

Migrar FDM para cdFMC usando FMT no CDO

Contents

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Informações de Apoio](#)

[Configurar](#)

[Verificar](#)

Introdução

Este documento descreve como migrar um Firepower Device Manager (FDM) para o FMC fornecido na nuvem (cdFMC) usando a ferramenta de migração do Firepower (FMT) no CDO.

Pré-requisitos

Requisitos

- Firepower Device Manager (FDM) 7.2+
- Centro de gerenciamento de firewall fornecido em nuvem (cdFMC)
- Ferramenta de migração Firepower (FMT) incluída no CDO

Componentes Utilizados

Este documento foi criado com base nos requisitos mencionados anteriormente.

- Firepower Device Manager (FDM) na versão 7.4.1
- Centro de gerenciamento de firewall fornecido em nuvem (cdFMC)
- Cloud Defense Orchestrator (CDO)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Os usuários administradores do CDO podem executar migrações de seus dispositivos para o cdFMC quando os dispositivos estiverem na versão 7.2 ou superior. Na migração descrita neste documento, o cdFMC já está habilitado no CDO Tenant.

Configurar

1.- Habilitar os Serviços em Nuvem da Cisco no FDM

Para iniciar a migração, é necessário ter o dispositivo FDM sem implantações pendentes e registrar-se nos Serviços de Nuvem. Para registrar-se nos serviços em nuvem, navegue para Configurações do sistema > Ver mais > Serviços em nuvem.

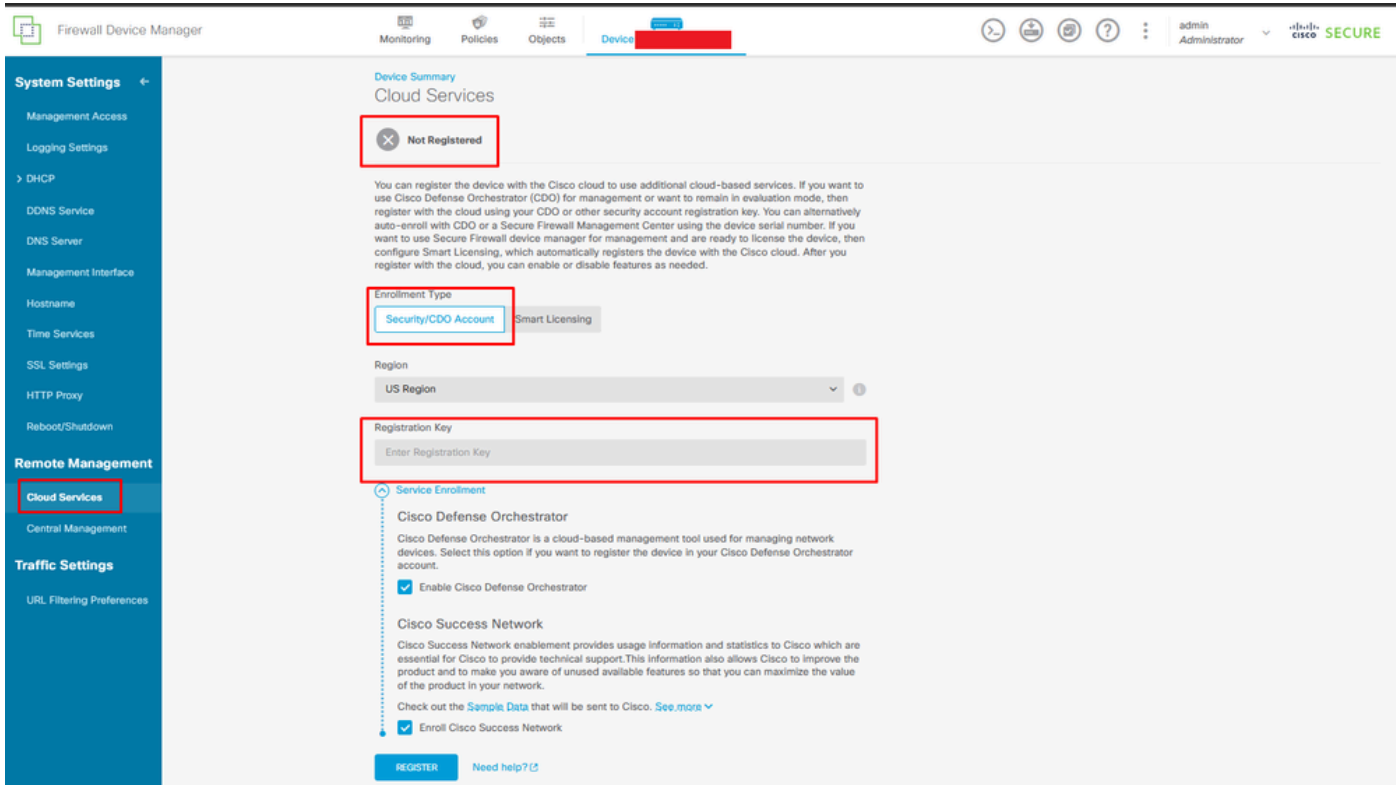
Na seção Cloud Services, você descobre que o dispositivo não está registrado, portanto, é necessário realizar a inscrição com o tipo Security/CDO Account. Você deve configurar uma Chave de Registro e, em seguida, Registrar.

The screenshot displays the Cisco FDM configuration interface. At the top, the navigation menu includes Monitoring, Policies, Objects, and Device. The main header shows the device model as Cisco Firepower Threat Defense for Azure, with software version 7.4.1-172 and VDB 376.0. The Cloud Services status is 'Connected | SEC TAC', and High Availability is 'Not Configured'. A network diagram shows the device connected to an Inside Network, an ISP/WAN/Gateway, and the Internet. Below the diagram, a grid of configuration tiles is visible:

- 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. See more.
- Device Administration:** Audit Events, Deployment History, Download Configuration. View Configuration.

Serviços em nuvem de registro

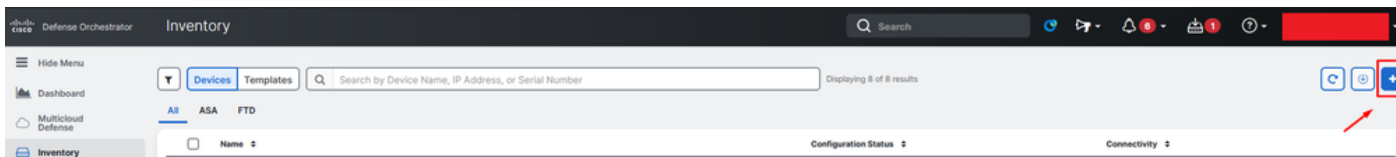
Em serviços de nuvem, é mostrado que não está registrado. Selecione o tipo de inscrição de Conta CDO e forneça a Chave de Registro do CDO.



