在CDO中使用FMT将FDM迁移到cdFMC

目录

简介

先决条件

  要求

  使用的组件

背景信息

配置

验证

简介

本文档介绍如何使用CDO中的Firepower迁移工具(FMT)将Firepower设备管理器(FDM)迁移到云交付的FMC (cdFMC)。

先决条件

要求

- Firepower设备管理器(FDM) 7.2+
- 云交付的防火墙管理中心(cdFMC)
- CDO中包含Firepower迁移工具(FMT)

使用的组件

本文档正是基于上述要求而创建的。

- 版本7.4.1上的Firepower设备管理器(FDM)
- 云交付的防火墙管理中心(cdFMC)
- 云防御协调器(CDO)

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

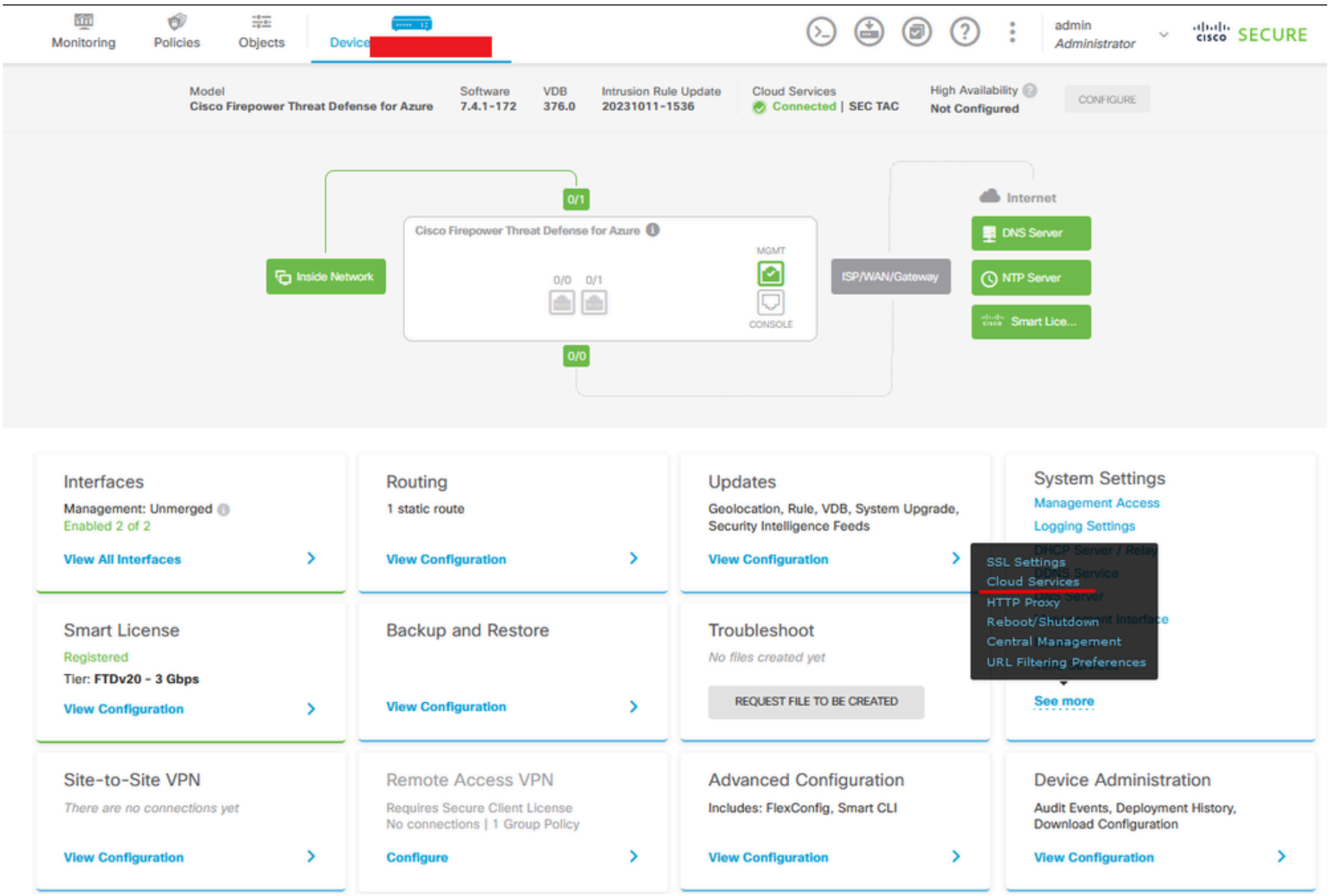
CDO管理员用户可以在设备使用版本7.2或更高版本时将其设备迁移到cdFMC。在本文档中介绍的迁移中，cdFMC已在CDO租户上启用。

配置

1.-在FDM上启用思科云服务

要开始迁移，必须使FDM设备没有挂起的部署并注册到云服务。要注册到云服务，请导航到系统设置(System Settings) >查看更多(See More) >云服务(Cloud Services)。

在云服务部分中，您发现设备未注册，因此必须使用类型安全/CDO帐户执行注册。您必须配置注册密钥，然后配置注册。



Model: Cisco Firepower Threat Defense for Azure
Software: 7.4.1-172
VDB: 376.0
Intrusion Rule Update: 20231011-1536
Cloud Services: Connected | SEC TAC
High Availability: Not Configured

Interfaces
Management: Unmerged
Enabled 2 of 2

Routing
1 static route

Updates
Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds

System Settings
Management Access
Logging Settings

Smart License
Registered
Tier: FTDv20 - 3 Gbps

Backup and Restore

Troubleshoot
No files created yet

Site-to-Site VPN
There are no connections yet

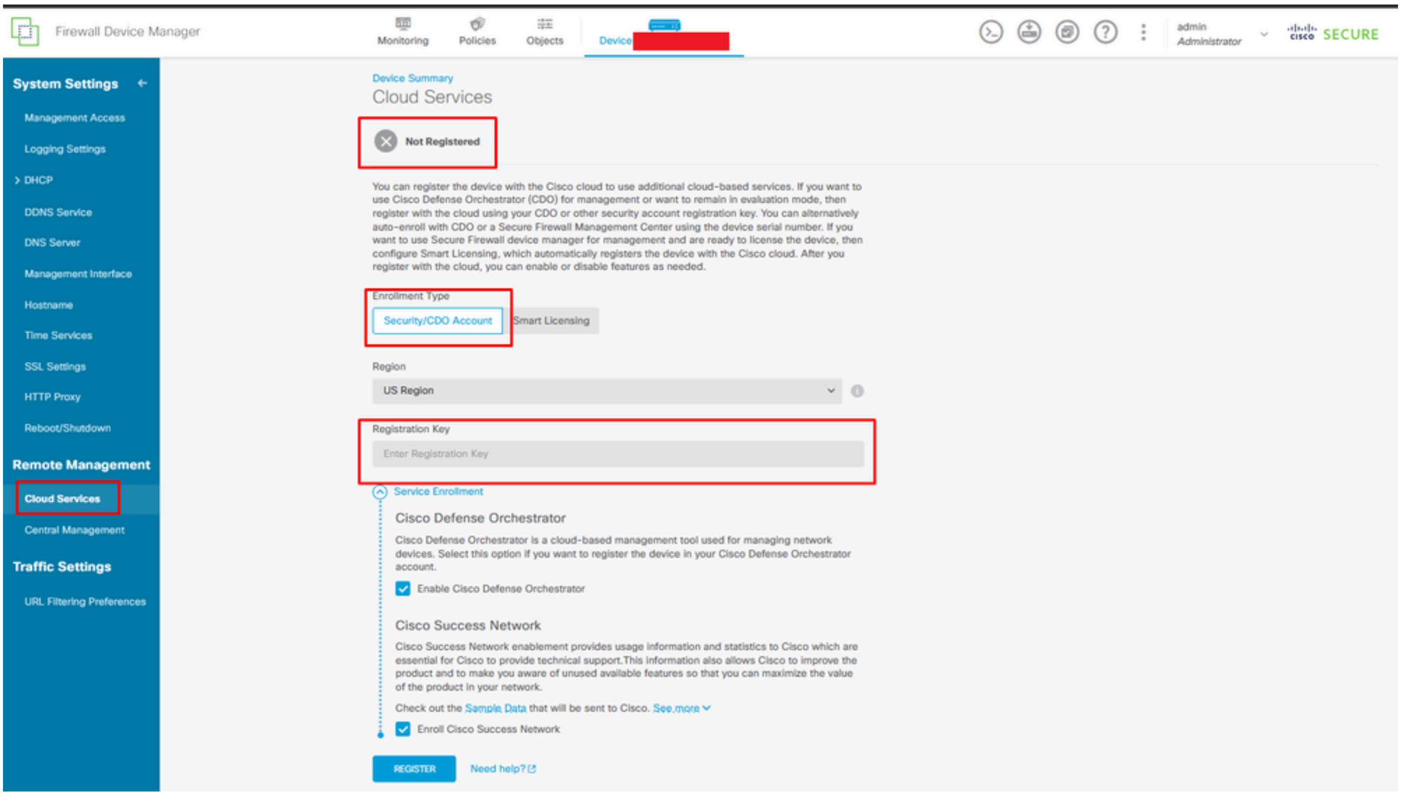
Remote Access VPN
Requires Secure Client License
No connections | 1 Group Policy

Advanced Configuration
Includes: FlexConfig, Smart CLI

Device Administration
Audit Events, Deployment History, Download Configuration

注册云服务

在云服务上，显示未注册。选择CDO帐户注册类型并提供CDO的注册密钥。



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: Enter Registration Key

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

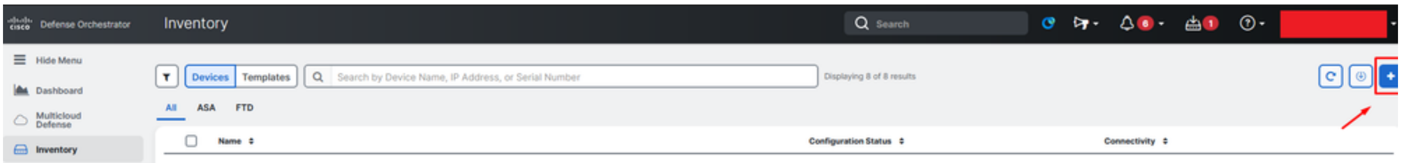
☑ Enroll Cisco Success Network

REGISTER Need help?

注册云服务

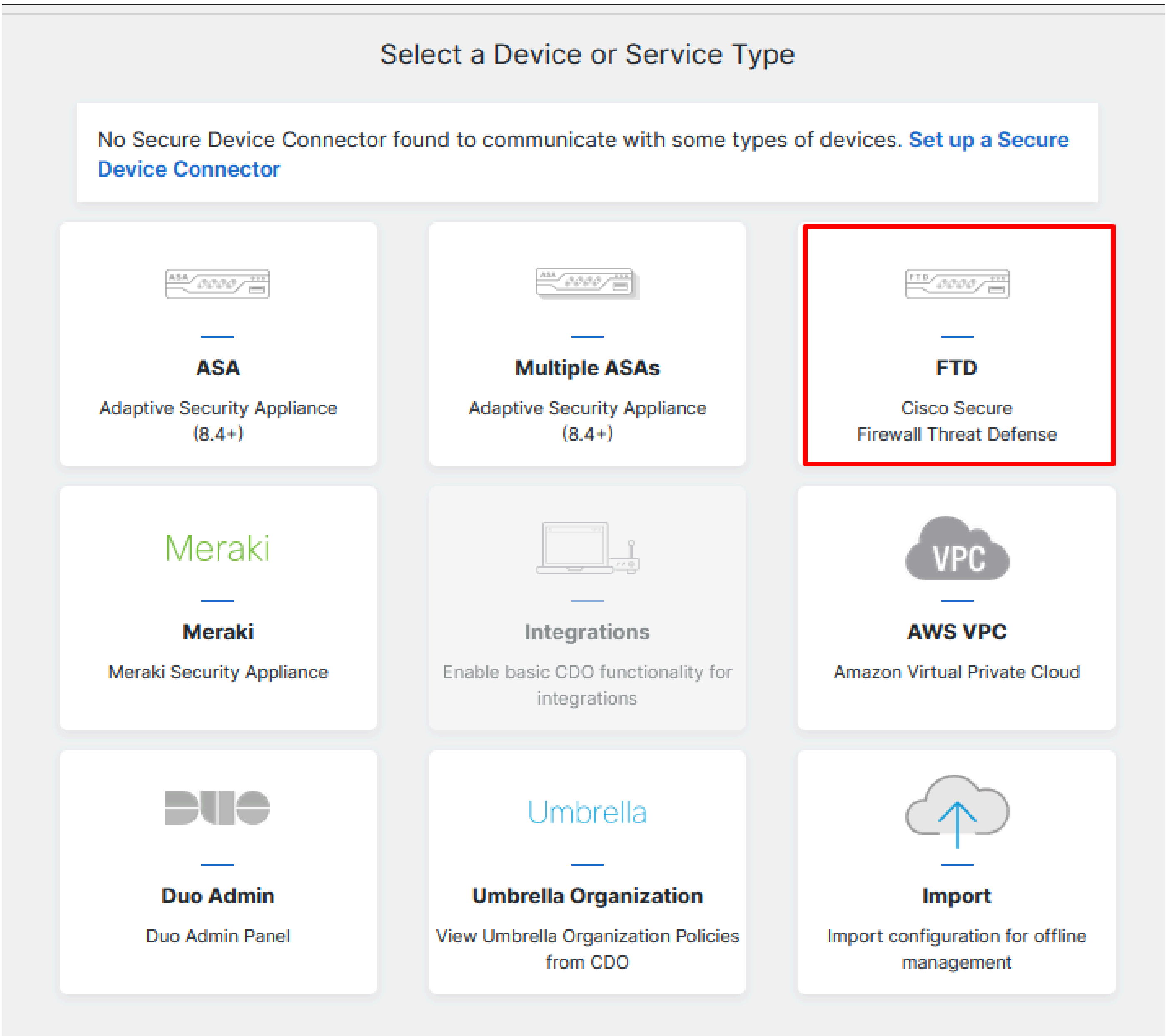
注册密钥可以在CDO中找到。导航至CDO，转至资产>添加符号。

系统将显示一个菜单，用于选择您拥有的设备类型。选择FTD选项。必须启用FDM选项；否则，无法执行相应的迁移。注册类型使用使用注册密钥。在此选项中，注册密钥出现在第3步中，我们必须将其复制并粘贴到FDM中。



板载FDM，添加选项

出现“Select a Device or Service Type（选择设备或服务类型）”菜单。



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 Security Appliance

Integrations
Enable basic CDO functionality for integrations

AWS VPC
Amazon Virtual Private Cloud

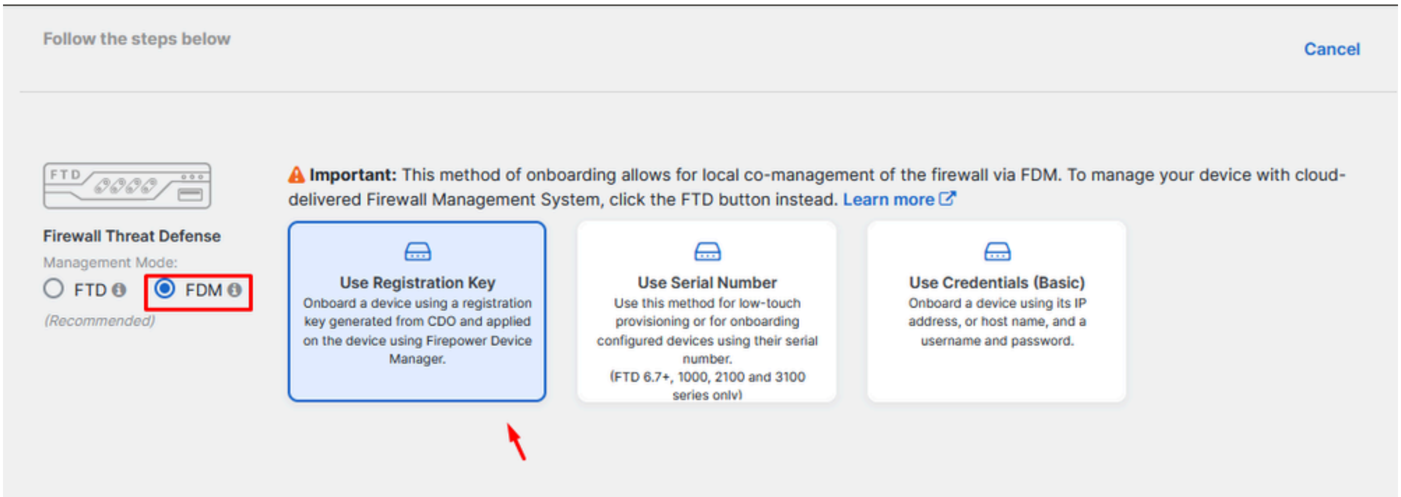
Duo Admin
Duo Admin Panel

Umbrella Organization
View Umbrella Organization Policies from CDO

Import
Import configuration for offline management

选择设备或服务类型

对于此文档，已选择“选择注册密钥”。



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

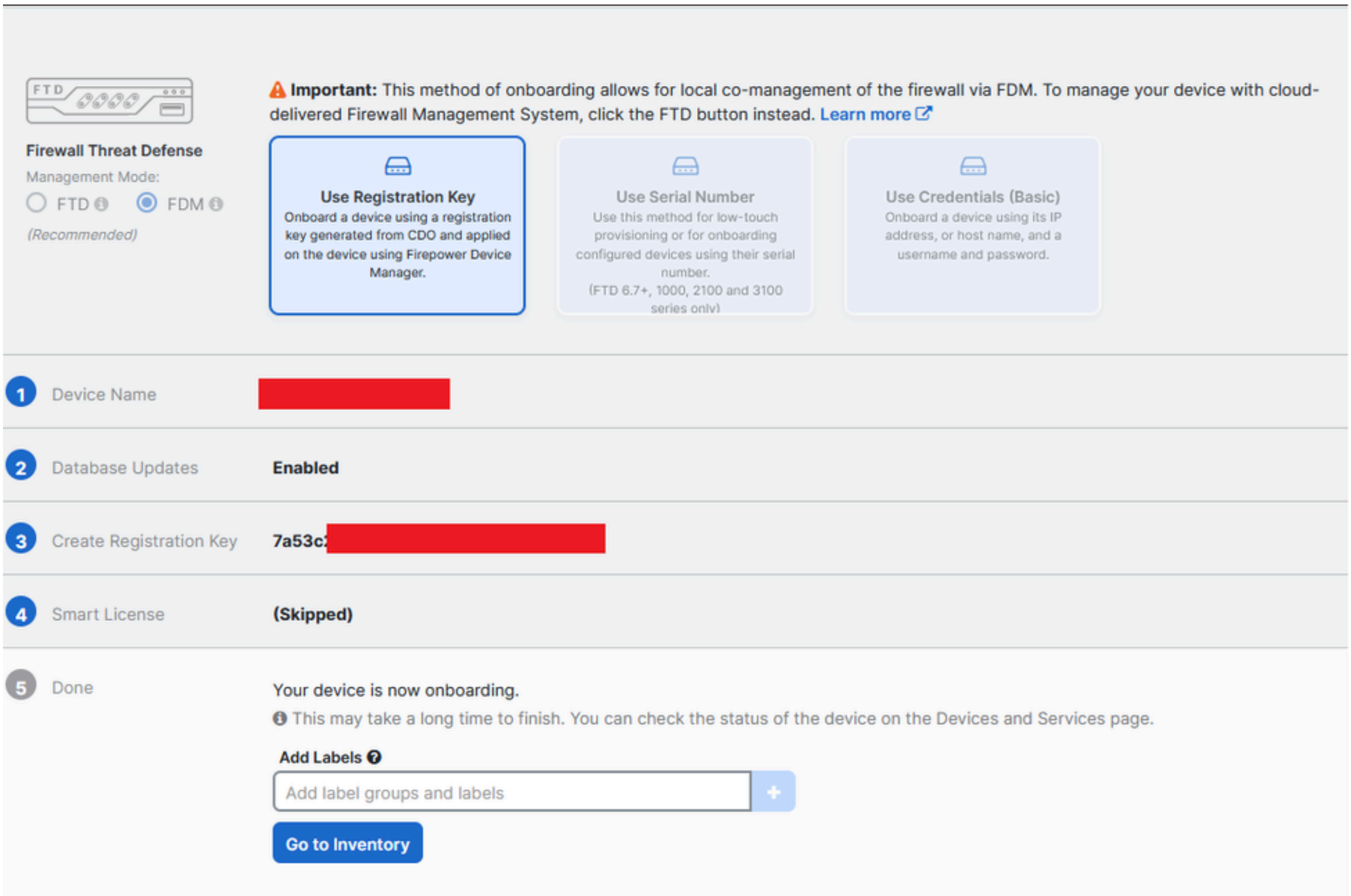
Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

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.

