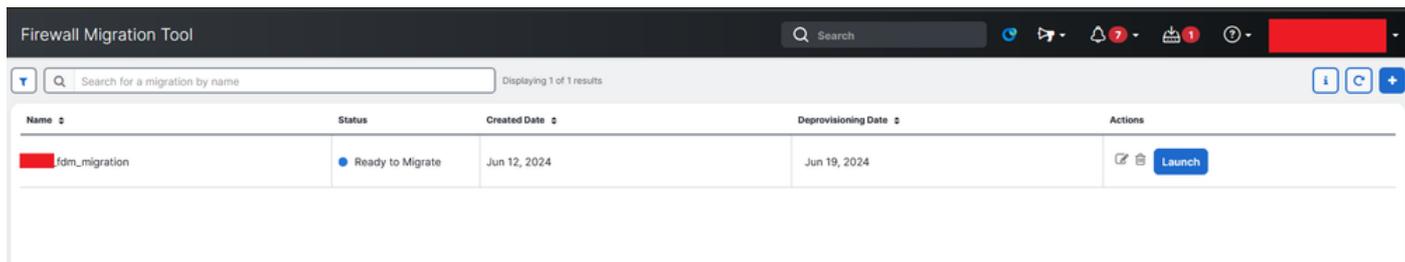


Después de cambiar el nombre, haga clic en Iniciar para iniciar la migración.



Inicializar migración

Haga clic en Iniciar para iniciar la configuración de migración.



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

Proceso de lanzamiento de migración

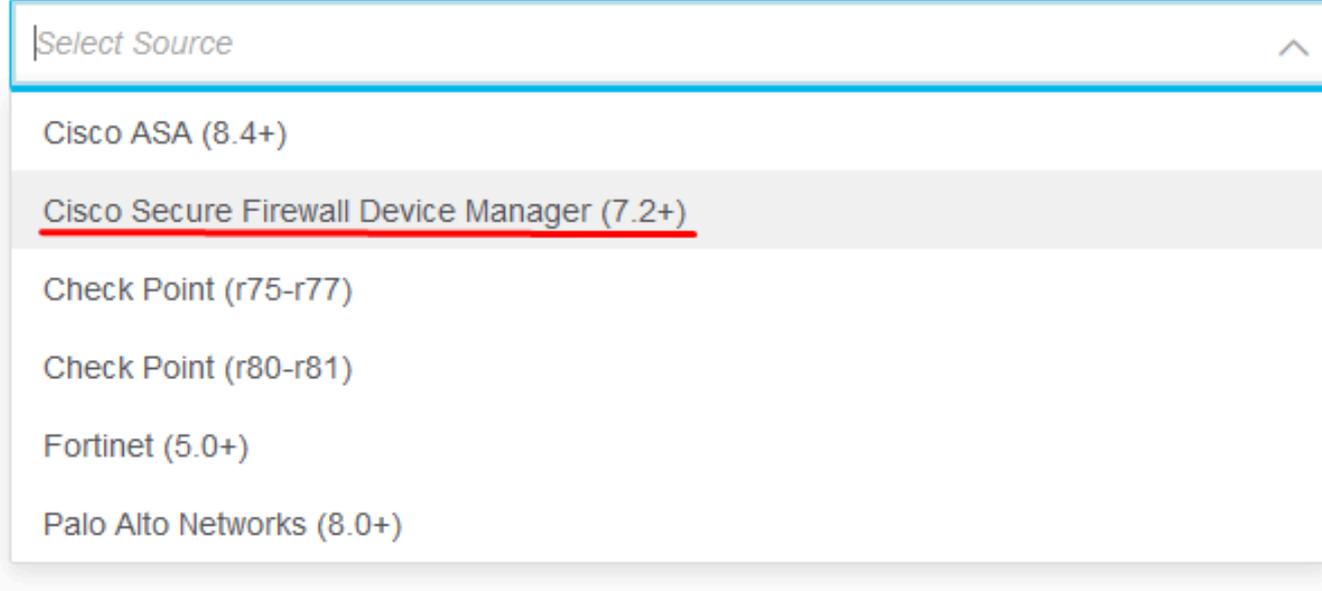
Después de hacer clic en Launch, se abrirá una ventana para el proceso de migración donde se selecciona la opción Cisco Secure Firewall Device Manager (7.2+). Como se mencionó anteriormente, esta opción está habilitada a partir de la versión 7.2.