Registro em serviços em nuvem

A chave de registro pode ser encontrada dentro do CDO. Navegue até CDO, vá até Inventário > Adicionar símbolo.

Um menu é exibido para selecionar o tipo de dispositivo que você possui. Selecione a opção FTD. A opção do FDM deve estar habilitada; caso contrário, a migração correspondente não poderá ser executada. O tipo de registro usa Usar chave de registro. Nessa opção, a Chave de Registro aparece na etapa 3, que deve ser copiada e colada no FDM.



FDM integrado, adicionar opção

Um menu é exibido para Selecionar um dispositivo ou tipo de serviço.

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



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

Selecionar dispositivo ou tipo de serviço

Para este documento, selecione Registration Key (Chave de registro).

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.

Tipo de registro

Aqui, ele mostra a chave de registro necessária na etapa 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

Processo de registro

Depois que a Chave de Registro tiver sido obtida, copie-a e cole-a no FDM e clique em Registrar. Após registrar o FDM nos Serviços em Nuvem, ele será exibido como Habilitado, conforme mostrado na imagem.

A Smart License foi ignorada, pois o dispositivo será registrado quando estiver em execução.

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

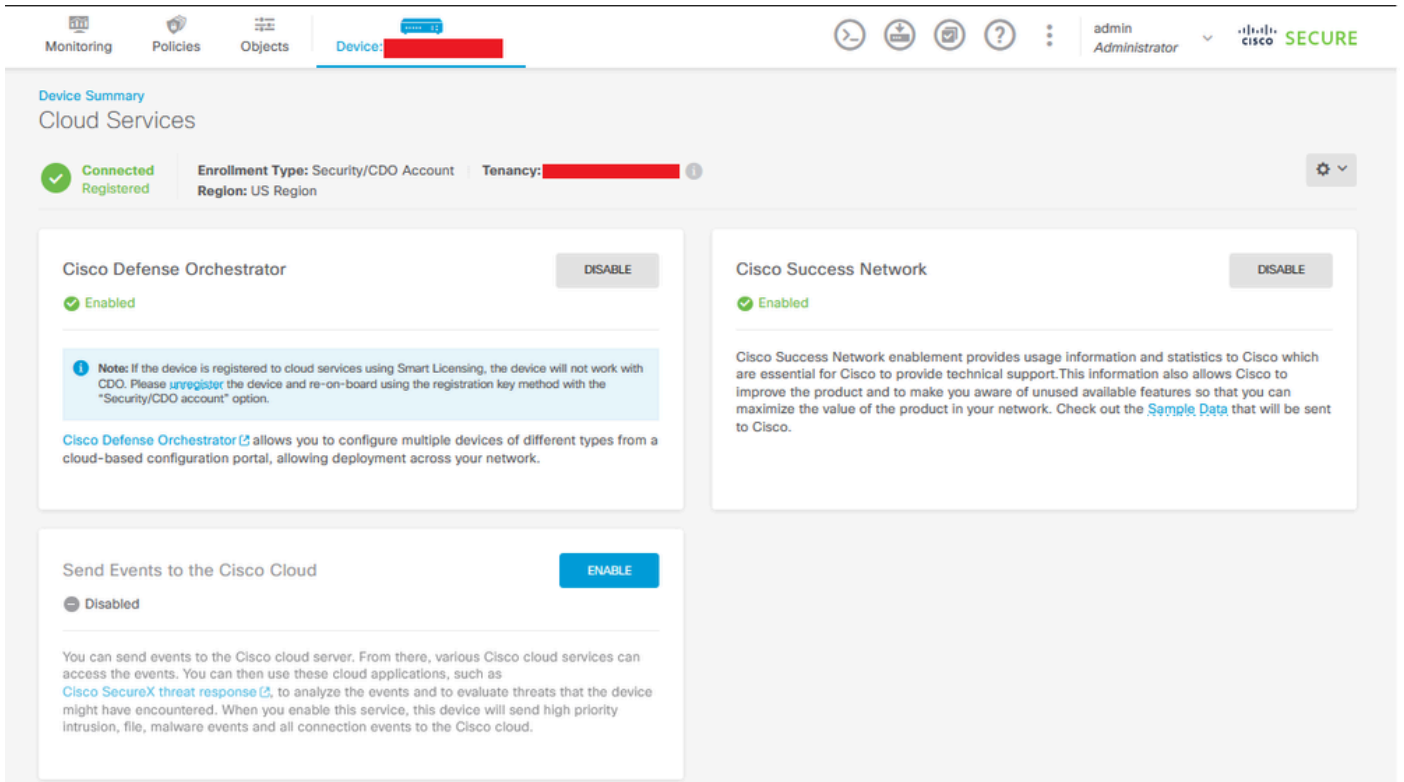
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product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

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

Enroll Cisco Success Network

REGISTER

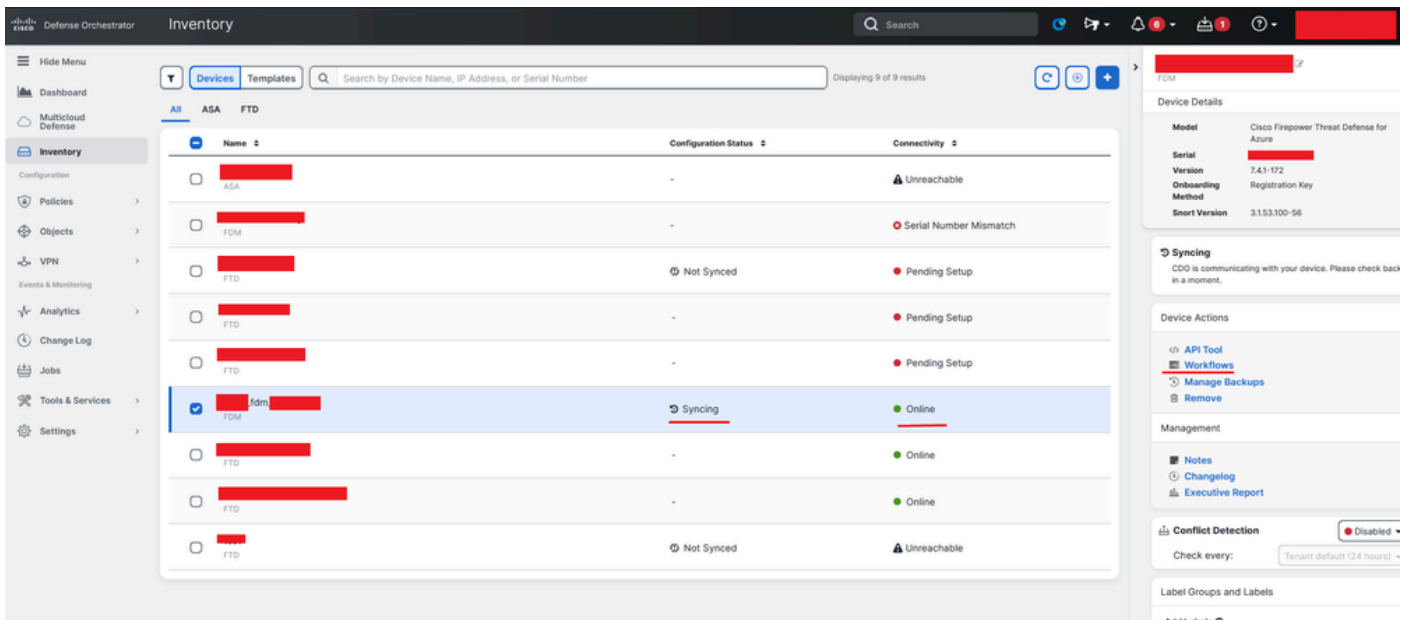
[Need help?](#)



Registro do FDM Concluído

No CDO, no menu Inventário, o FDM pode ser encontrado no processo de integração e sincronização. O progresso e o fluxo dessa sincronização podem ser revisados na seção Fluxos de Trabalho.