注册类型

此处显示上一步所需的注册密钥。



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

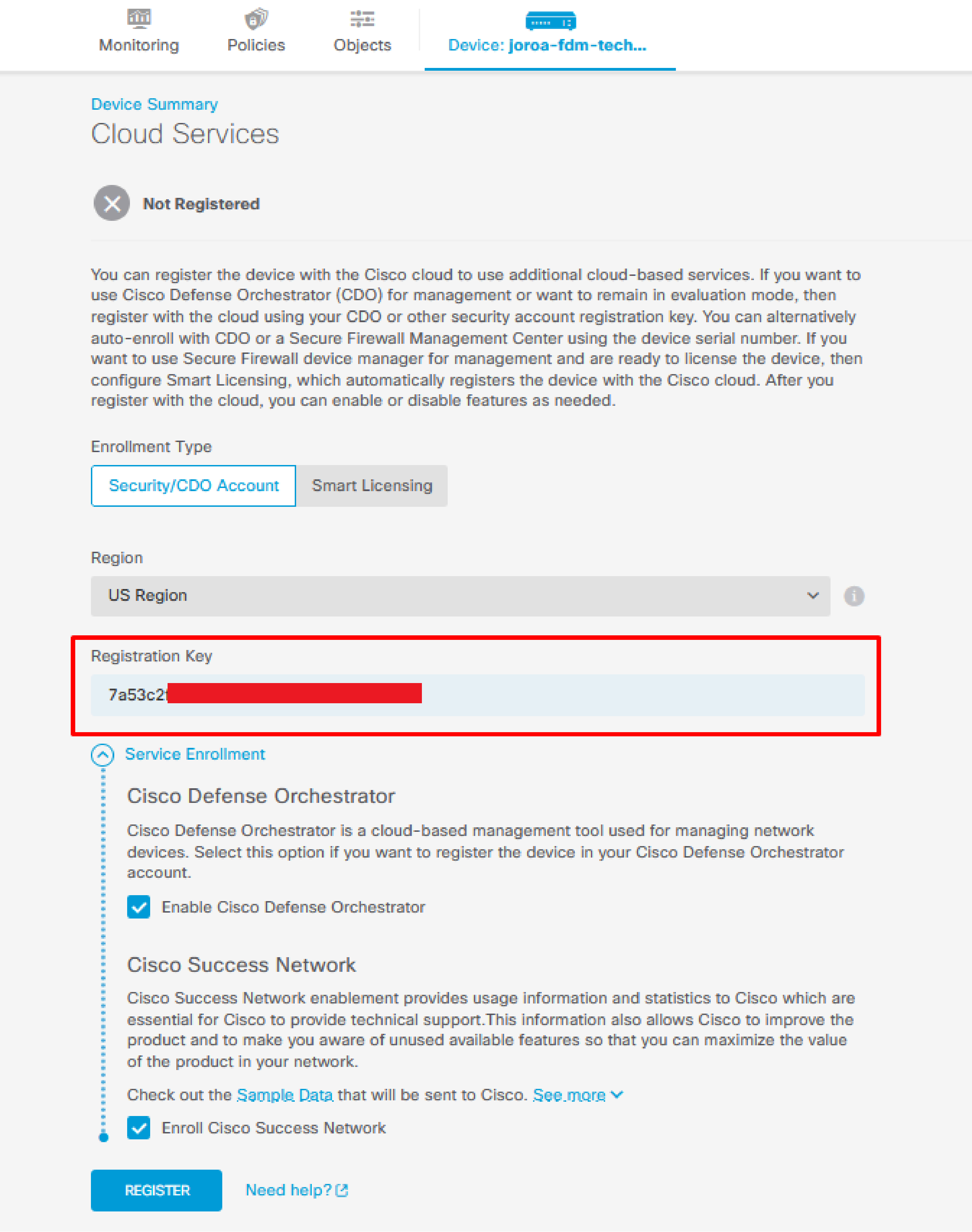
Add label groups and labels

Go to Inventory

注册流程

获取注册密钥后，将其复制并粘贴到FDM中，然后单击注册(Register)。在云服务中注册FDM后，其将显示为启用，如图所示。

已跳过智能许可证，因为设备将在启动并运行后进行注册。



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[redacted]

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

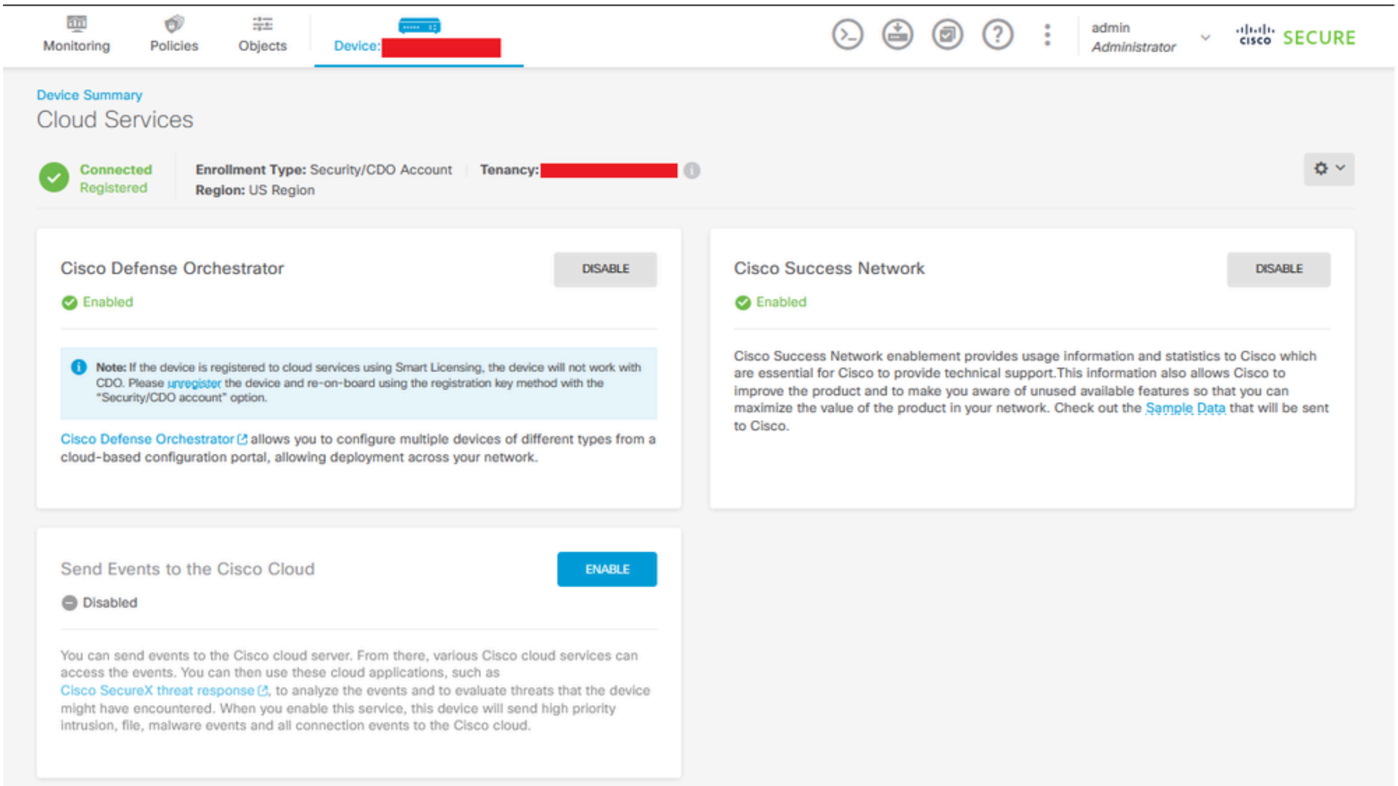
Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support.This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product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

Check out the Sample Data that will be sent to Cisco. See more

☑ Enroll Cisco Success Network

FDM注册

注册FDM时，它将显示租户、已连接和已注册的云服务。



Monitoring | Policies | Objects | Device: [redacted]

admin
Administrator

SECURE

Device Summary
Cloud Services

Connected
Registered

Enrollment Type: Security/CDO Account | **Tenancy:** [redacted]
Region: US Region

Cisco Defense Orchestrator DISABLE
Enabled

Note: If the device is registered to cloud services using Smart Licensing, the device will not work with CDO. Please unregister the device and re-on-board using the registration key method with the "Security/CDO account" option.

Cisco Defense Orchestrator allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network DISABLE
Enabled

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

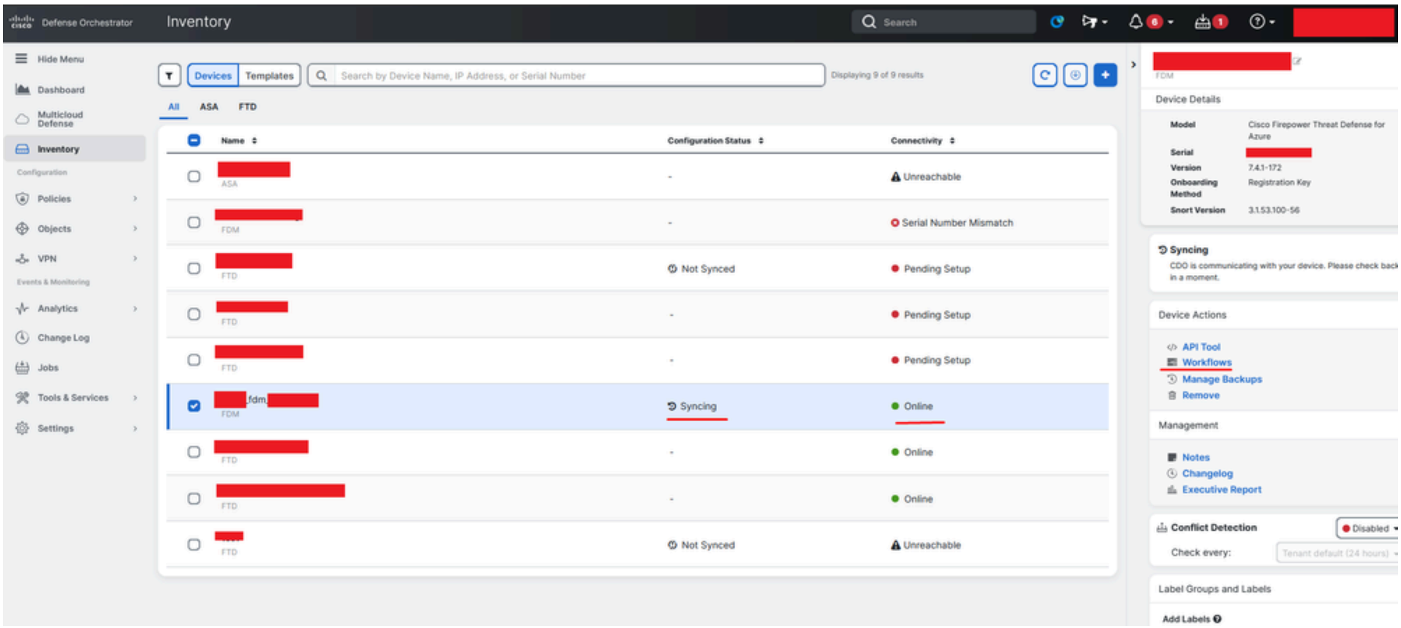
Send Events to the Cisco Cloud ENABLE
Disabled

You can send events to the Cisco cloud server. From there, various Cisco cloud services can access the events. You can then use these cloud applications, such as Cisco SecureX threat response, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.

FDM注册完成

在CDO中的“库存”(Inventory)菜单中，FDM可在入网和同步过程中找到。可以在Workflows部分中查看此同步的进度和流程。

此过程完成后，将显示为“已同步”和“联机”。



Defense Orchestrator — Inventory — Search — [redacted]

Hide Menu
Dashboard
Multicloud Defense
Inventory
Configuration
Policies
Objects
VPN
Events & Monitoring
Analytics
Change Log
Jobs
Tools & Services
Settings

Devices | Templates — Search by Device Name, IP Address, or Serial Number — Displaying 9 of 9 results

All | ASA | FTD

	Name	Configuration Status	Connectivity
☐	[redacted] ASA	-	Unreachable
☐	[redacted] FDM	-	Serial Number Mismatch
☐	[redacted] FTD	Not Synced	● Pending Setup
☐	[redacted] FTD	-	● Pending Setup
☐	[redacted] FTD	-	● Pending Setup
☑	[redacted]_fdm_[redacted] FDM	Syncing	● Online
☐	[redacted] FTD	-	● Online
☐	[redacted] FTD	-	● Online
☐	[redacted] FTD	Not Synced	Unreachable

[redacted]
FDM

Device Details

Model	Cisco Firepower Threat Defense for Azure
Serial	[redacted]
Version	7.4.1-172
Onboarding Method	Registration Key
Snort Version	3.1.53.100-56

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

Device Actions
API Tool
Workflows
Manage Backups
Remove

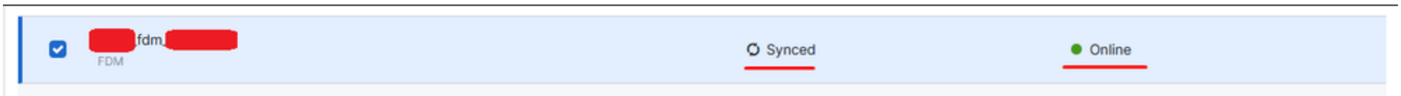
Management
Notes
Changelog
Executive Report

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

Label Groups and Labels
Add Labels

CDO资产FDM已注册

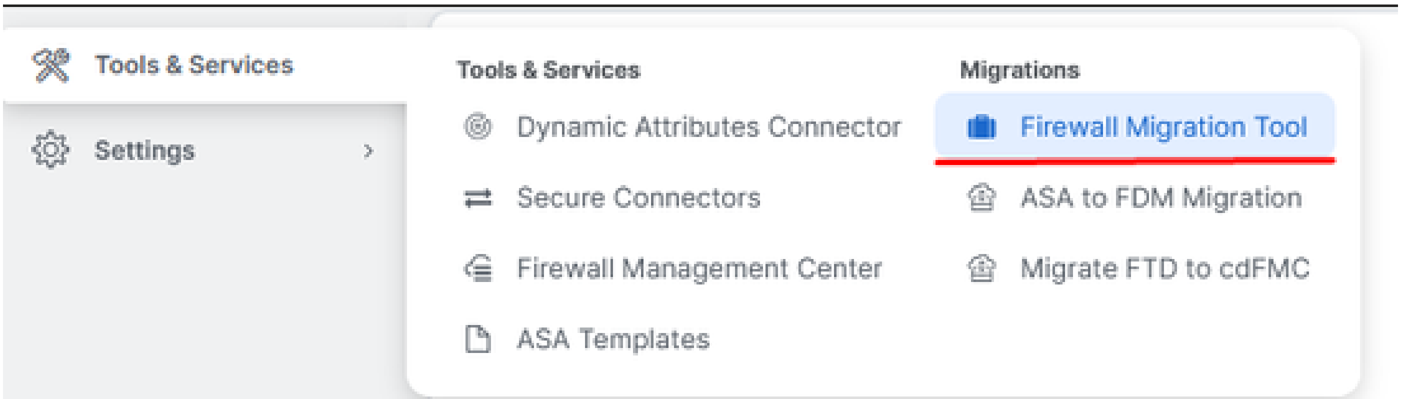
设备同步后，将显示为“联机”和“已同步”。



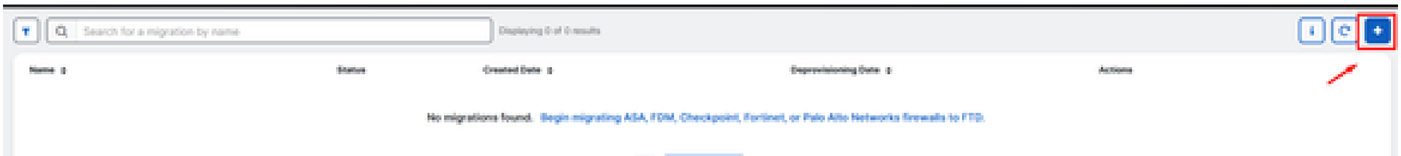
☑	[redacted]_fdm_[redacted] FDM	Synced	● Online