Firewall Migration Tool (Version 6.0.1)

Select Source Configuration

Source Firewall Vendor



| *Select Source* 

- Cisco ASA (8.4+)
- Cisco Secure Firewall Device Manager (7.2+)
- Check Point (r75-r77)
- Check Point (r80-r81)
- Fortinet (5.0+)
- Palo Alto Networks (8.0+)

FMT Seleccionar configuración de origen

Una vez seleccionada, se presentan tres opciones de migración diferentes: Shared Configuration Only (Sólo configuración compartida), Includes Device & Shared Configurations (Incluye configuraciones compartidas y de dispositivos) e Include Device & Shared Configurations to FTD New Hardware.

Para esta instancia, se ejecuta la segunda opción, Migrar el administrador de dispositivos de

Firepower (incluye el dispositivo y la configuración compartida).

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 :

Opciones de migración

Una vez seleccionado el método de migración, seleccione el dispositivo en la lista proporcionada.

Live Connect to FDM

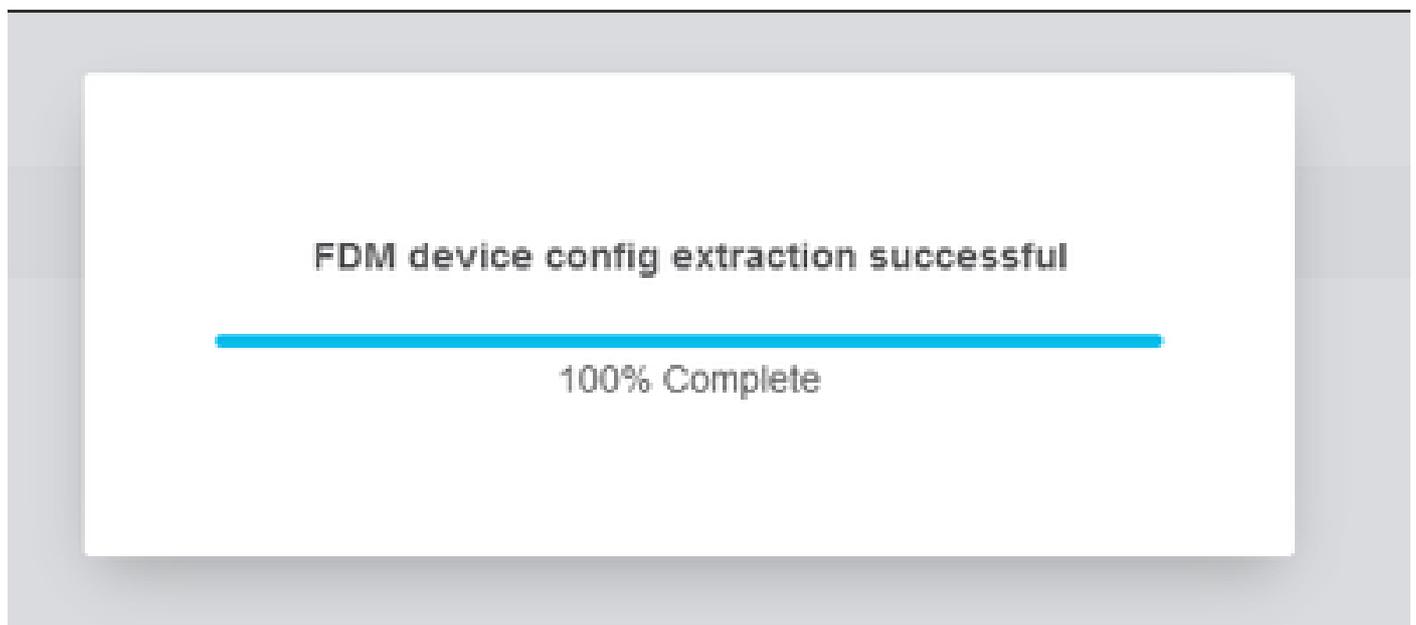
- Select any FDM device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.
- Click on change device status button to update the FDM device status from In-Use to Available.

Select FDM Managed Device

████████_fdm_████████ - Available

Connect 

Selección de dispositivos de FDM



Extracción de configuración completada

Se recomienda abrir la pestaña situada en la parte superior para revisar y comprender en qué paso nos encontramos cuando se ha seleccionado el dispositivo.