Quando esse processo estiver concluído, ele será exibido como Sincronizado e On-line.



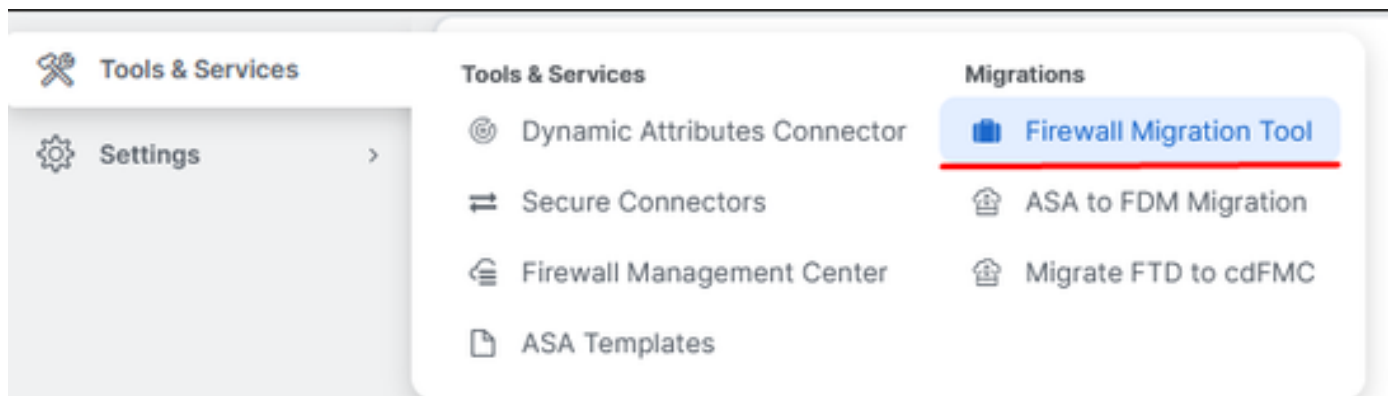
Inventário de CDO do FDM Integrado

Quando os dispositivos estiverem sincronizados, aparecerá como Online e Sincronizado.



FDM Integrado

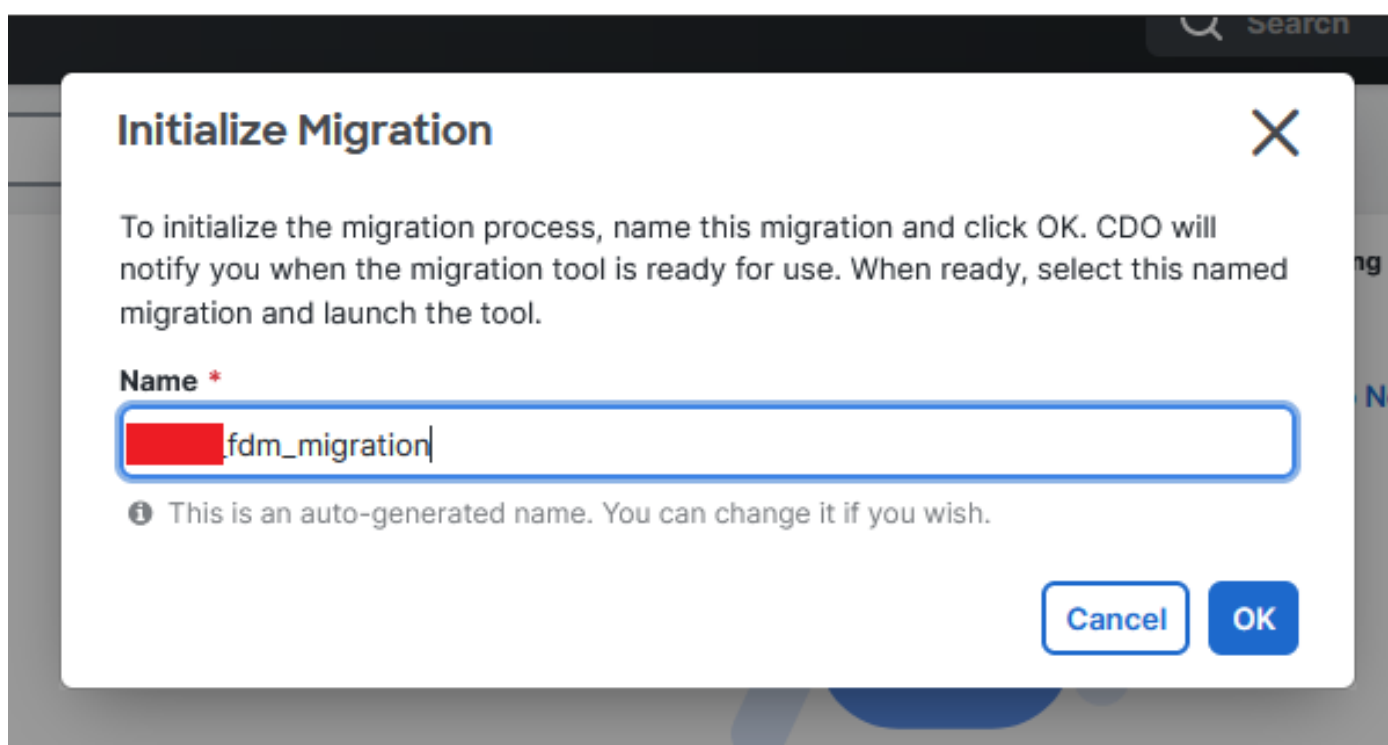
Quando o FDM tiver sido integrado com êxito ao CDO, será necessário fazer logoff do FDM. Após fazer logoff do FDM, navegue no CDO para Ferramentas e Serviços > Migração > Ferramenta de Migração do Firewall.



Clique no símbolo Adicionar e um nome aleatório será exibido, indicando que o nome precisa ser renomeado para iniciar o processo de migração.