FDM已注册

当FDM成功注册到CDO后，我们必须注销FDM。退出FDM后，在CDO中导航到工具和服务>迁移>防火墙迁移工具。

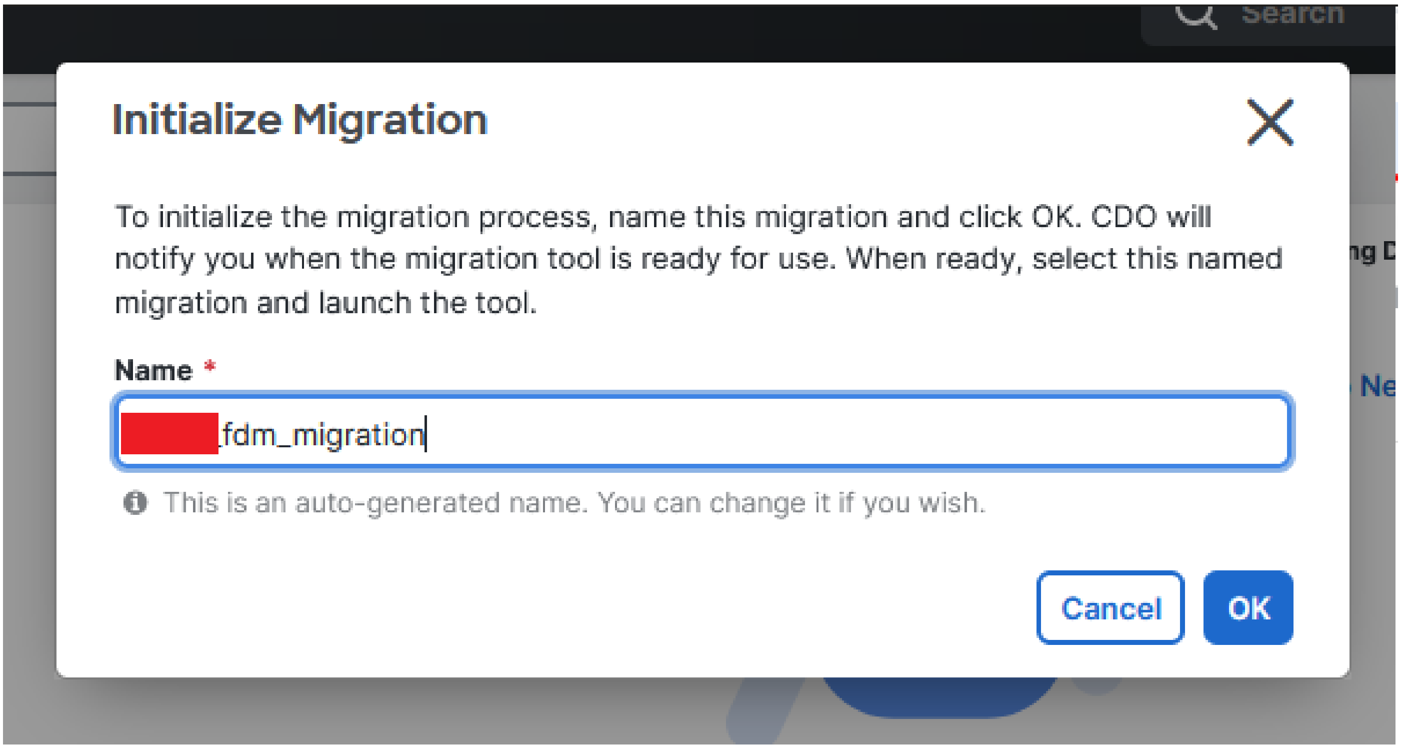


单击Add符号，将显示一个随机名称，表示需要重命名该名称以启动迁移进程。



No migrations found. Begin migrating ASA, FDM, Checkpoint, Fortinet, or Palo Alto Networks firewalls to FTD.

重命名后，单击Launch开始迁移。



Initialize Migration

To initialize the migration process, name this migration and click OK. CDO will notify you when the migration tool is ready for use. When ready, select this named migration and launch the tool.

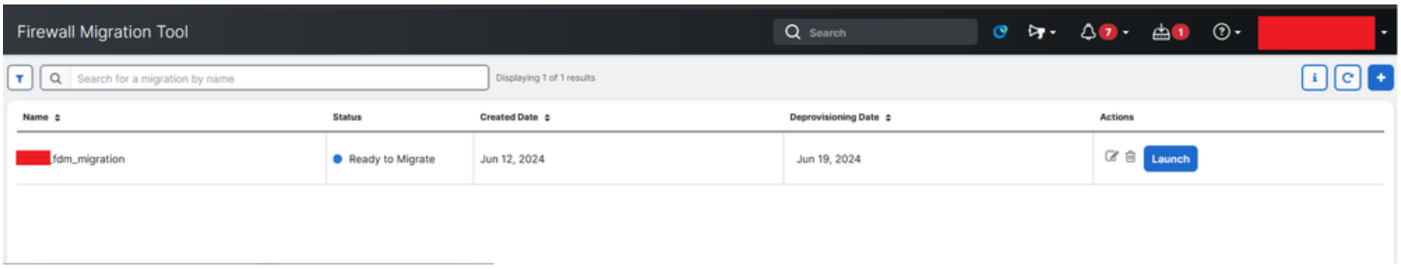
Name *

[redacted]fdm_migration

This is an auto-generated name. You can change it if you wish.

初始化迁移

单击Launch开始迁移配置。



Firewall Migration Tool

Search

[redacted]

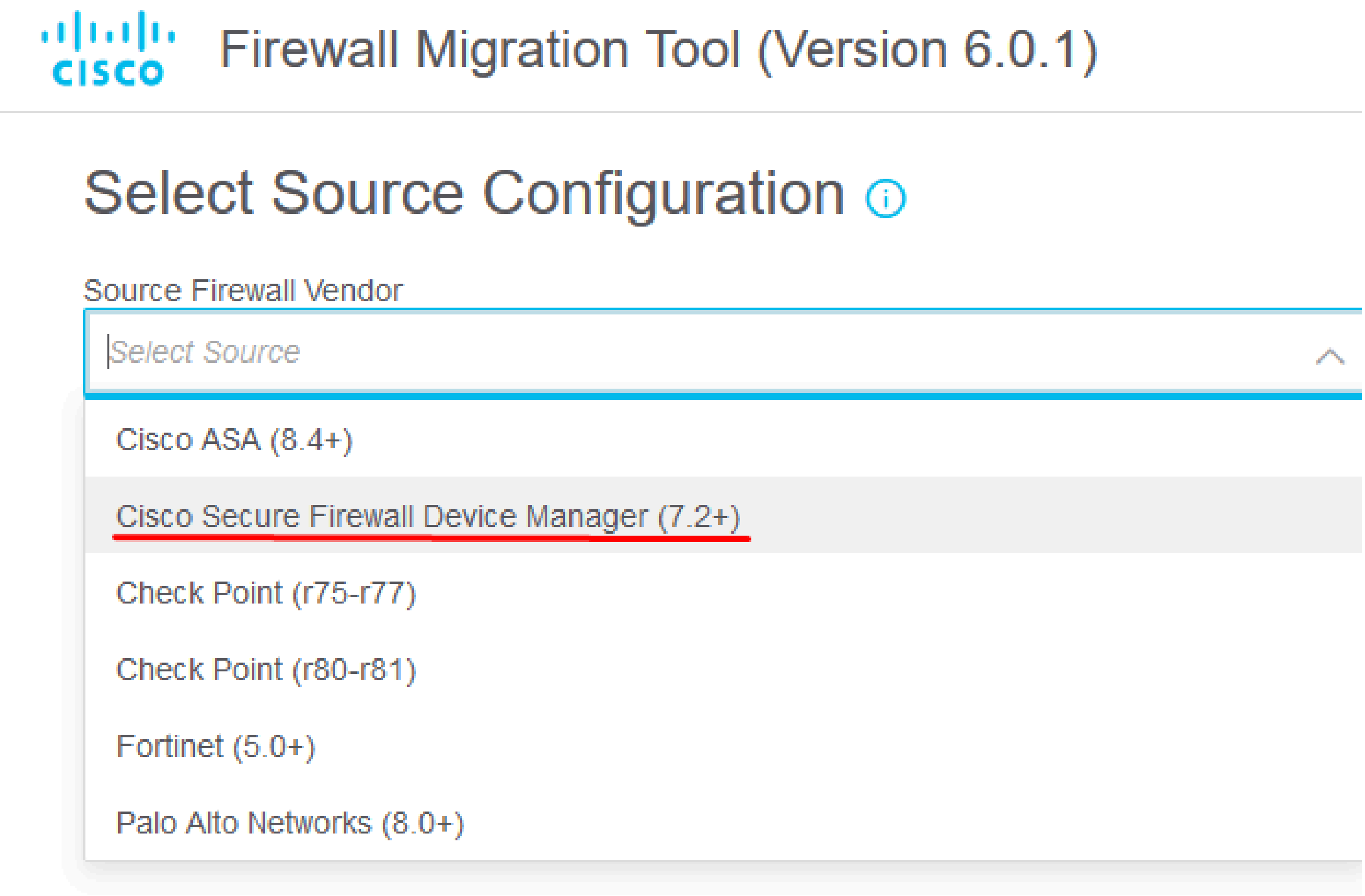
Search for a migration by name

Displaying 1 of 1 results

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

迁移启动流程

单击Launch后，将打开一个窗口，显示选择选项Cisco Secure Firewall Device Manager (7.2+)的迁移过程。如前所述，此选项从版本7.2开始启用。



Firewall Migration Tool (Version 6.0.1)

Select Source Configuration

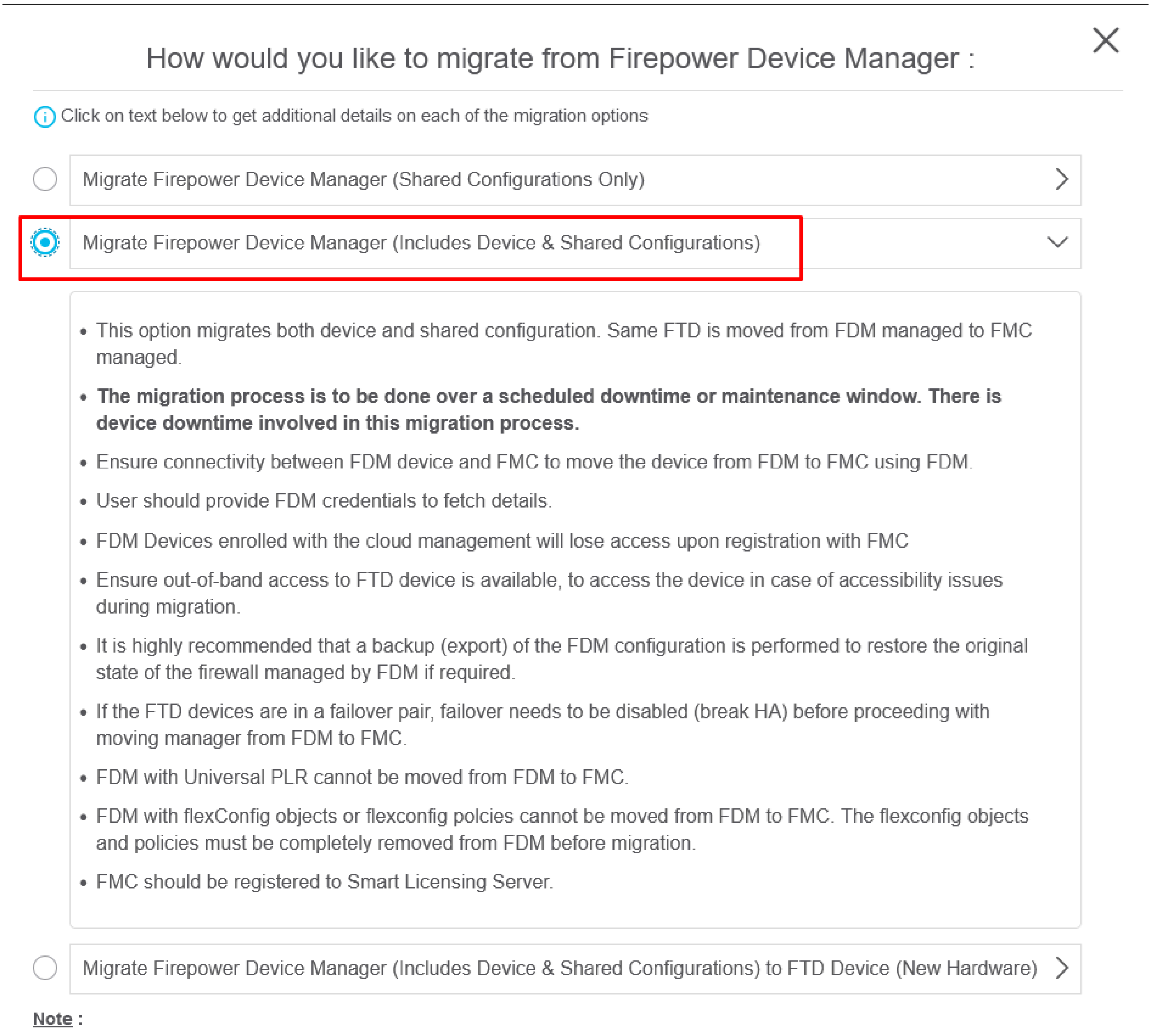
Source Firewall Vendor

Select Source

FMT选择源配置

选择后，系统将显示三种不同的迁移选项：仅共享配置、包括设备和共享配置，以及从“设备和共享配置”到“FTD新硬件”。

对于此实例，将执行第二个选项“迁移Firepower设备管理器”(Migrate Firepower Device Manager)（包括设备和共享配置）。



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)

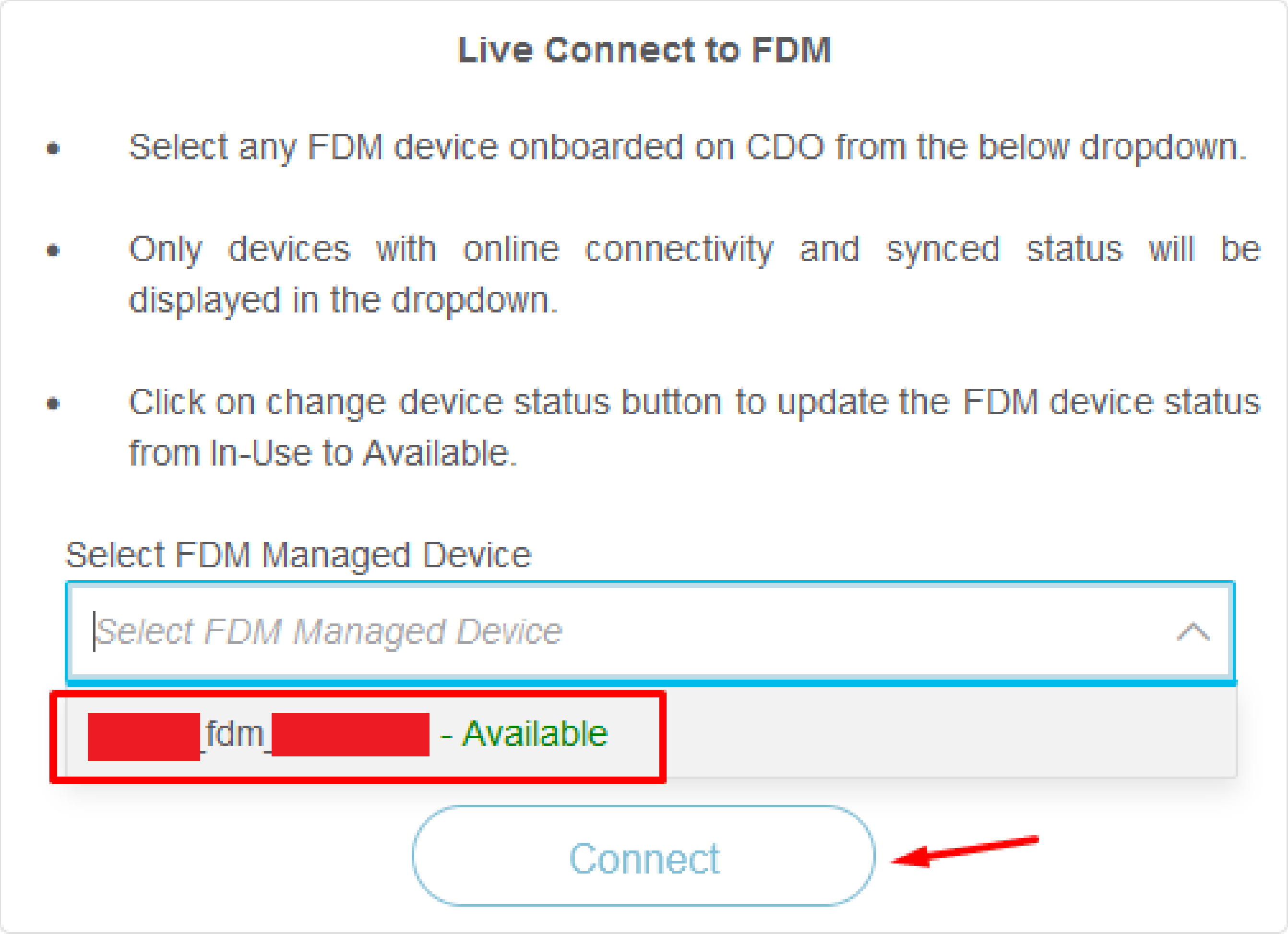
- This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
- **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
- Ensure connectivity between FDM device 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 polcies 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 :

迁移选项

选择迁移方法后，继续从提供的列表中选择设备。



Live Connect to FDM

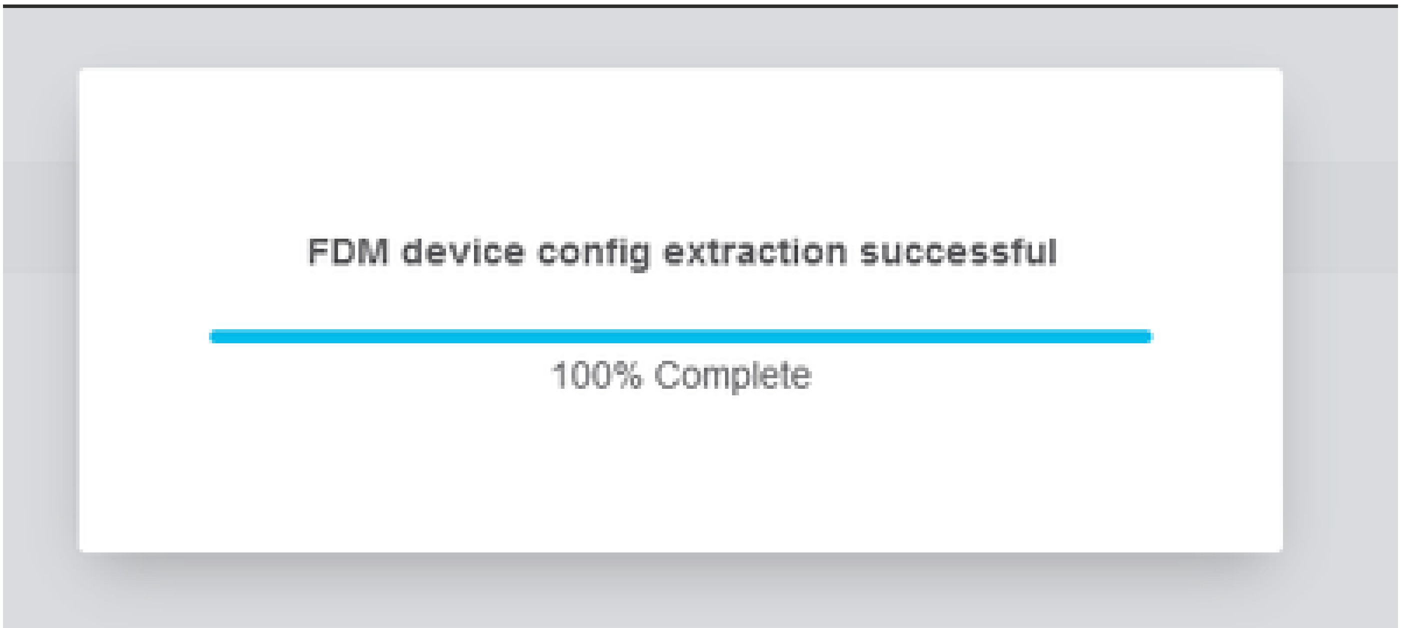
- Select any FDM device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.
- Click on change device status button to update the FDM device status from In-Use to Available.