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:

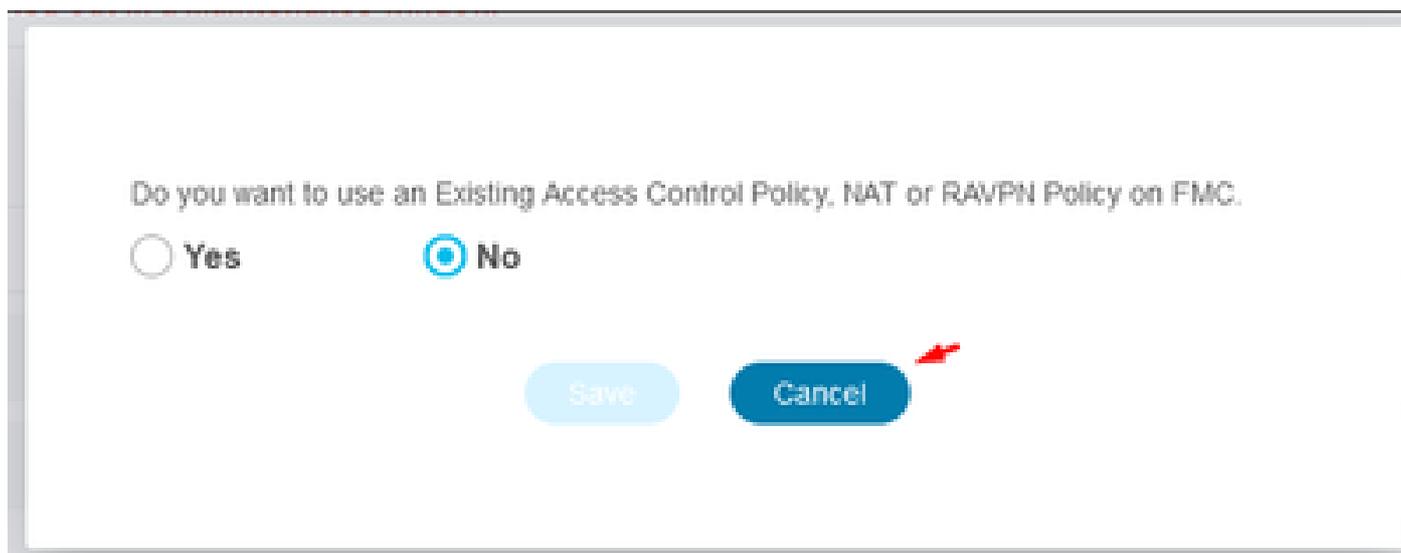
Parsed Summary

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

Pasos del proceso de migración

Al tratarse de una migración nueva, seleccione Cancel cuando se le solicite con la opción "¿Desea utilizar una política de control de acceso, NAT o RAVPN existente en FMC?"



Cancelar opción para configuración existente

Después, habrá opciones para seleccionar las funciones que se migrarán, como se muestra en la imagen. Haga clic en 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.

Funciones que se seleccionarán

A Continuación, Inicie Conversión.

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

Inicie la conversión.

Una vez finalizado el proceso de análisis, se pueden utilizar dos opciones: Descargar el documento y continuar con la migración haciendo clic en Siguiente.

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/ RAVPN/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

Descargar informe.

Las interfaces de dispositivo están configuradas para mostrarse. Como práctica recomendada, se recomienda hacer clic en Refresh para actualizar las interfaces. Una vez validados, puede continuar haciendo clic en Siguiente.



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 mostradas

Navegue hasta la sección Zonas de seguridad y Grupos de interfaz, donde necesita agregar

manualmente con Add SZ & IG. Para este ejemplo, se ha elegido Auto-Create. Esto ayuda a generar automáticamente las interfaces dentro del FMC al que se está migrando. Después de finalizar, haga clic en el botón Next.

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

Zonas de seguridad y grupos de interfaces

La opción Creación automática asigna las interfaces de FDM a las zonas de seguridad de FTD existentes y a los grupos de interfaces de FMC que tengan el mismo nombre.