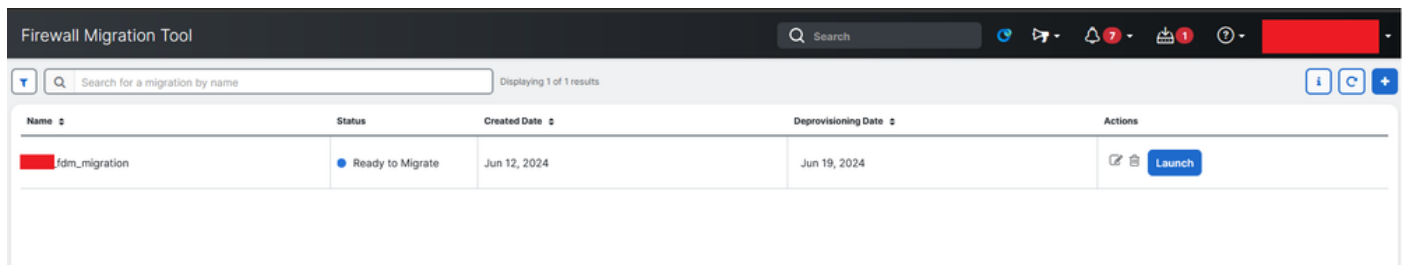



Após renomear, clique em Iniciar para iniciar a migração.



Inicializar Migração

Clique em Iniciar para iniciar a configuração de migração.



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

Processo de lançamento da migração

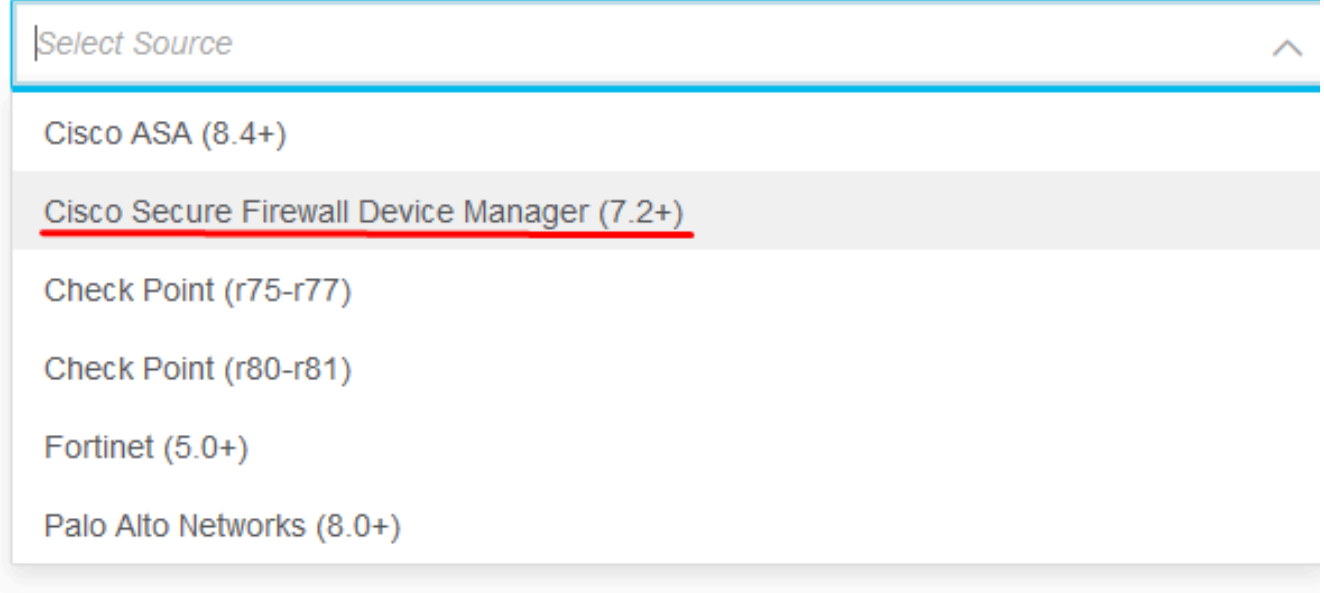
Após clicar em Iniciar, uma janela será aberta para o processo de migração onde a opção Cisco Secure Firewall Device Manager (7.2+) é selecionada. Como mencionado anteriormente, essa opção está ativada a partir da versão 7.2.



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+)


Selecionar Configuração de Origem FMT

Uma vez selecionadas, três opções de migração diferentes são apresentadas: Somente configuração compartilhada, Inclui configurações de dispositivo e compartilhadas e Inclui configurações de dispositivo e compartilhadas para FTD Novo hardware.

Para essa instância, a segunda opção, Migrate Firepower Device Manager (Inclui dispositivo e configuração compartilhada), é executada.

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) ✓

- 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 :

Opções de migração

Depois que o método de migração tiver sido selecionado, continue para selecionar o dispositivo na lista fornecida.

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



Seleção de Dispositivo do FDM

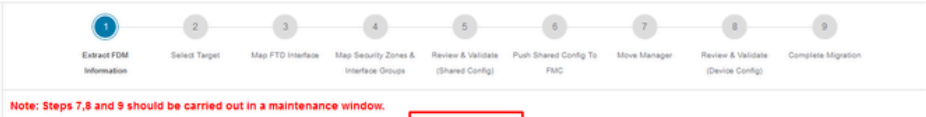
FDM device config extraction successful



100% Complete

Extração de Configuração Concluída

É recomendável abrir a guia localizada na parte superior para revisar e entender em que etapa estamos quando o dispositivo foi selecionado.



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:

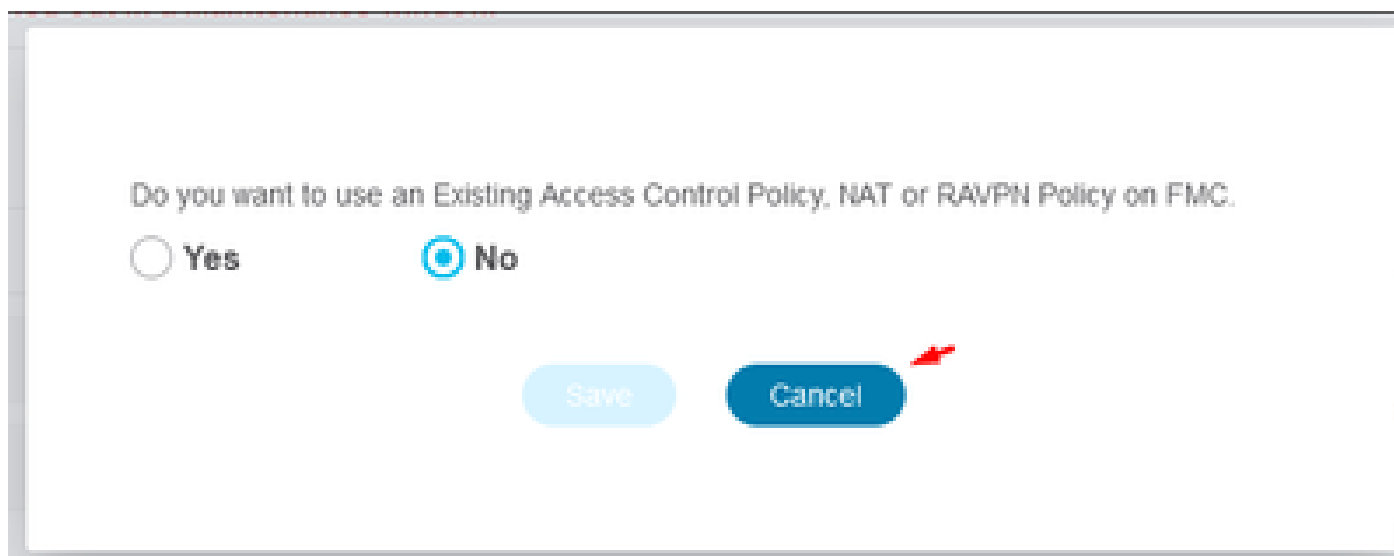
Parsed Summary

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

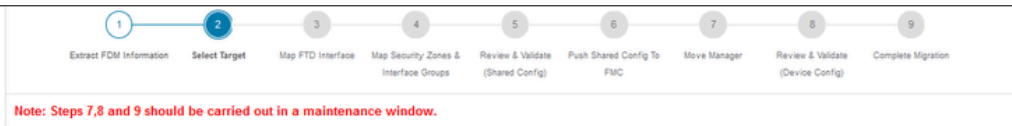
Etapas para o processo de migração

Sendo uma nova migração, selecione Cancel quando solicitado com a opção "Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC?" (Deseja usar uma política de controle de acesso, NAT ou política RAVPN existente no FMC?)



Cancelar opção para Configuração Existente

Depois, haverá opções para selecionar os recursos a serem migrados, conforme mostrado na imagem. Clique em Continuar.



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 ⓘ

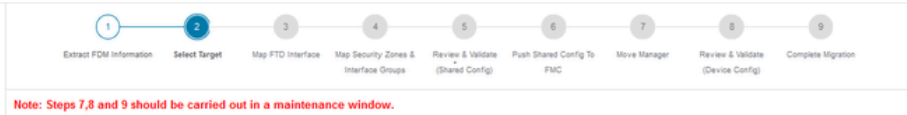
Proceed

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

Recursos a serem selecionados

Em Seguida, Inicie A Conversão.

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

Iniciar conversão.

Após a conclusão do processo de análise, duas opções podem ser usadas: Download do documento e continuar com a migração clicando em Avançar.

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

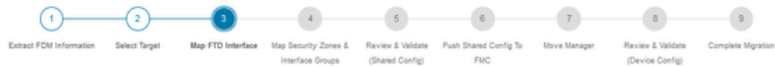
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPM/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)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

Download do relatório.

As interfaces do dispositivo estão configuradas para serem exibidas. Como prática recomendada, é recomendável clicar em Atualizar para atualizar as interfaces. Depois de validado, você pode continuar clicando em Avançar.



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 exibidas

Navegue para a seção Zonas de segurança e Grupos de interface, onde você precisa adicionar

manualmente com Adicionar SZ & IG. Para este exemplo, Criação Automática foi escolhida. Isso ajuda a gerar automaticamente as interfaces dentro do FMC para o qual você está migrando. Depois de terminar, clique no botão Avançar.

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.

Zonas de segurança e grupos de interface

A opção Criação Automática mapeia interfaces do FDM para Zonas de Segurança do FTD existentes e grupos de interfaces no FMC que têm o mesmo nome.

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

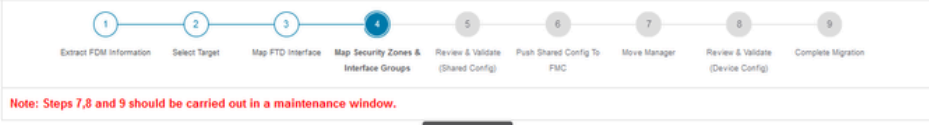
Security Zones Interface Groups

Cancel Auto-Create

Opção de Criação Automática.

Em seguida, selecione 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

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.

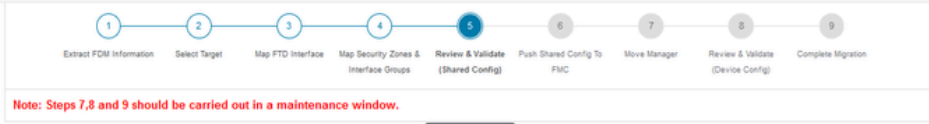
10 DEF.P938 2 Page 1 of 1

Back Next

Após a opção de Criação Automática.

Na etapa 5, como mostrado na barra superior, reserve um tempo para examinar as Políticas de Controle de Acesso (ACP), Objetos e regras de NAT. Continue revisando cuidadosamente cada item e clique em Validar para confirmar se não há problemas com nomes ou configurações.

Firewall Migration Tool (Version 6.0.1)