Select FDM Managed Device

Select FDM Managed Device

[redacted]_fdm_[redacted] - Available

FDM设备选择

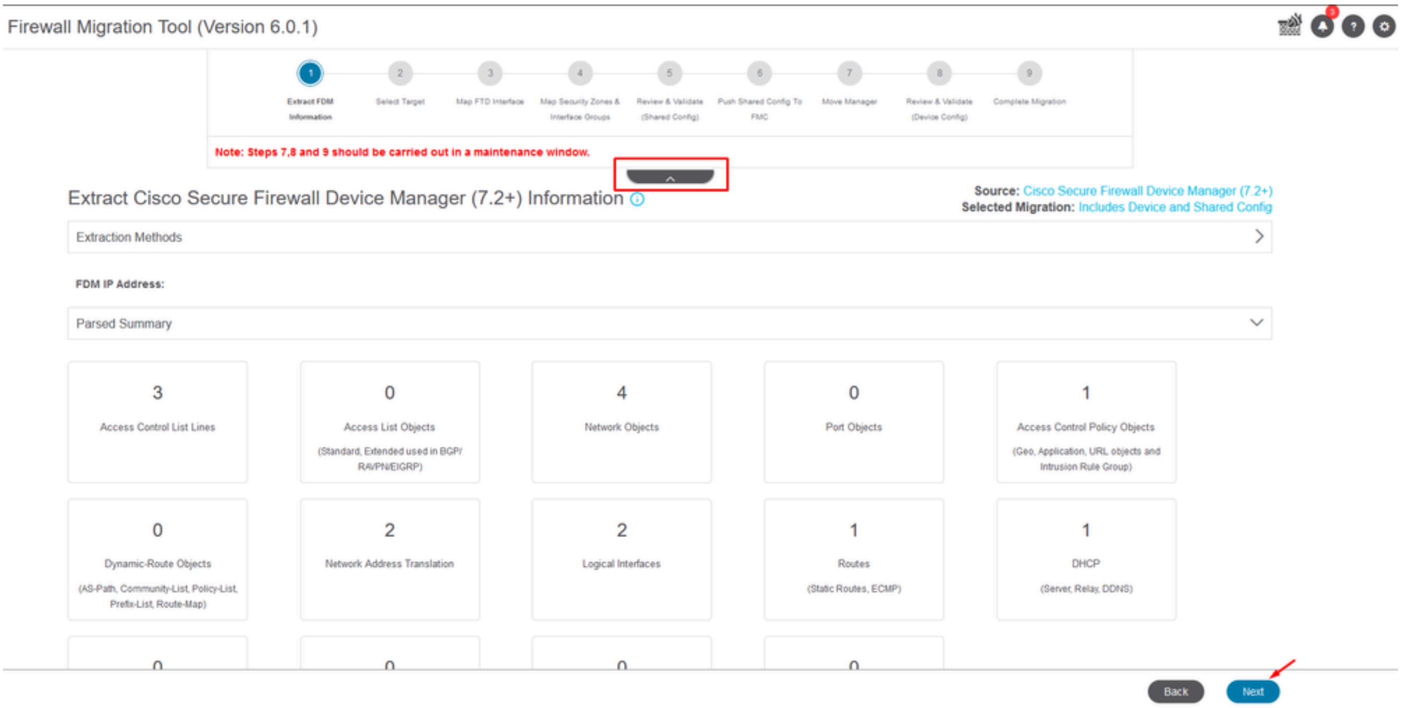


FDM device config extraction successful

100% Complete

配置提取已完成

建议打开顶部的选项卡，查看并了解选择设备时的步骤。



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
Back
Next

Firewall Migration Tool (Version 6.0.1)

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

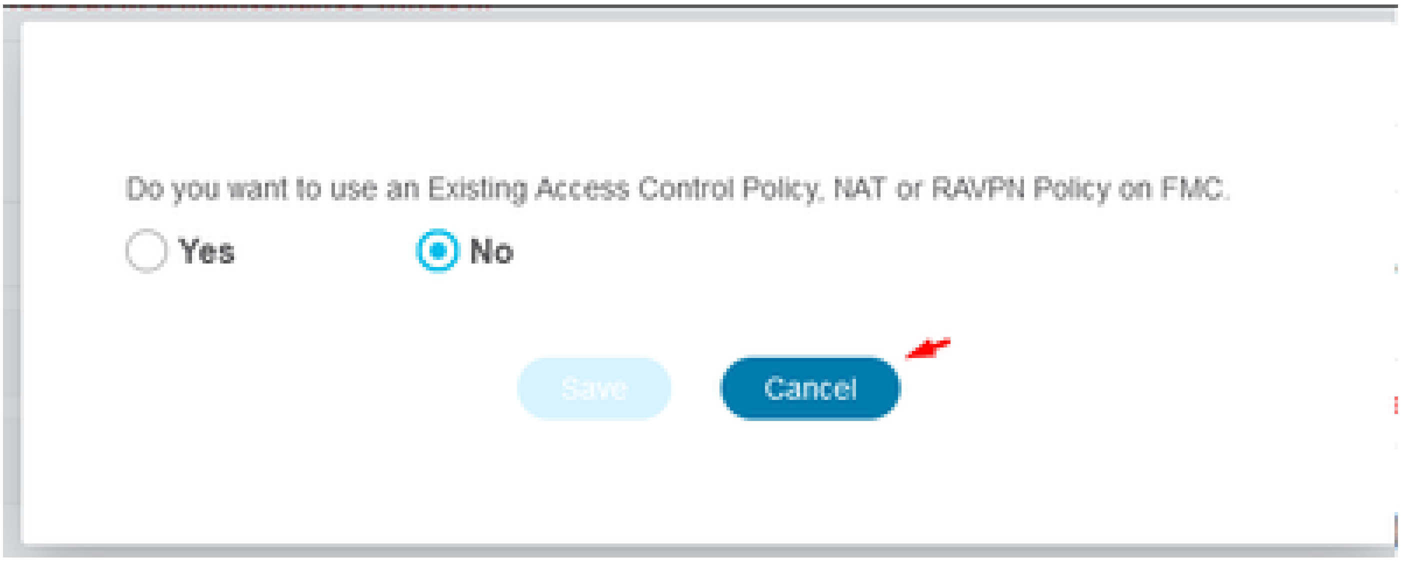
FDM IP Address:

Parsed Summary

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

迁移过程的步骤

作为新迁移，请在系统提示时选择Cancel选项“Do you want to use an Existing Access Control Policy， NAT or RAVPN Policy on FMC？”

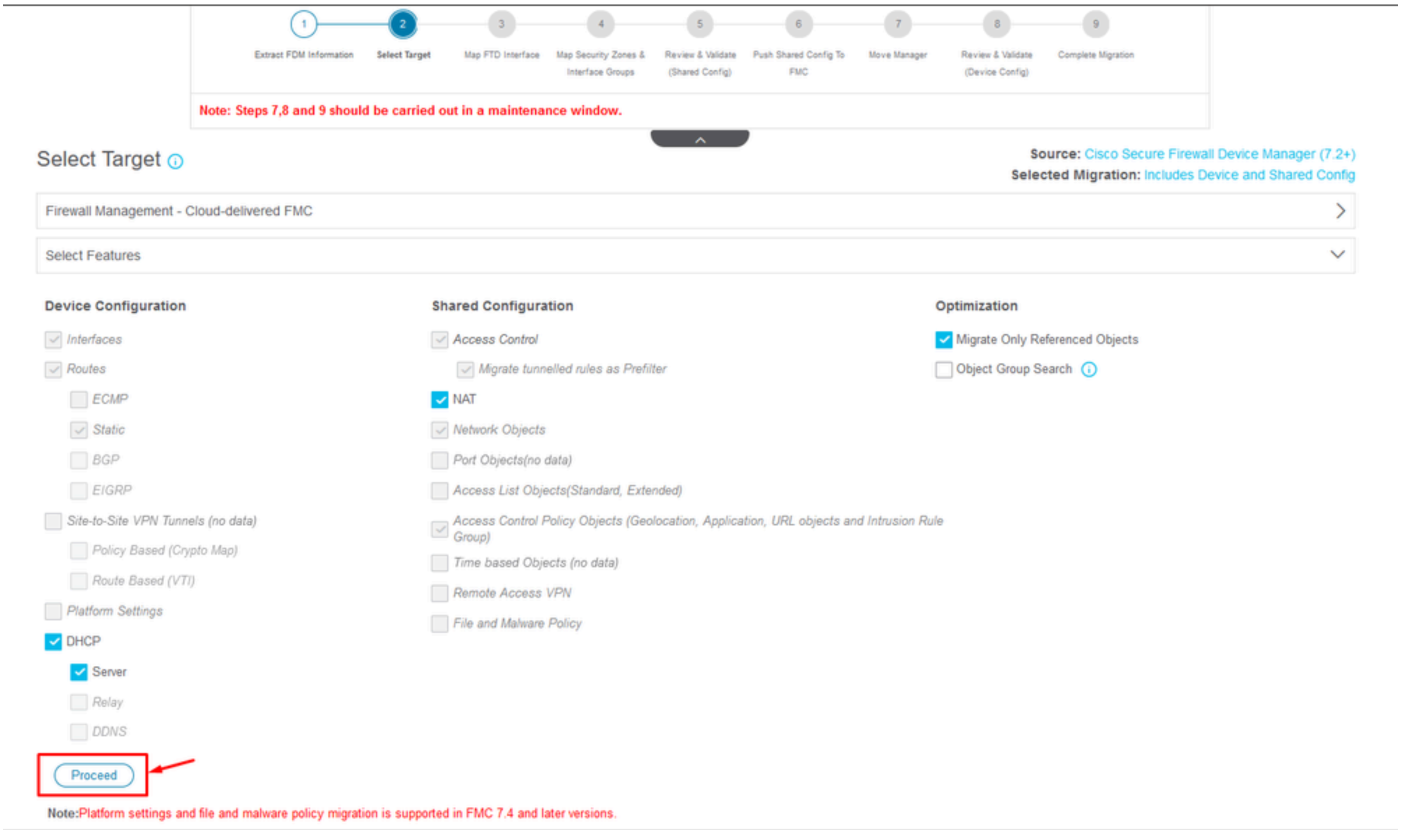


Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.

○ Yes ● No

现有配置的取消选项

然后，系统将提供用于选择要迁移的功能（如图所示）的选项。单击Proceed。



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.

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

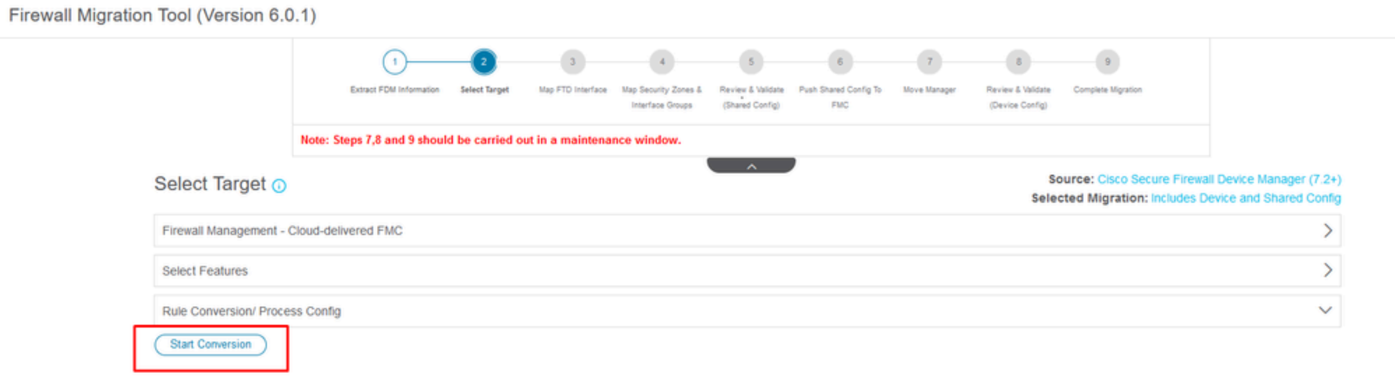
Optimization

- ☑ Migrate Only Referenced Objects
- □ Object Group Search

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

要选择的功能

然后Start Conversion。



Firewall Migration Tool (Version 6.0.1)

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

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

Select Target

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

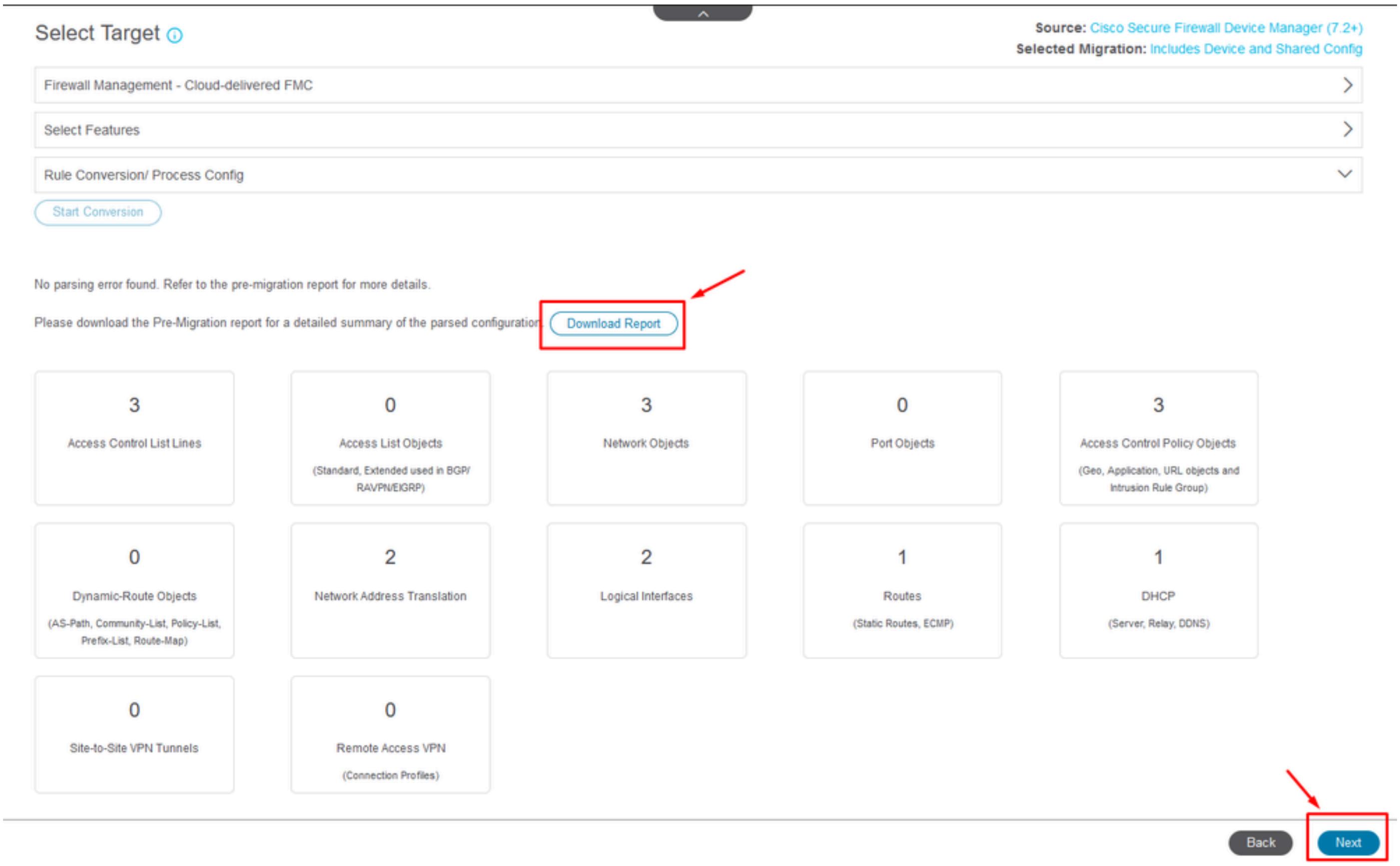
Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

开始转换。

解析过程结束后，可以使用两个选项：下载文档并通过点击下一步继续迁移。


Select Target
Firewall Management - Cloud-delivered FMC
Select Features
Rule Conversion/ Process Config
Start Conversion
Download Report
Back
Next

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

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

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)

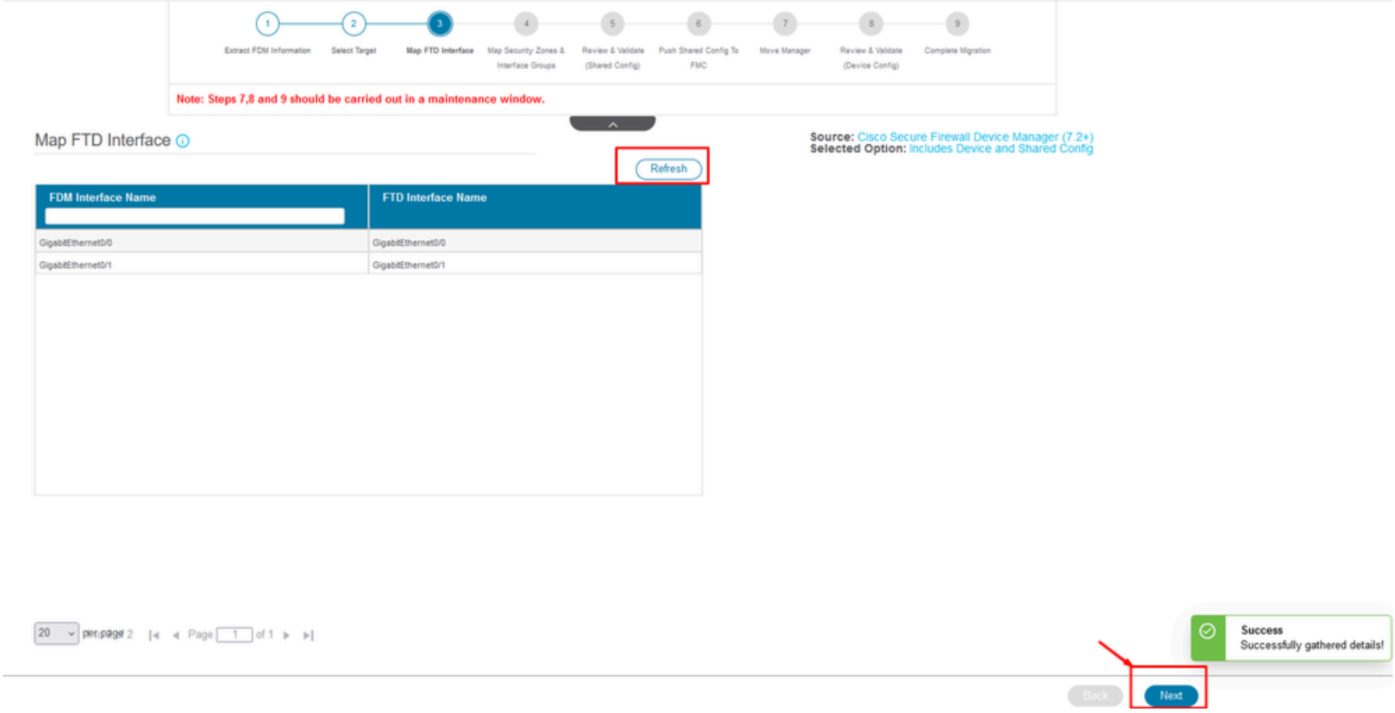
1 DHCP (Server, Relay, DDNS)

0 Site-to-Site VPN Tunnels

0 Remote Access VPN (Connection Profiles)

下载报告.