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

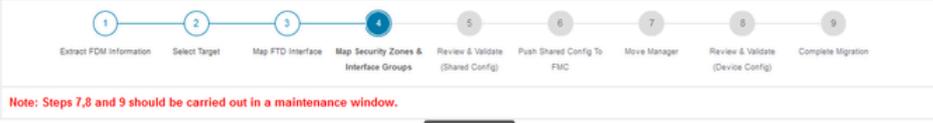
Security Zones Interface Groups

Cancel Auto-Create

Opción de creación automática.

A continuación, seleccione Siguiente.

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)

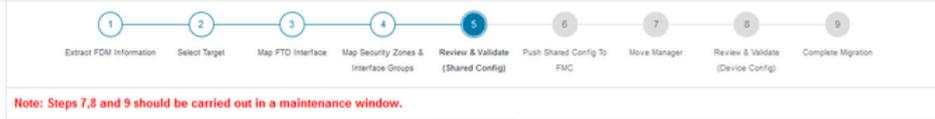
Note: Click on Auto-Create button to auto map the FDM name as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

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

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

Después de la creación automática.

En el paso 5, como se muestra en la barra superior, dedique tiempo a examinar las políticas de control de acceso (ACP), los objetos y las reglas NAT. Continúe revisando cuidadosamente cada elemento y, a continuación, haga clic en Validar para confirmar que no hay problemas con los nombres o las configuraciones.



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



Control de acceso, objetos y configuraciones NAT

A Continuación, Introduzca Sólo La Configuración Compartida

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</p> <p style="font-size: 10px; margin: 0;">(Standard, Extended used in BGP/RAVPNEIGRP)</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</p> <p style="font-size: 10px; margin: 0;">(Connection Profiles)</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</p> <p style="font-size: 10px; margin: 0;">(Geo, Application, URL objects and Intrusion Rule Group)</p> </div>	

Push Shared Configuration Only

Enviar sólo configuración compartida

Se puede observar el porcentaje de finalización y la tarea específica en la que se está trabajando.

Firewall Migration Tool (Version 6.0.1)

Push Shared Config to FMC

Migration Status

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

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

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

Porcentaje de pulsación

Una vez finalizado el paso 5, vaya al paso 6, como se muestra en la barra superior, donde se realiza la operación Push Shared Configuration to FMC. En este punto, seleccione el botón Next para avanzar.

Firewall Migration Tool (Version 6.0.1)

6
7
8
9

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.

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

Push Shared Config to FMC

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, RA/VN/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

Envío de la configuración compartida a FMC finalizado

Esta opción activa un mensaje de confirmación, que solicita la continuación de la migración del jefe.

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

Confirmar Mover jefe

Para continuar con la migración del administrador, es necesario tener a mano el ID de Management Center y el ID de NAT, lo cual es esencial. Estos ID se pueden recuperar seleccionando Actualizar detalles. Esta acción inicia una ventana emergente en la que se introduce el nombre deseado para la representación de FDM en el cdFMC y, a continuación, se guardan las modificaciones.



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

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

Show

Move Manager

ID de Manager Center e ID de NAT

Actualizar nombre de dispositivo para registro.

Después de esta acción, se muestran los ID de los campos mencionados anteriormente.



Advertencia: no realice ningún cambio en la interfaz de Management Center. De forma predeterminada, la opción Management (Administración) está seleccionada, deje esta opción como configuración predeterminada.



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	3aPMT	fdm-Azure	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management Select Data interface

Save

Move Manager

ID del centro de administración e ID de NAT.

Después de elegir la opción Update Details, el dispositivo que va a iniciar la sincronización.



Sincronización del dispositivo FDM

Una vez finalizada la migración, el siguiente paso consiste en examinar las interfaces, las rutas y los parámetros DHCP configurados en FDM seleccionando Validate.



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	10.1.1.1	Enabled

Page 1 to 2 of 2 Page 1 of 1



Validar configuración de FDM

Después de la validación, elija Push Configuration para iniciar el proceso de transferencia de la configuración, que continuará hasta que finalice la migración. Además, es posible supervisar las tareas que se están ejecutando.