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

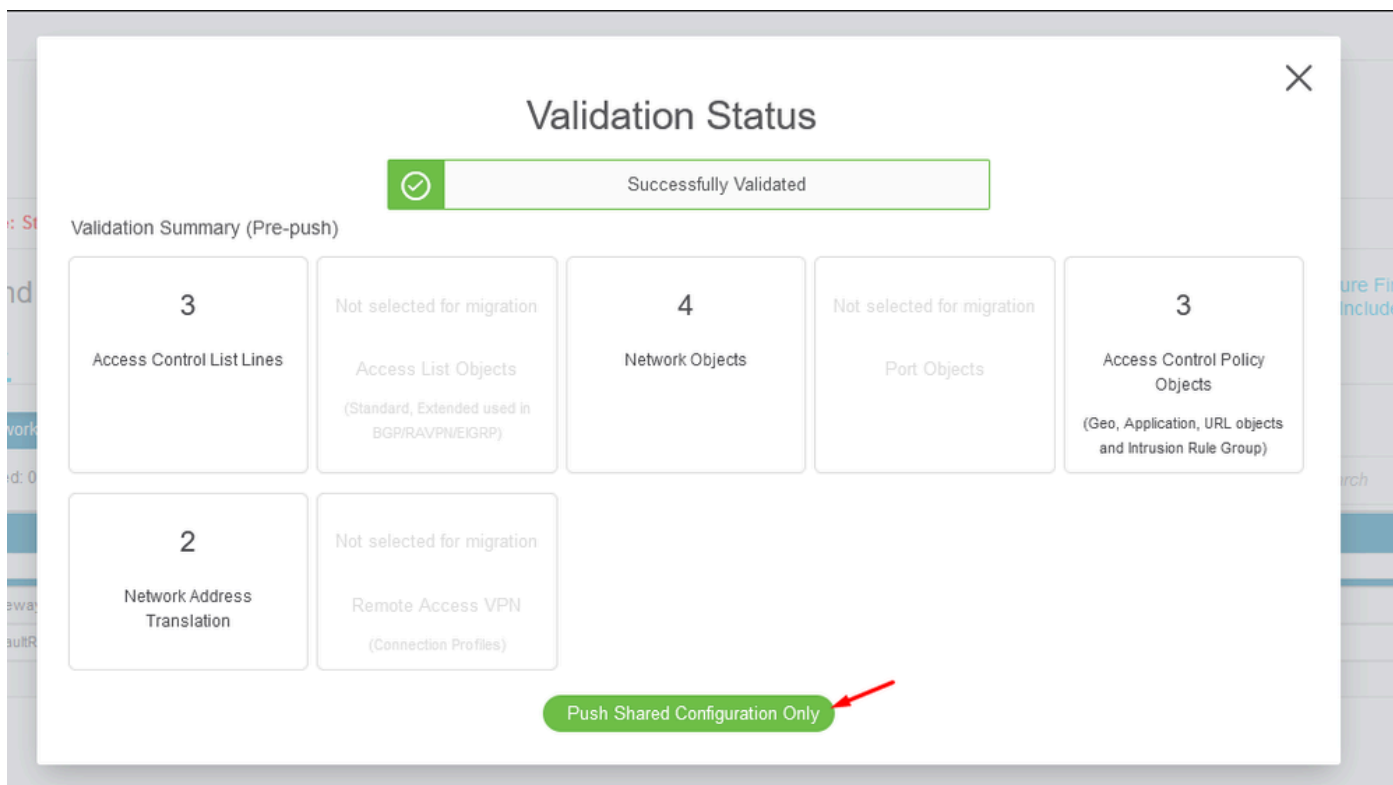
#	Name	Validation State	Type	Value
<input type="checkbox"/>	1 OutsidePv4Gateway	Validation pending	Network Object	172.16.1.1
<input type="checkbox"/>	2 OutsidePv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
<input type="checkbox"/>	3 Banned	Validation pending	Network Object	103.104.73.155

Page 1 to 3 of 3 Page 1 of 1

Validate

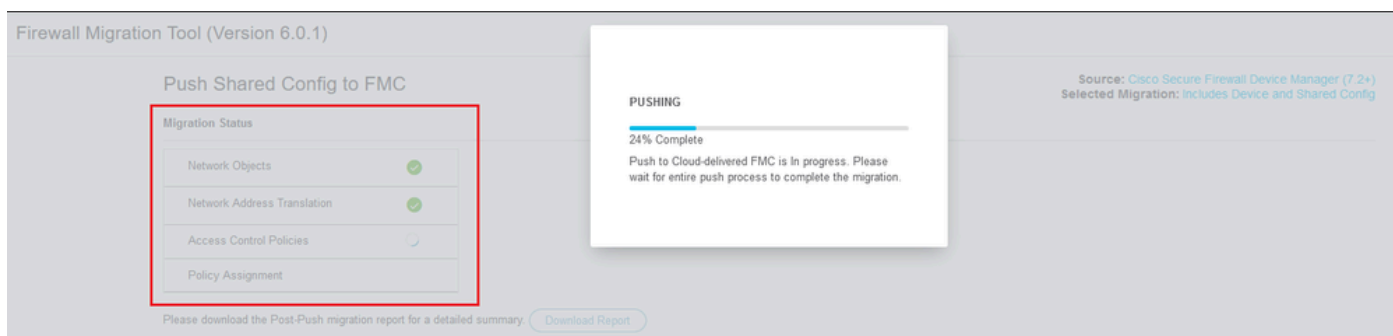
Controle de acesso, objetos e configurações de NAT

Em seguida, envie somente a configuração compartilhada



Enviar Somente Configuração Compartilhada

A porcentagem de conclusão e a tarefa específica que está sendo trabalhada podem ser observadas.



Porcentagem de Envio

Após a conclusão da etapa 5, vá para a etapa 6, conforme exibido na barra superior, onde ocorre Push Shared Configuration to FMC. Neste ponto, selecione o botão Next para avançar.



Push Shared Config to FMC

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

Migration Status

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

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

Next

Push de configuração compartilhada para FMC concluído

Essa opção aciona uma mensagem de confirmação, solicitando a continuação da migração do gerenciador.

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.

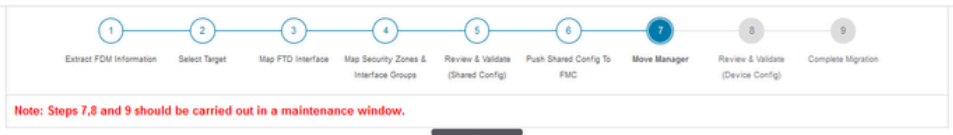
I acknowledge all the steps mentioned above have been completed.

Proceed

Cancel

Confirmar Mover Gerenciador

Para prosseguir com a migração do gerenciador, é necessário ter a ID do Management Center e a ID do NAT à mão, o que é essencial. Essas IDs podem ser recuperadas selecionando Atualizar detalhes. Esta ação inicia uma janela pop-up em que o nome desejado para a representação do FDM no cdFMC é inserido, seguido pelo salvamento das alterações.



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

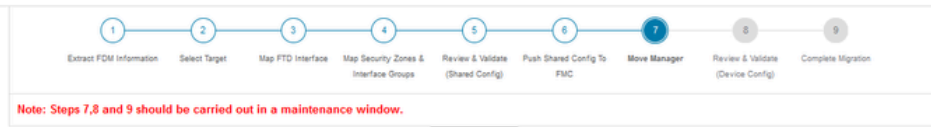
ID do Centro de Gerentes e ID de NAT

Atualize o nome do dispositivo para registro.

Após essa ação, as IDs dos campos mencionados acima serão exibidas.



Aviso: Não faça nenhuma alteração na Interface do Centro de Gerenciamento. Por padrão, a opção Gerenciamento está selecionada. Deixe essa opção como a configuração padrão.



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

Save

Move Manager

ID do centro de gerenciamento e ID NAT.

Depois de escolher a opção Update Details, o dispositivo que começará a sincronizar.



Sincronizando Dispositivo do FDM

Após a conclusão da migração, a próxima etapa é examinar as interfaces, as rotas e as configurações de DHCP configuradas no FDM selecionando Validar.



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



Validar Definições de configuração do FDM

Após a validação, escolha Configuração Push para iniciar o processo de push de configuração, que continuará até a conclusão da migração. Além disso, é possível monitorar as tarefas que estão sendo executadas.