设备接口设置为显示。最佳做法是单击Refresh更新接口。验证完成后，您可以点击下一步继续。


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
Map FTD Interface
Refresh
20 per page 2 Page 1 of 1
Back
Next

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

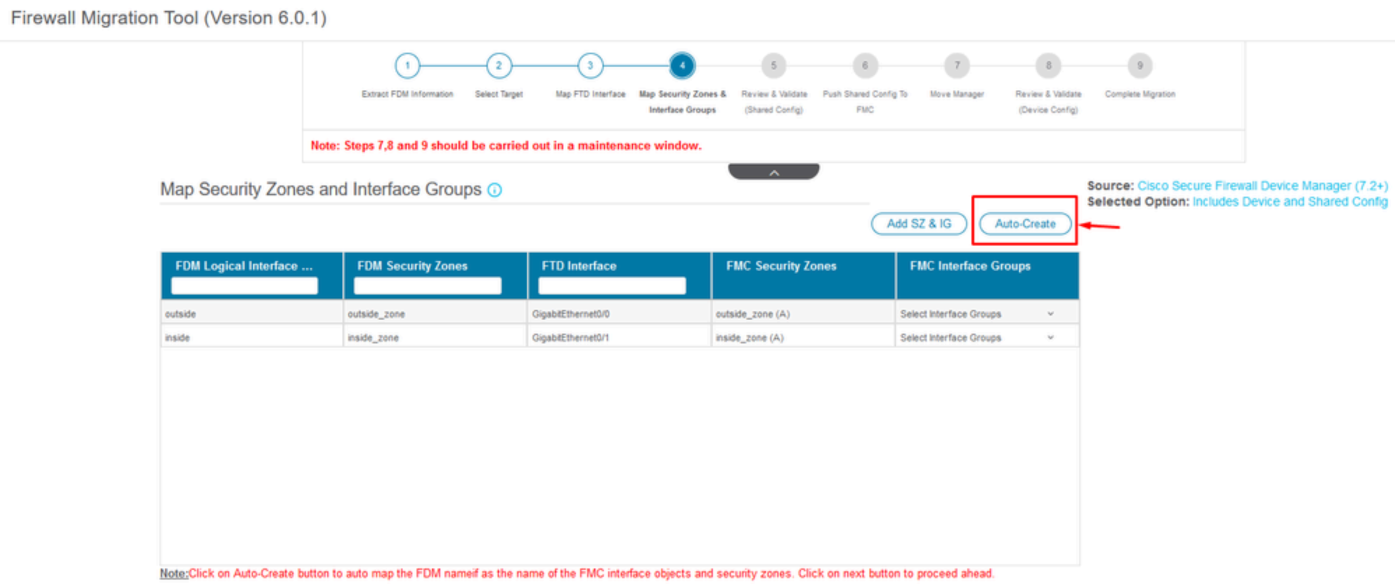
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Interface Name	FTD Interface Name
GigabitEthernet0/0	GigabitEthernet0/0
GigabitEthernet0/1	GigabitEthernet0/1

Success
Successfully gathered details!

显示的接口

导航到安全区域和接口组部分，需要在这里使用添加SZ和IG手动添加。 对于本示例，已选择Auto-Create。这有助于在要迁移到的FMC内自动生成接口。完成后，单击Next按钮。



Firewall Migration Tool (Version 6.0.1)

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

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

Map Security Zones and Interface Groups

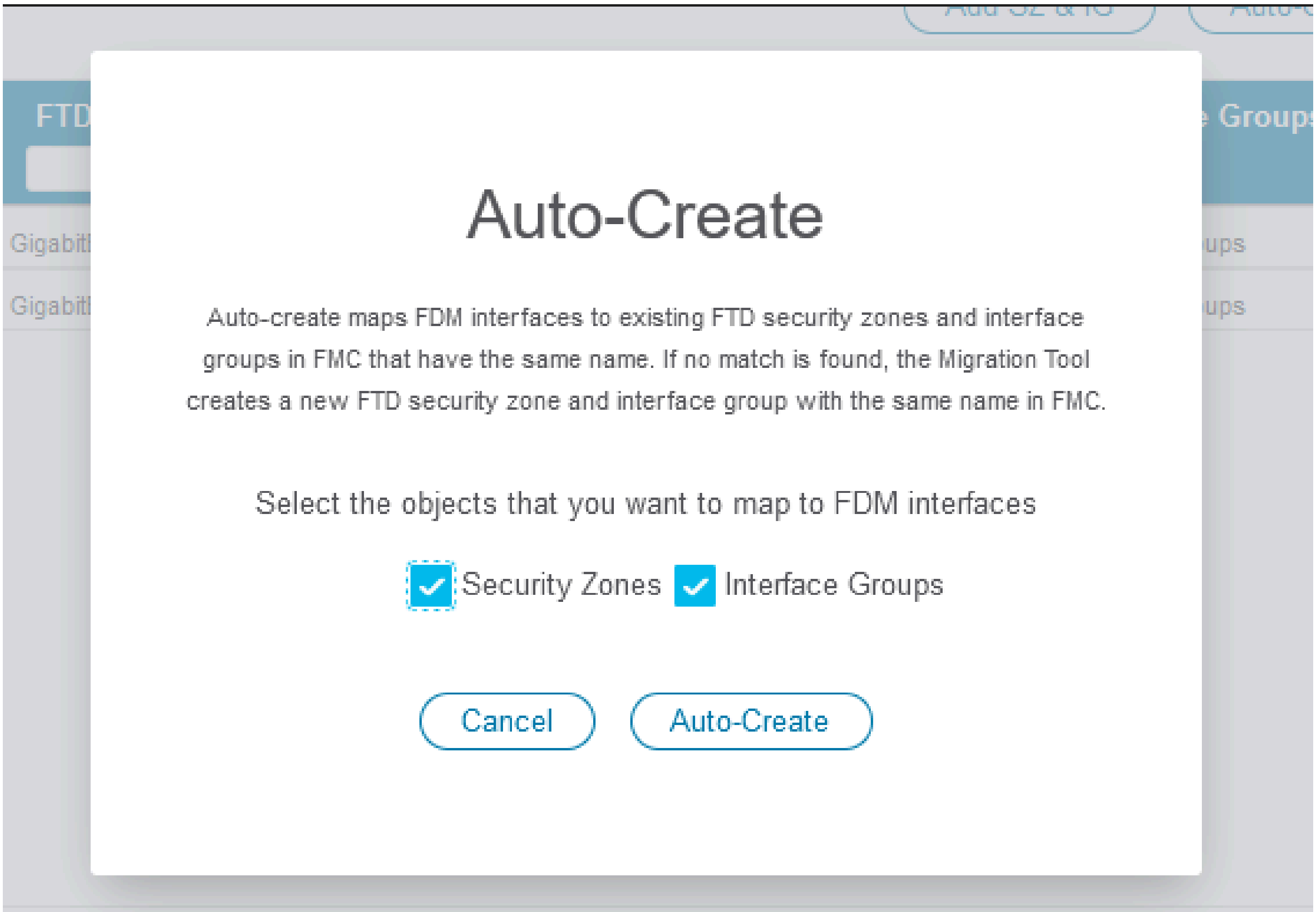
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

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

安全区域和接口组

Auto-Create选项将FDM接口映射到具有相同名称的现有FTD安全区域和FMC中的接口组。



Auto-Create

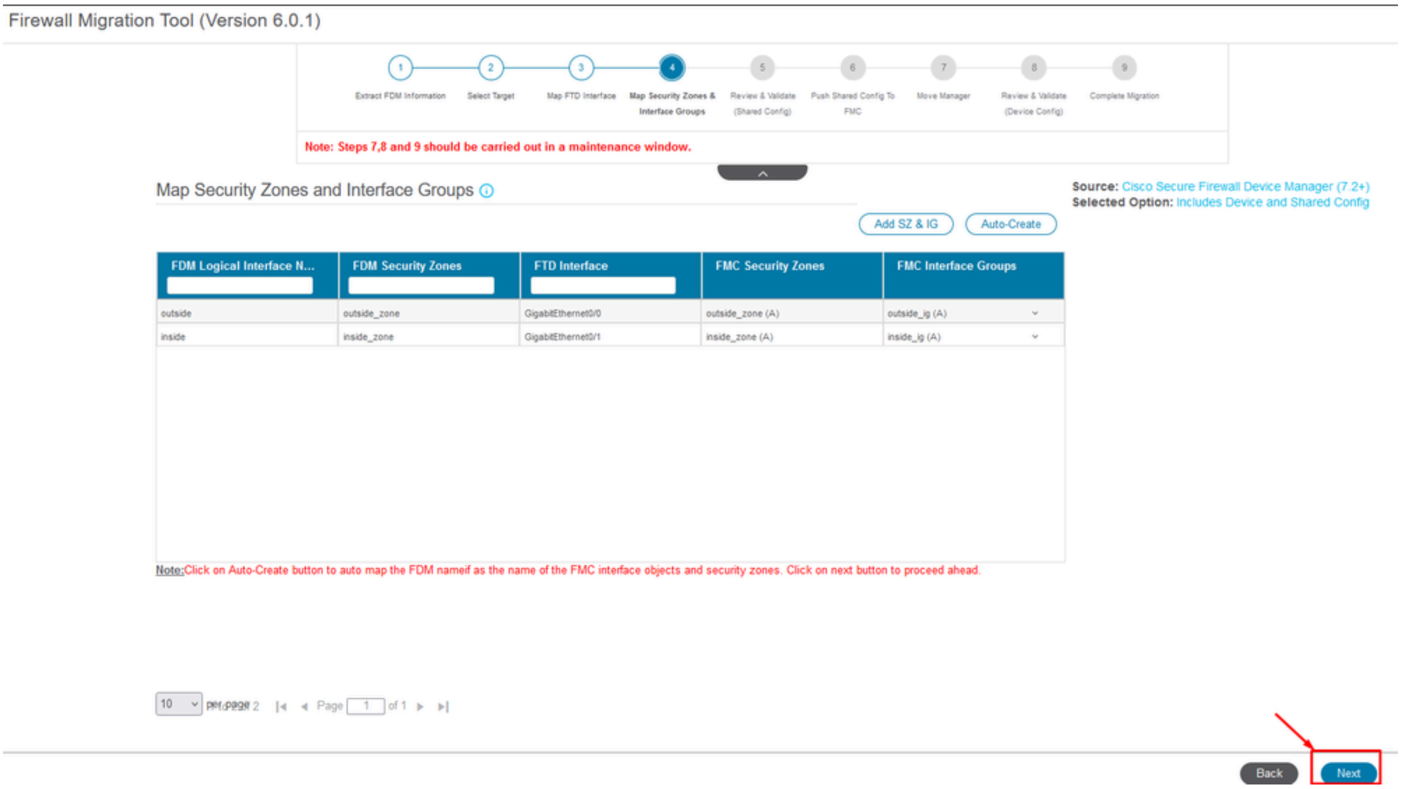
Auto-create maps FDM interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to FDM interfaces

☑ Security Zones ☑ Interface Groups

Auto-Create选项。

然后选择Next。


Firewall Migration Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration
Add SZ & IG
Auto-Create
10 per page
Page 1 of 1
Back
Next

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

Map Security Zones and Interface Groups

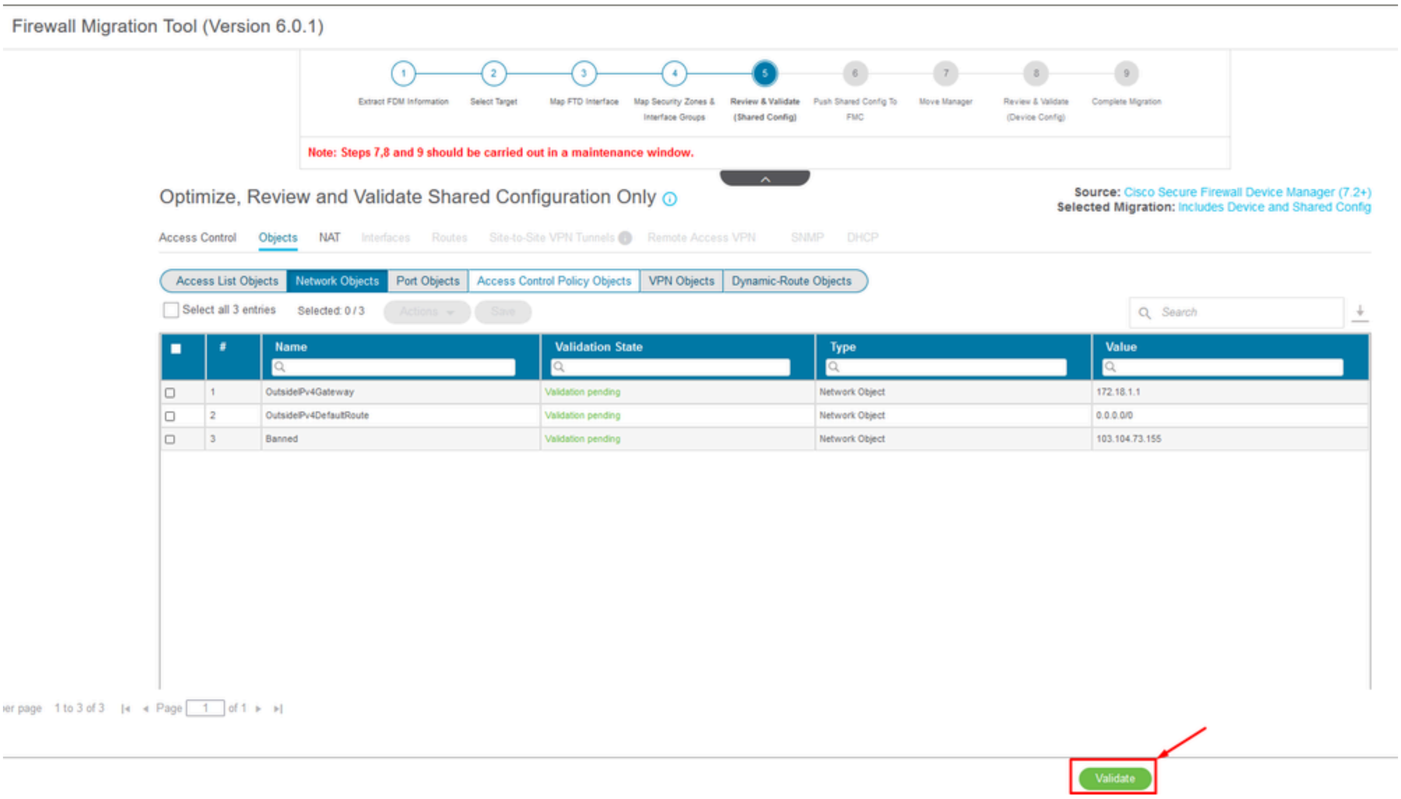
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Logical Interface 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 nameif as the name of the FMC interface objects and security zones. Click on next button to proceed ahead.