Validation Status

✔ Successfully Validated

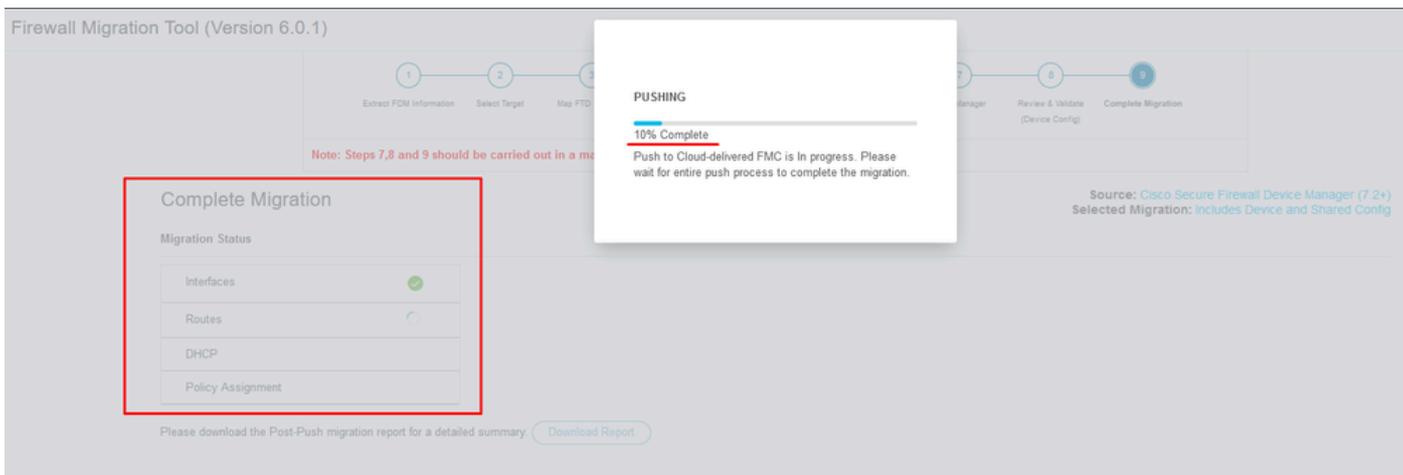
Validation Summary (Pre-push)

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

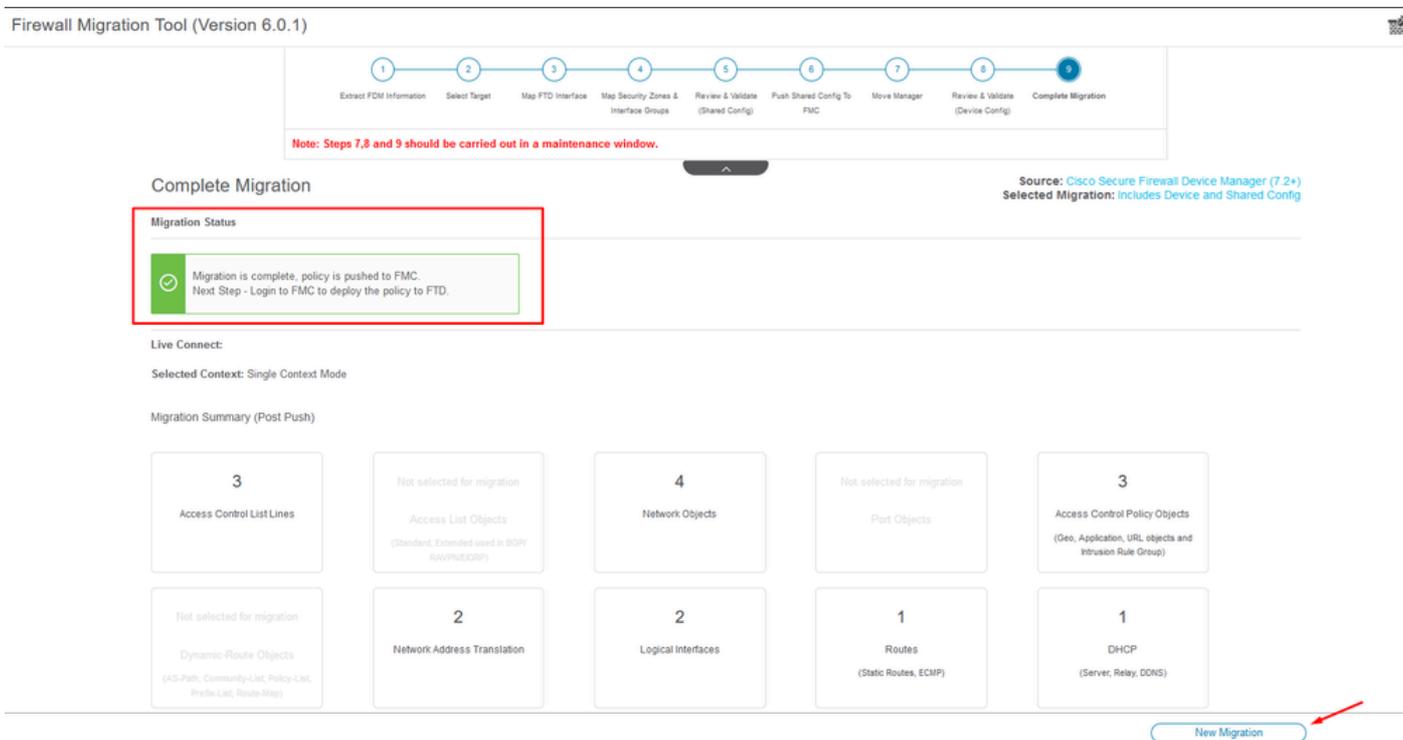
Estado de validación: configuración de inserción.