Validation Status

✔ Successfully Validated

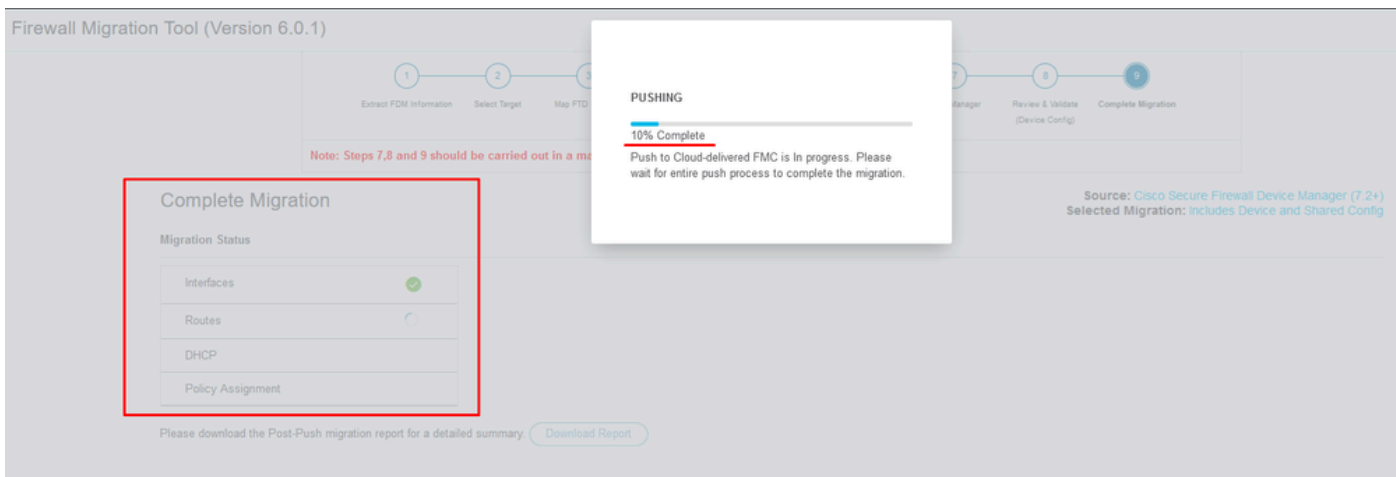
Validation Summary (Pre-push)

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	1
		Logical Interfaces	Routes <small>(Static Routes, ECMP)</small>
Not selected for migration Site-to-Site VPN Tunnels	0	0	1
	Platform Settings <small>(snmp,http)</small>	Malware & File Policy	DHCP <small>(Server, Relay, DDNS)</small>

Push Configuration

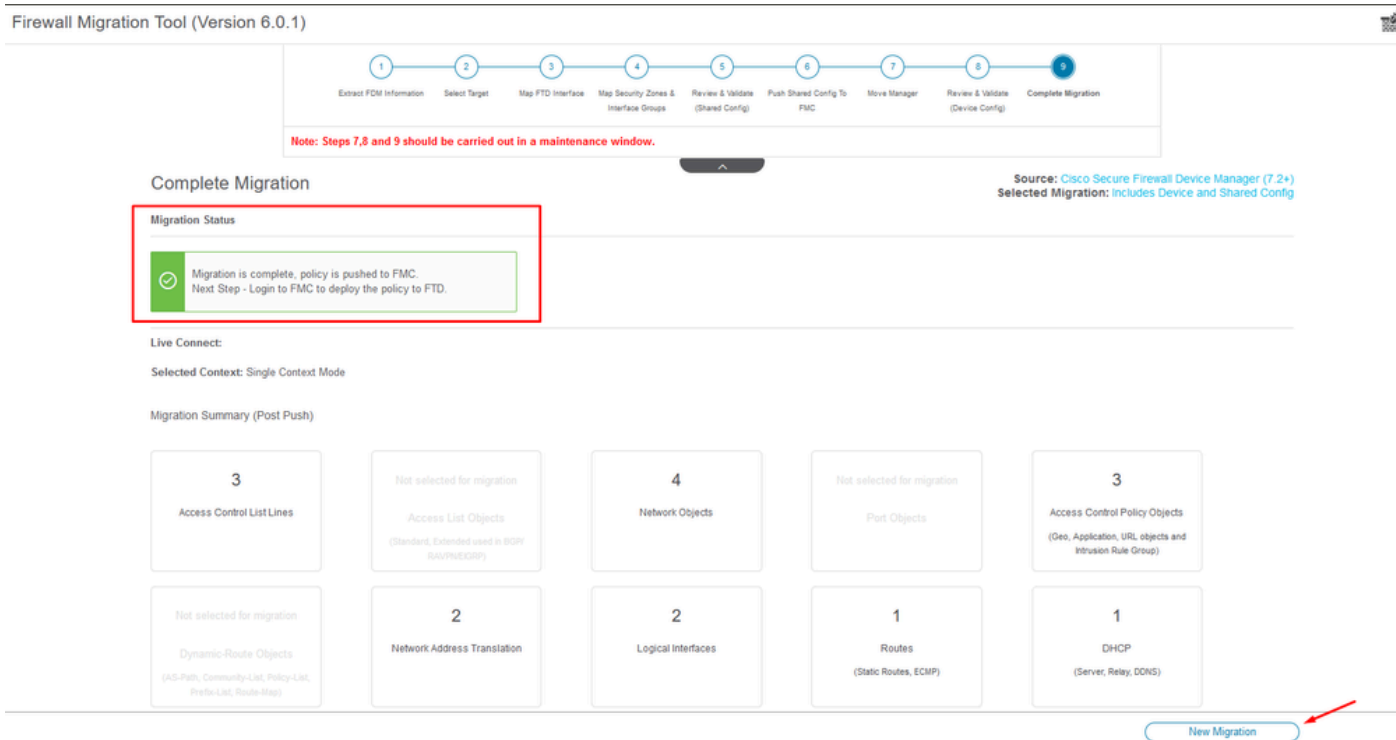
Status da validação - Configuração de envio por push.

Janela pop-up com a configuração de porcentagem de envio.



Porcentagem de Envio Concluída

Após a conclusão, uma opção para iniciar uma nova migração é apresentada, marcando o final do processo de migração do FDM para o cdFMC.