After-Creation选项。

在步骤5中，如顶部栏中所示，请花时间检查访问控制策略(ACP)、对象和NAT规则。继续仔细检查每个项目，然后单击Validate确认名称或配置没有问题。



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

Optimize, Review and Validate Shared Configuration Only

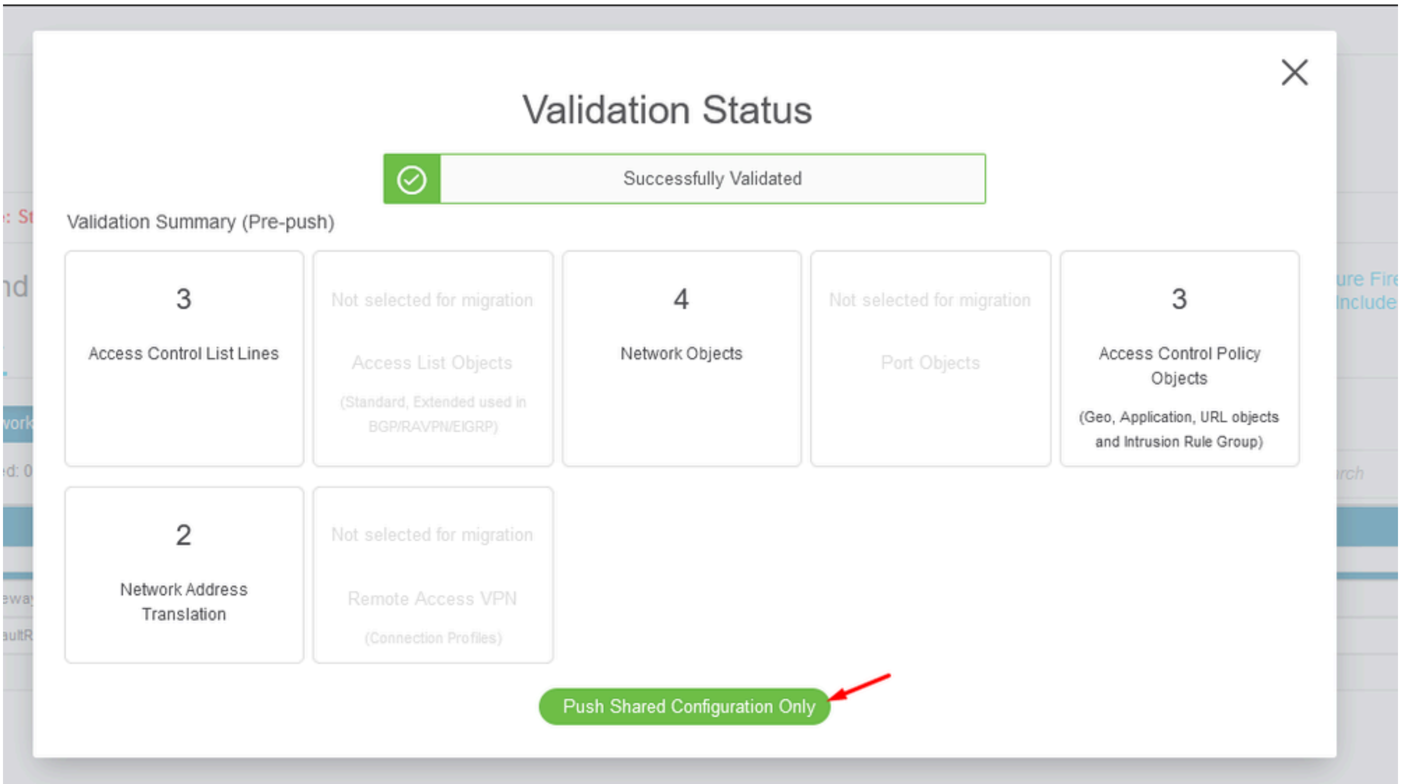
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

□ Select all 3 entries Selected: 0 / 3

■	#	Name	Validation State	Type	Value
□	1	OutsideIPv4Gateway	Validation pending	Network Object	172.18.1.1
□	2	OutsideIPv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
□	3	Banned	Validation pending	Network Object	103.104.73.155

访问控制、对象和NAT配置

然后仅推送共享配置



Validation Status

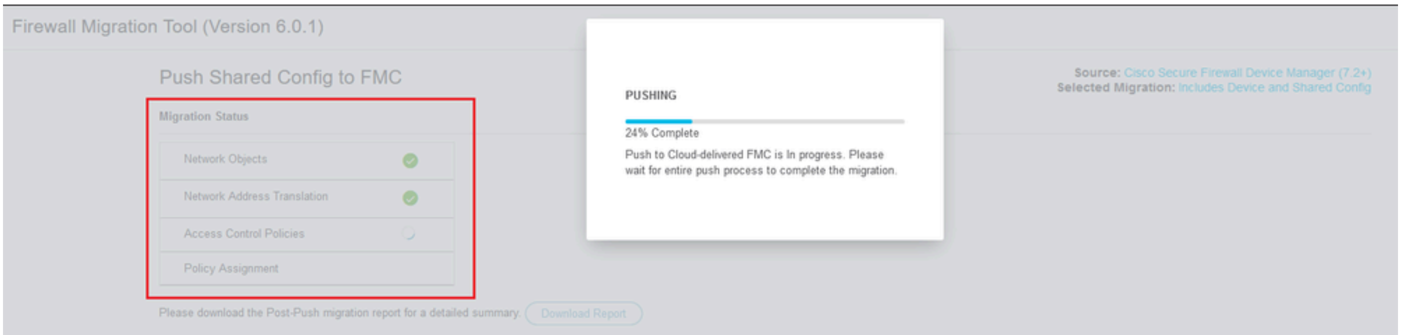
Successfully Validated

Validation Summary (Pre-push)

3 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2 Network Address Translation	Not selected for migration Remote Access VPN (Connection Profiles)			

仅推送共享配置

可以观察到完成的百分比和正在处理的特定任务。



Firewall Migration Tool (Version 6.0.1)

Push Shared Config to FMC

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

Migration Status

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

Please download the Post-Push migration report for a detailed summary.

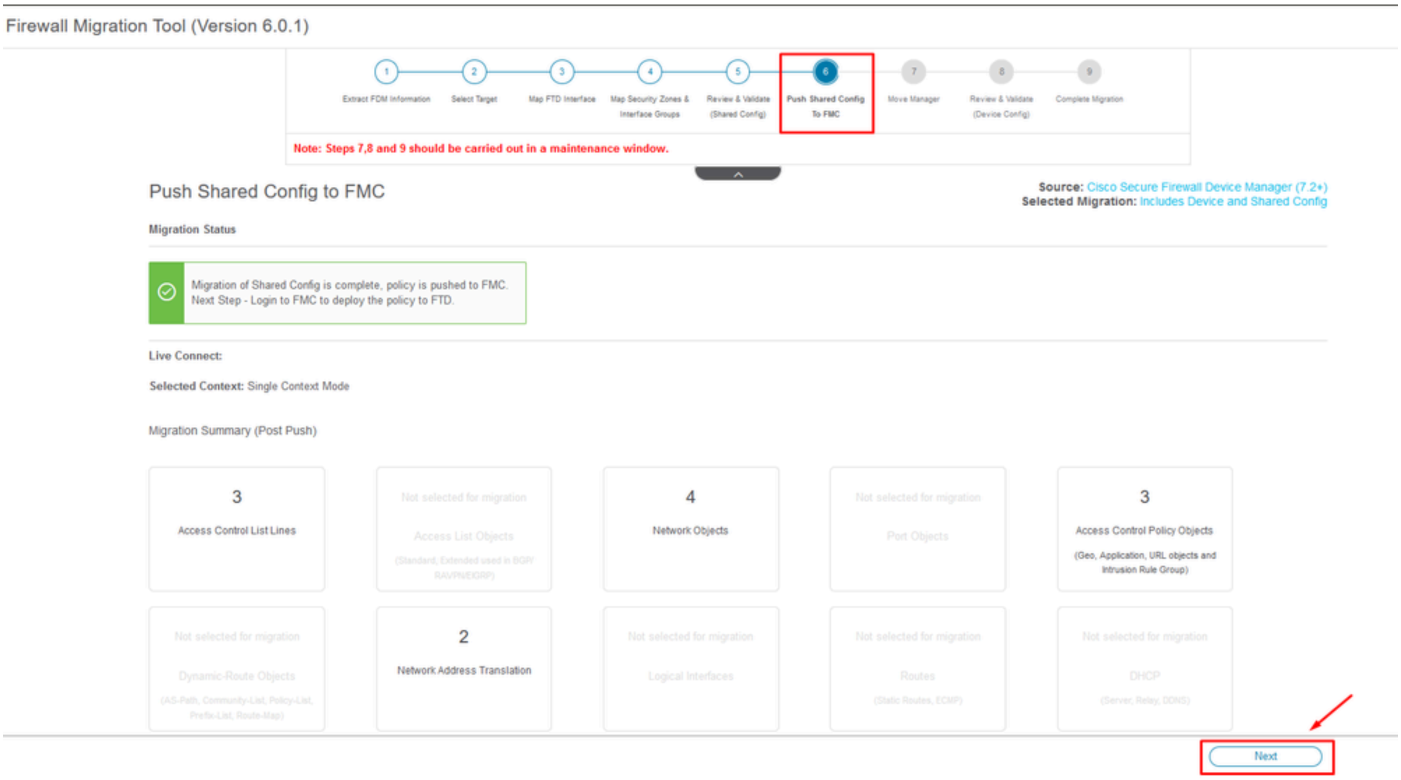
PUSHING

24% Complete

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

推送百分比

完成步骤5后，继续执行步骤6（如顶部栏所示），此时将将共享配置推送到FMC发生。此时，请选择Next按钮前进。



Firewall Migration Tool (Version 6.0.1)

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

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

Push Shared Config to FMC

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

Migration Status

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

Live Connect:

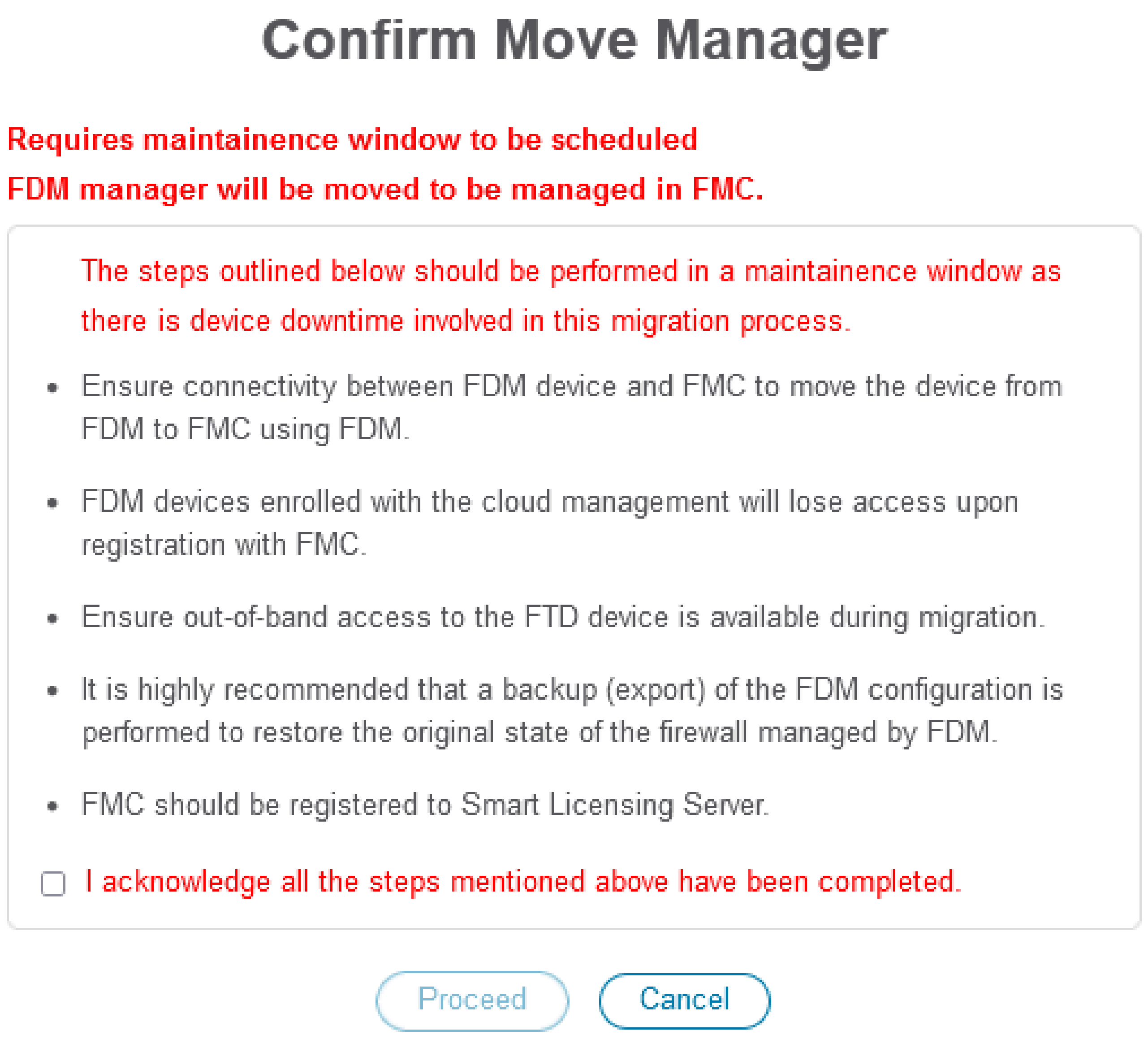
Selected Context: Single Context Mode

Migration Summary (Post Push)

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

将共享配置推送到FMC已完成

此选项会触发确认消息，提示继续管理器迁移。



Confirm Move Manager

Requires maintainence window to be scheduled

FDM manager will be moved to be managed in FMC.

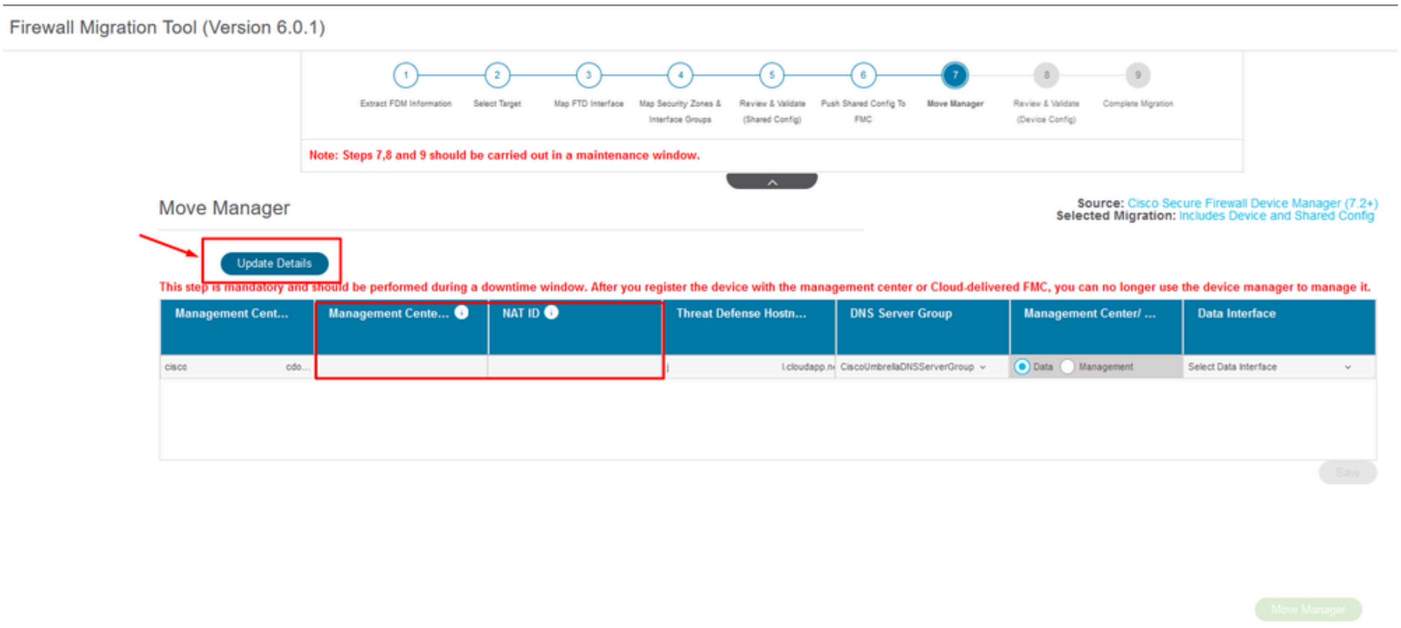
The steps outlined below should be performed in a maintainence window as there is device downtime involved in this migration process.

- 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.

确认移动管理器

继续管理员迁移需要拥有管理中心ID和NAT ID，这是必不可少的。通过选择Update Details，可以检索这些ID。此操作将启动一个弹出窗口，在此窗口中输入cdFMC中FDM表示的所需名称，然后保存更改。


Firewall Migration Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration
Update Details
Save
Move Manager

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

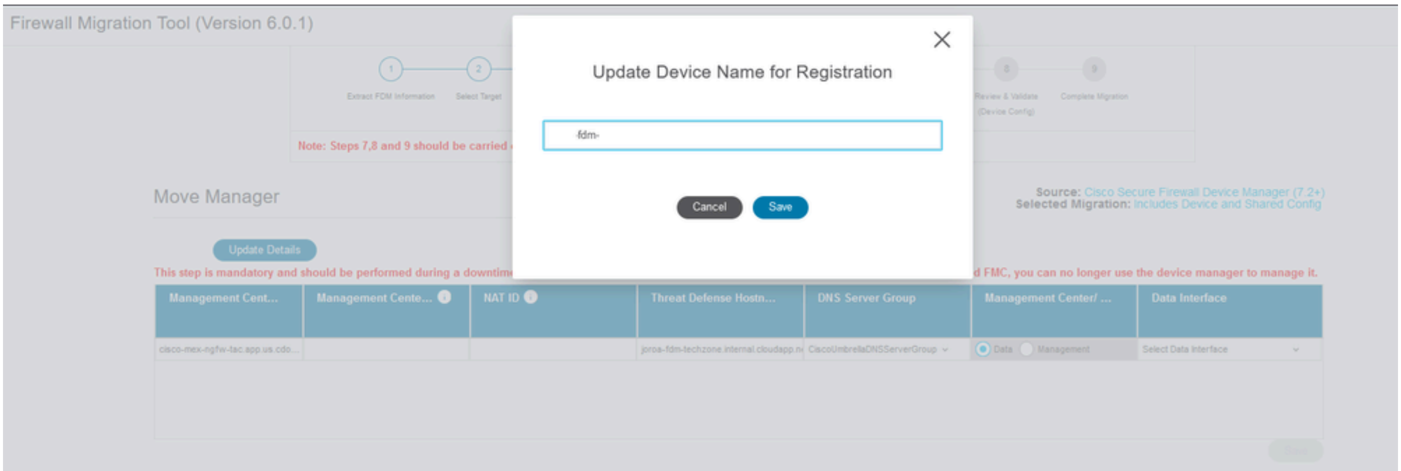
Move Manager

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

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...			j l.cloudapp.n	CiscoUmbrellaDNSServerGroup ⌄	● Data ○ Management	Select Data Interface ⌄

管理员中心ID和NAT ID


Firewall Migration Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
8 Review & Validate (Device Config)
9 Complete Migration
Cancel
Save
Update Details