Ventana emergente con el porcentaje de envío de la configuración.



Porcentaje de envío completado

Al finalizar, se presenta una opción para iniciar una nueva migración, lo que marca el final del proceso de migración de FDM a cdFMC.

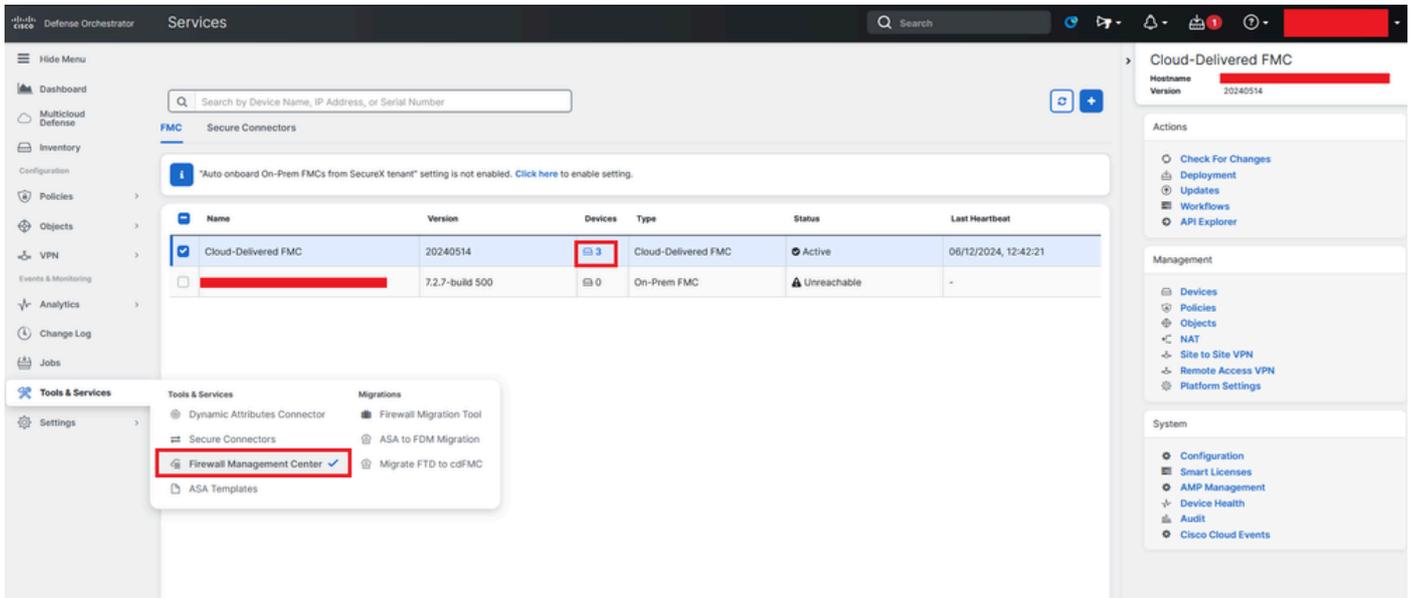


Migración completa

Verificación

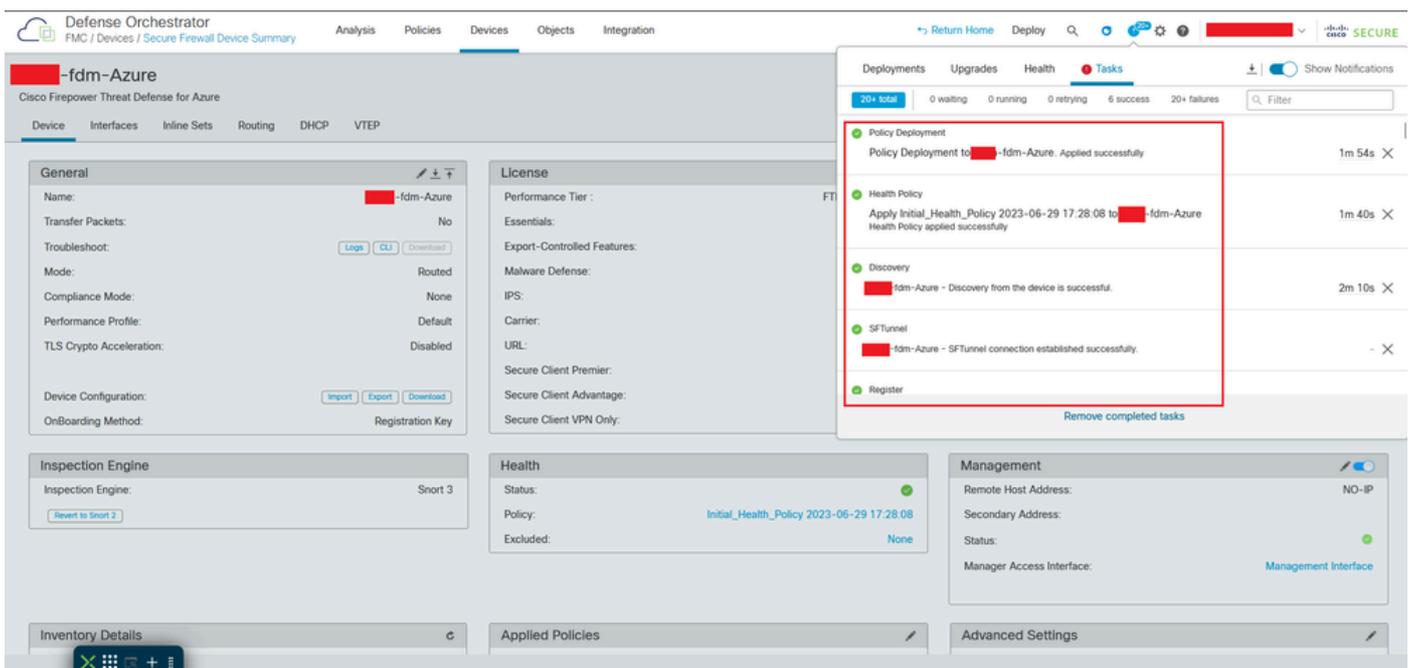
Para comprobar que el FDM se ha migrado correctamente al cdFMC.

Vaya a CDO > Tools & Services > Firepower Management Center. Allí, se encuentra el número de dispositivos registrados ha aumentado.



Dispositivos registrados de cdFMC

Verifique el dispositivo dentro de Devices > Device Management. Además, dentro de las tareas del FMC, puede encontrar cuándo el dispositivo se registró correctamente y la primera implementación se completó correctamente.



Tarea de registro de cdFMC completada.

El dispositivo está en cdFMC > Device > Device Management.

Defense Orchestrator
FMC / Devices / Device Management

Analysis Policies Devices Objects Integration

Return Home Deploy Search [User] [Cisco Secure]

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	

Dispositivo registrado en cdFMC

Política de control de acceso migrada en Políticas > Control de acceso.

Defense Orchestrator
FMC / Policies / Access Control / Access Control

Analysis Policies Devices Objects Integration

Return Home Deploy Search [User] [Cisco Secure]

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 [User]	

Política de migración

Del mismo modo, puede revisar los objetos creados en FDM que se migraron correctamente al 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	

Objetos migrados de FDM a cdFMC

Interfaces de gestión de objetos migradas.

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 administración de objetos migradas.

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).