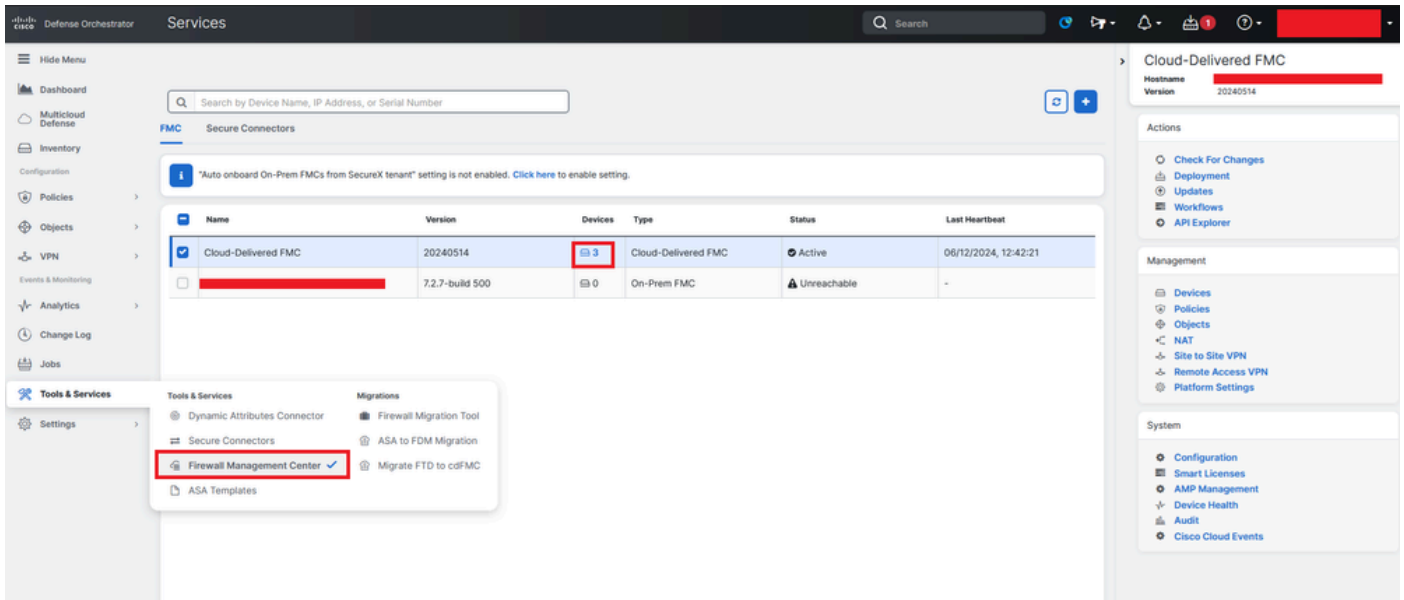


Migração completa

Verificar

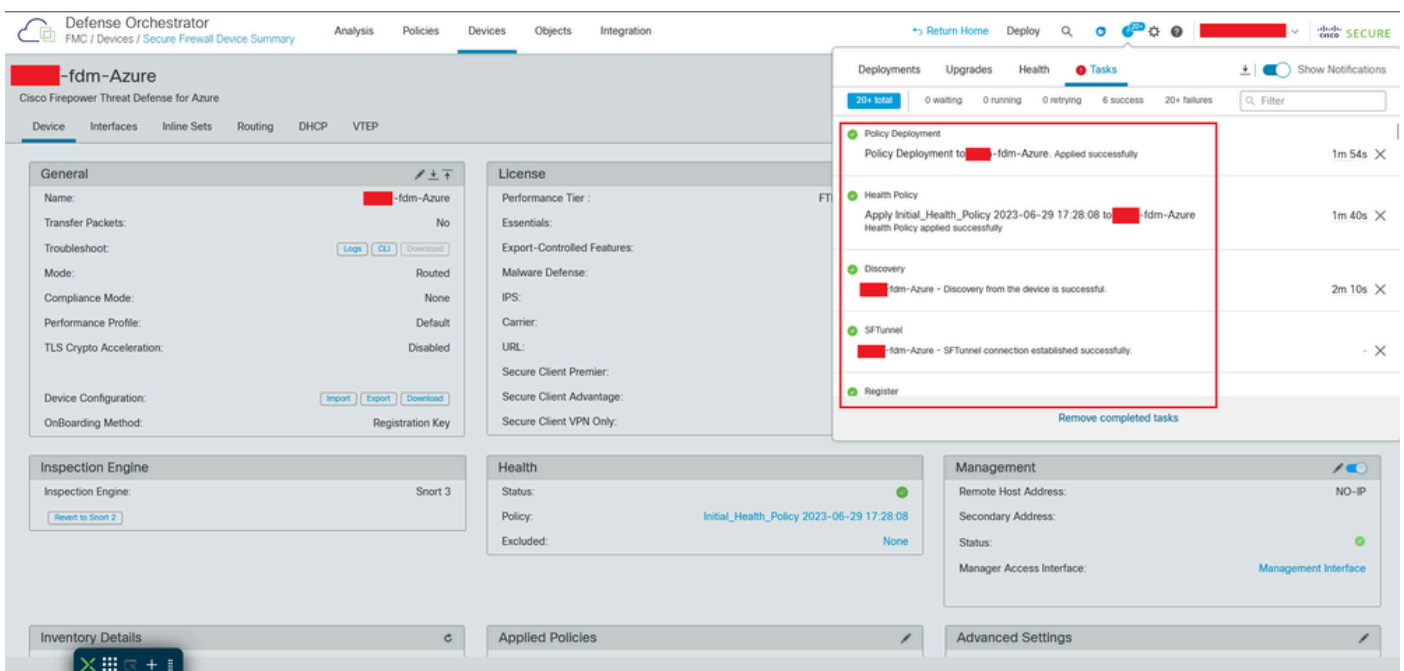
Para verificar se o FDM foi migrado com êxito para o cdFMC.

Navegue até CDO > Tools & Services > Firepower Management Center. Lá, você descobre que o número de dispositivos registrados aumentou.



Dispositivos registrados do cdFMC

Verifique o dispositivo em Devices > Device Management. Além disso, nas tarefas do FMC, você pode descobrir quando o dispositivo foi registrado com êxito e a primeira implantação foi concluída com êxito.



Tarefa de registro do cdFMC concluída.

O dispositivo está em cdFMC > Device > Device Management.

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

Dispositivo registrado no cdFMC

Access Control Policy (Política de controle de acesso) migrada em Policies > Access Control (Políticas > Controle de acesso).

Access Control Policy	Status	Last Modified	Lock Status
FTD-Mig-ACP-1718216278	Targeting 1 devices Up-to-date on all targeted devices	2024-06-12 12:18:00	

Política de migração

Da mesma forma, você pode revisar os objetos criados no FDM que foram corretamente migrados para o cdFMC.

Name	Value	Type	Override
Banned	103.104.73.155	Host	Yes
Inside_Network_IP	192.168.192.10	Host	Yes

Objetos Migrados do FDM para o cdFMC

Interfaces de gerenciamento de objetos migradas.

Defense Orchestrator
FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration

Return Home Deploy Q Filter

SECURE

Interface

Add Filter

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

Name	Type	Interface Type	
inside_ig	Interface Group	Routed	
> fdm-Azure			
inside_zone	Security Zone	Routed	
> fdm-Azure			
outside_ig	Interface Group	Routed	
> fdm-Azure			
outside_zone	Security Zone	Routed	
> fdm-Azure			

Interfaces de Gerenciamento de Objetos Migradas.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.