Update Device Name for Registration

-fdm-

Note: Steps 7,8 and 9 should be carried

Move Manager

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

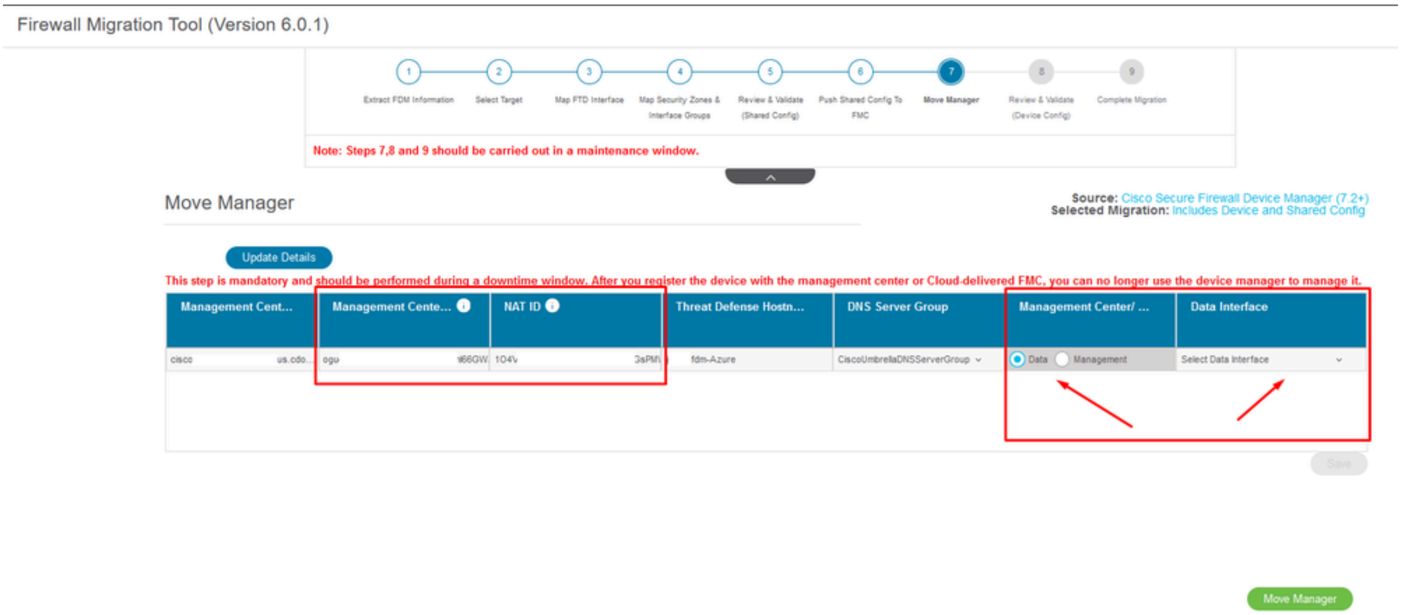
This step is mandatory and should be performed during a downtim d FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente... ⓘ	NAT ID ⓘ	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco-mex-ngfw-tac.app.us.cdo...			joroa-fdm-techzone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup ⌄	● Data ○ Management	Select Data Interface ⌄

更新设备名称以进行注册。

执行此操作后，将显示上述字段的ID。

警告：请勿对管理中心界面进行任何更改。默认情况下，Management选项处于选中状态，保留该选项为默认设置。


Firewall Migration Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration
Update Details
Save
Move Manager

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

Move Manager

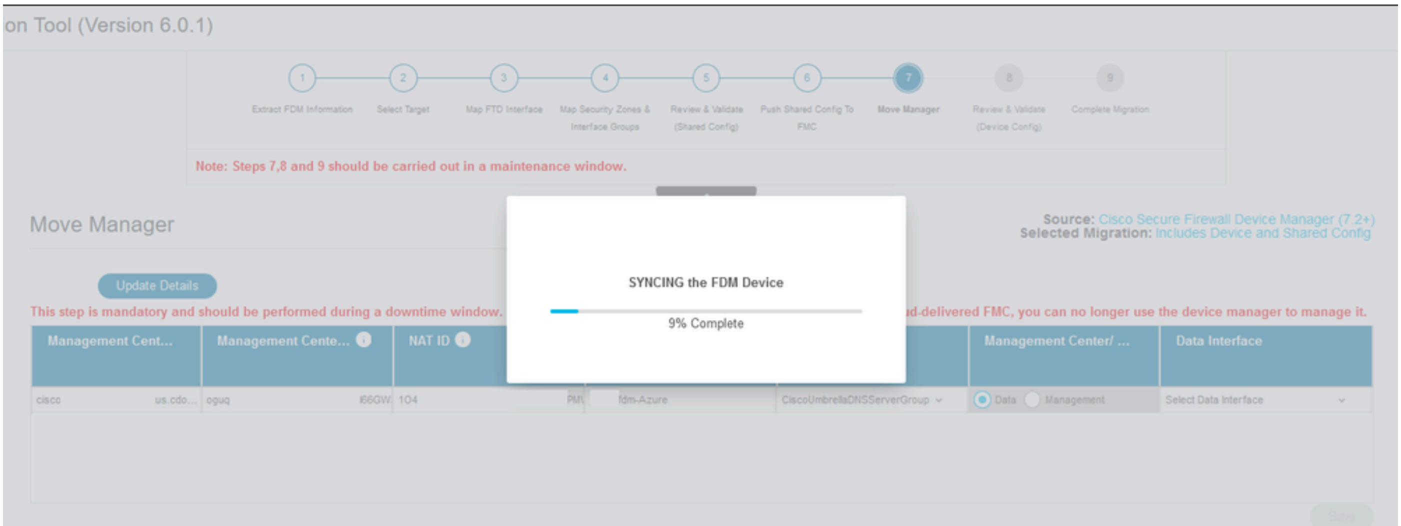
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

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...	ogu 66GW	104\ 3sPM\	fdm-Azure	CiscoUmbrellaDNSServerGroup ⌄	● Data ○ Management	Select Data Interface ⌄

管理中心ID & NAT ID。

选择Update Details选项后，设备将开始同步。


on Tool (Version 6.0.1)
1 Extract FDM Information
2 Select Target
3 Map FTD Interface
4 Map Security Zones & Interface Groups
5 Review & Validate (Shared Config)
6 Push Shared Config To FMC
7 Move Manager
8 Review & Validate (Device Config)
9 Complete Migration
Update Details
Move Manager

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

This step is mandatory and should be performed during a downtime window. ...d-delivered FMC, you can no longer use the device manager to manage it.

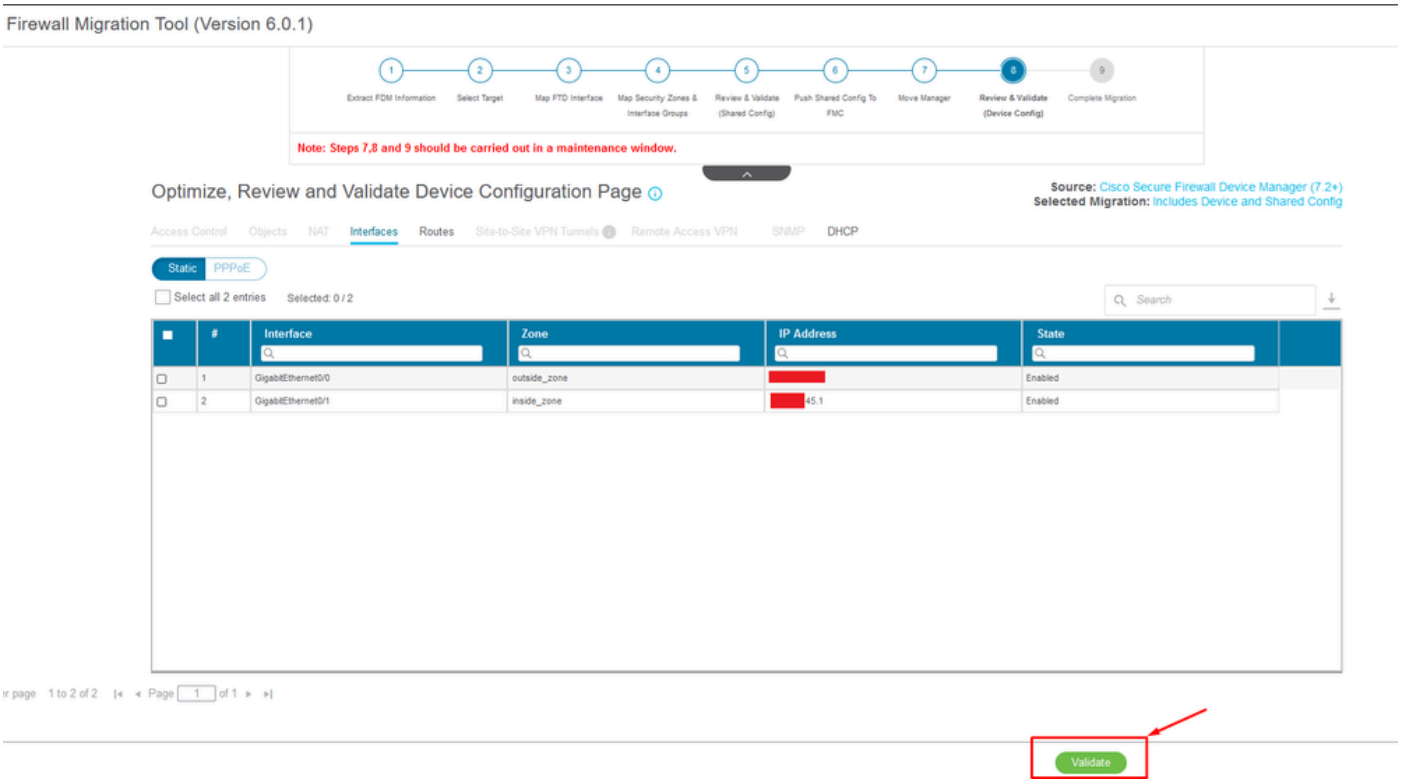
SYNCING the FDM Device

9% Complete

Management Cent...	Management Cente...	NAT ID			Management Center/ ...	Data Interface
cisco us.cdo...	oguq 66GW	104 PM\	fdm-Azure	CiscoUmbrellaDNSServerGroup ⌄	● Data ○ Management	Select Data Interface ⌄

同步FDM设备

完成迁移后，下一步是通过选择验证来检查FDM中配置的接口、路由和DHCP设置。



Firewall Migration Tool (Version 6.0.1)

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

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

Optimize, Review and Validate Device Configuration Page

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

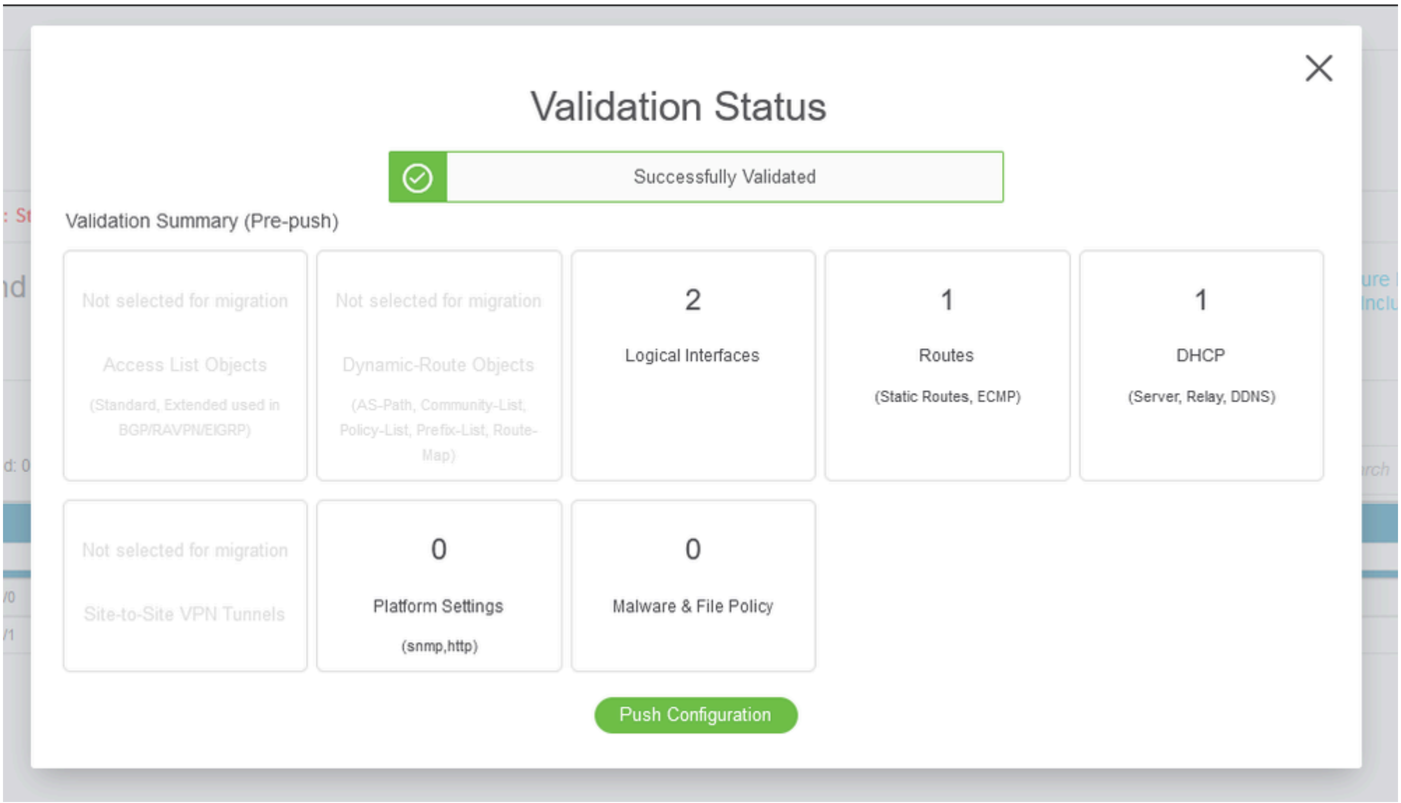
□ Select all 2 entries Selected: 0 / 2

■	#	Interface	Zone	IP Address	State
□	1	GigabitEthernet0/0	outside_zone	[redacted]	Enabled
□	2	GigabitEthernet0/1	inside_zone	[redacted]45.1	Enabled

r page 1 to 2 of 2 |◂ ◂ Page 1 of 1 ▸ ▸|

验证FDM配置设置

验证之后，选择Push Configuration以启动配置推送进程，该进程将持续到迁移结束为止。此外，还可以监控正在执行的任务。



Validation Status

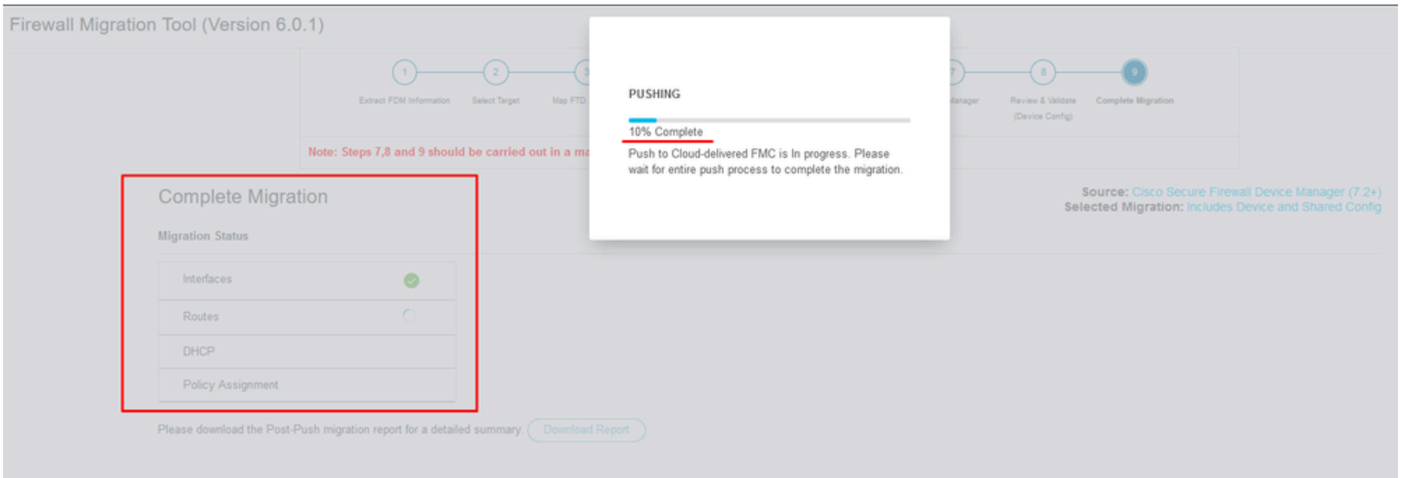
Successfully Validated

Validation Summary (Pre-push)

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

验证状态-推送配置。

包含百分比推送配置的弹出窗口。



Firewall Migration Tool (Version 6.0.1)

Note: Steps 7,8 and 9 should be carried out in a ma

PUSHING

10% Complete

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

Complete Migration

Migration Status

Interfaces

Routes

DHCP

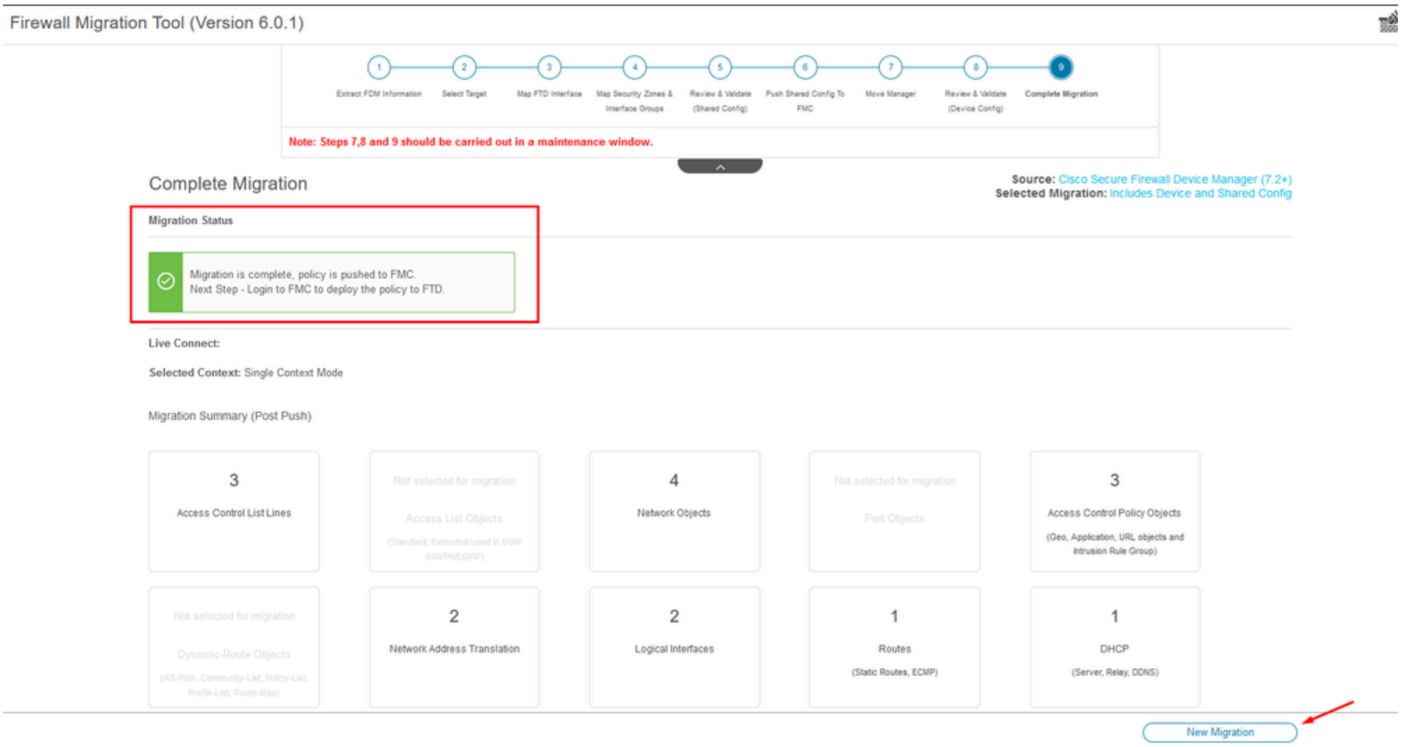
Policy Assignment

Please download the Post-Push migration report for a detailed summary.

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

推送完成百分比

完成后，将显示启动新迁移的选项，标记从FDM到cdFMC的迁移过程的结束。



Firewall Migration Tool (Version 6.0.1)

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

Complete Migration

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

Migration Status

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

Live Connect:

Selected Context: Single Context Mode

Migration Summary (Post Push)

3 Access Control List Lines

Not selected for migration — Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)

4 Network Objects

Not selected for migration — Port Objects

3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)

Not selected for migration — 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)

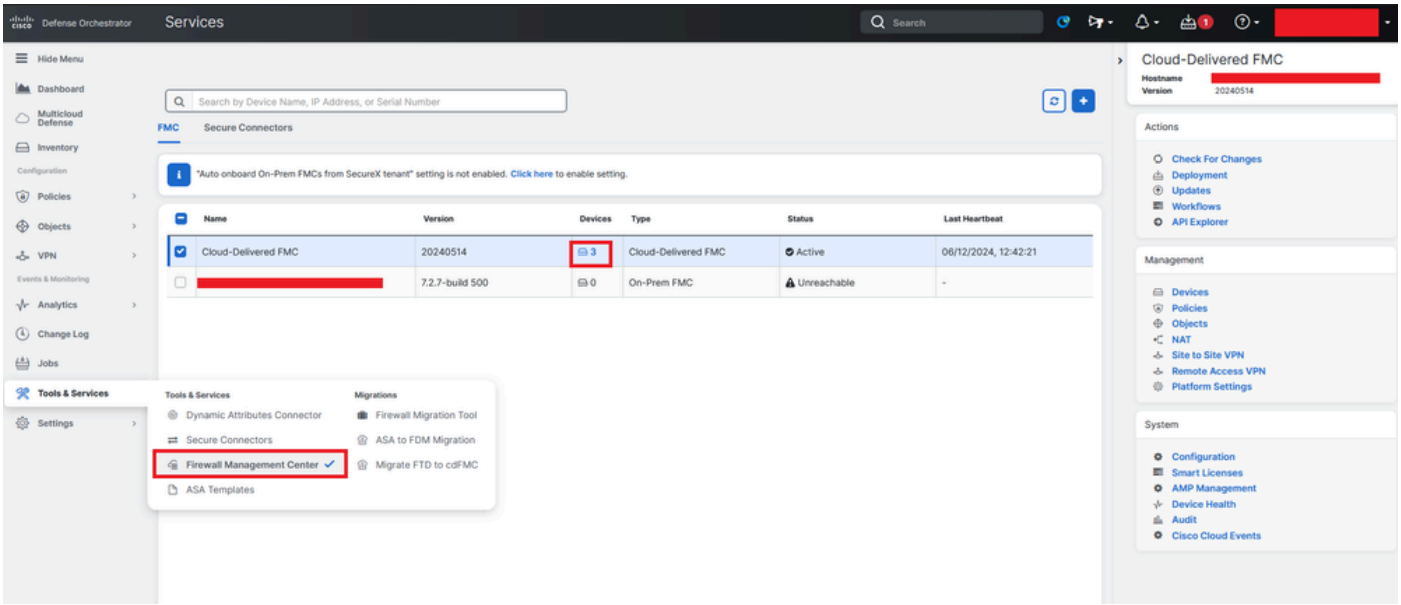
1
Extract FDM Information
2
Select Target
3
Map FTD Interface
4
Map Security Zones & Interface Groups
5
Review & Validate (Shared Config)
6
Push Shared Config To FMC
7
Move Manager
8
Review & Validate (Device Config)
9
Complete Migration
New Migration

完成迁移

验证

验证FDM是否已成功迁移到cdFMC。

导航到CDO > Tools & Services > Firepower Management Center。您会发现注册设备的数量已增加。



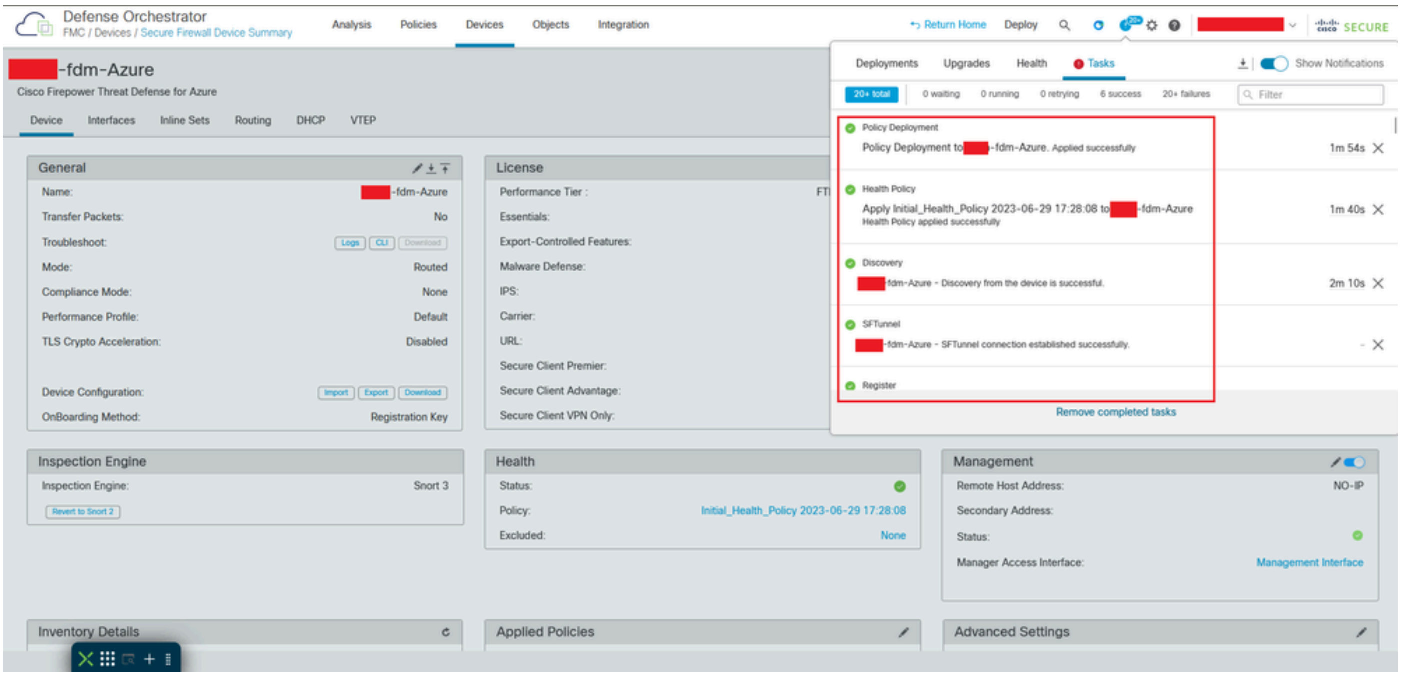
"Auto onboard On-Prem FMCs from SecureX tenant" setting is not enabled. Click here to enable setting.

Name	Version	Devices	Type	Status	Last Heartbeat
☑ Cloud-Delivered FMC	20240514	3	Cloud-Delivered FMC	Active	06/12/2024, 12:42:21
□ [redacted]	7.2.7-build 500	0	On-Prem FMC	Unreachable	-

Cloud-Delivered FMC
Hostname [redacted]
Version 20240514

cdFMC注册设备

在Devices > Device Management中检查设备。此外，在FMC的任务中，您可以找到设备成功注册和首次部署成功完成的时间。



[redacted]-fdm-Azure
Cisco Firepower Threat Defense for Azure

General
Name: [redacted]-fdm-Azure
Transfer Packets: No
Troubleshoot: Logs CLI Download
Mode: Routed
Compliance Mode: None
Performance Profile: Default
TLS Crypto Acceleration: Disabled
Device Configuration: Import Export Download
OnBoarding Method: Registration Key

Tasks: 20+ total 0 waiting 0 running 0 retrying 6 success 20+ failures

Policy Deployment
Policy Deployment to [redacted]-fdm-Azure. Applied successfully 1m 54s

Health Policy
Apply Initial_Health_Policy 2023-06-29 17:28:08 to [redacted]-fdm-Azure
Health Policy applied successfully 1m 40s

Discovery
[redacted]-fdm-Azure - Discovery from the device is successful. 2m 10s

SFTunnel
[redacted]-fdm-Azure - SFTunnel connection established successfully. -

Register

Remove completed tasks

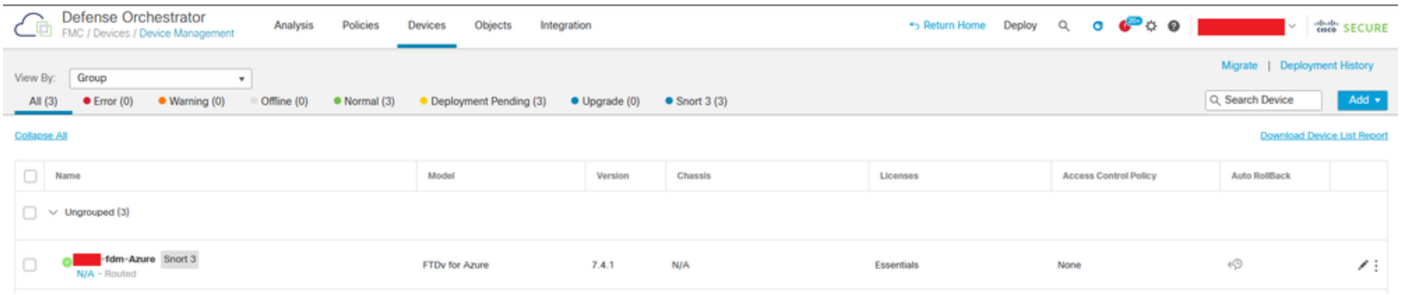
Inspection Engine
Inspection Engine: Snort 3
Revert to Snort 2

Health
Status: ●
Policy: Initial_Health_Policy 2023-06-29 17:28:08
Excluded: None

Management
Remote Host Address: NO-IP
Secondary Address:
Status: ●
Manager Access Interface: Management Interface

cdFMC注册任务已完成。

设备位于cdFMC > Device > Device Management中。



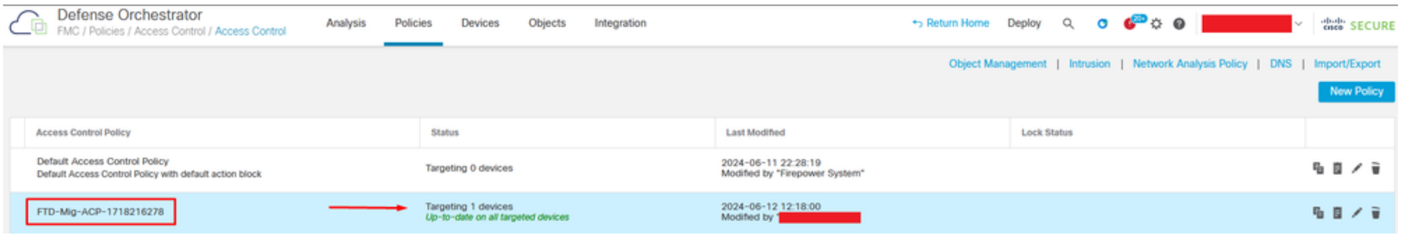
View By: Group

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

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

在cdFMC上注册的设备

在Policies > Access Control下迁移的访问控制策略。

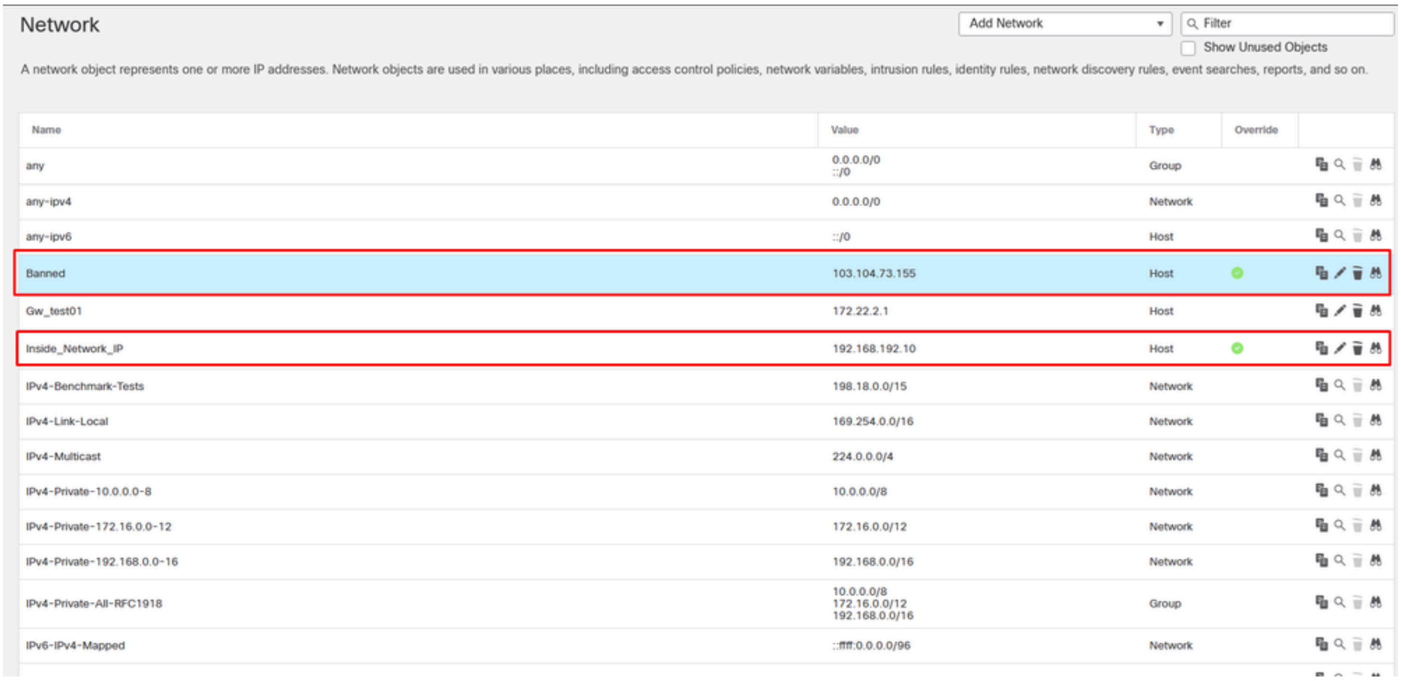


Defense Orchestrator
FMC / Policies / Access Control / Access Control
Analysis
Policies
Devices
Objects
Integration
Return Home
Deploy
[redacted]
SECURE
Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export
New Policy

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 [redacted]	

迁移策略

同样，您可以查看在FDM中创建的对象，这些对象已正确迁移到cdFMC。

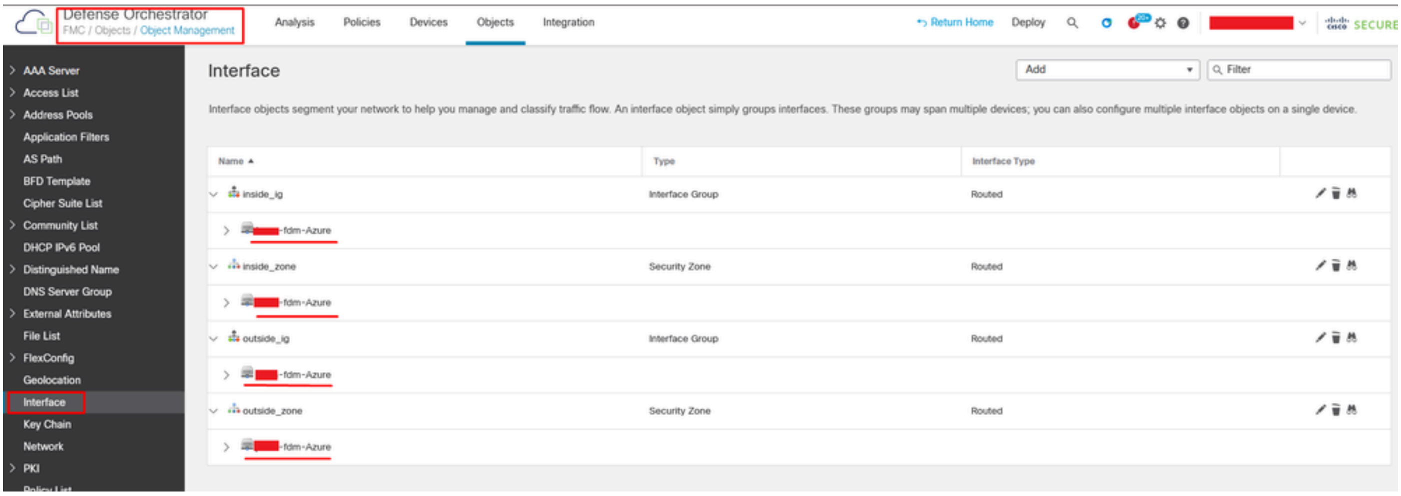


A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

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	

从FDM迁移到cdFMC的对象

已迁移对象管理接口。



Interface objects segment your network to help you manage and 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
[redacted]-fdm-Azure		
inside_zone	Security Zone	Routed
[redacted]-fdm-Azure		
outside_ig	Interface Group	Routed
[redacted]-fdm-Azure		
outside_zone	Security Zone	Routed
[redacted]-fdm-Azure		

已迁移对象管理接口。

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。