CDO内のFMTを使用したcdFMCへのFDMの移行

内容

はじめに

このドキュメントでは、CDOのFirepower移行ツール(FMT)を使用して、Firepower Device Manager(FDM)をクラウド配信FMC(cdFMC)に移行する方法について説明します。

前提条件

要件

- Firepowerデバイスマネージャ(FDM)7.2+
- クラウド提供のファイアウォール管理センター(cdFMC)
- CDOに含まれるFirepower Migration Tool(FMT)

使用するコンポーネント

このドキュメントは、前述の要件に基づいて作成されました。

- バージョン7.4.1上のFirePOWERデバイスマネージャ(FDM)
- クラウド提供のファイアウォール管理センター(cdFMC)
- クラウド防衛オーケストレータ(CDO)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

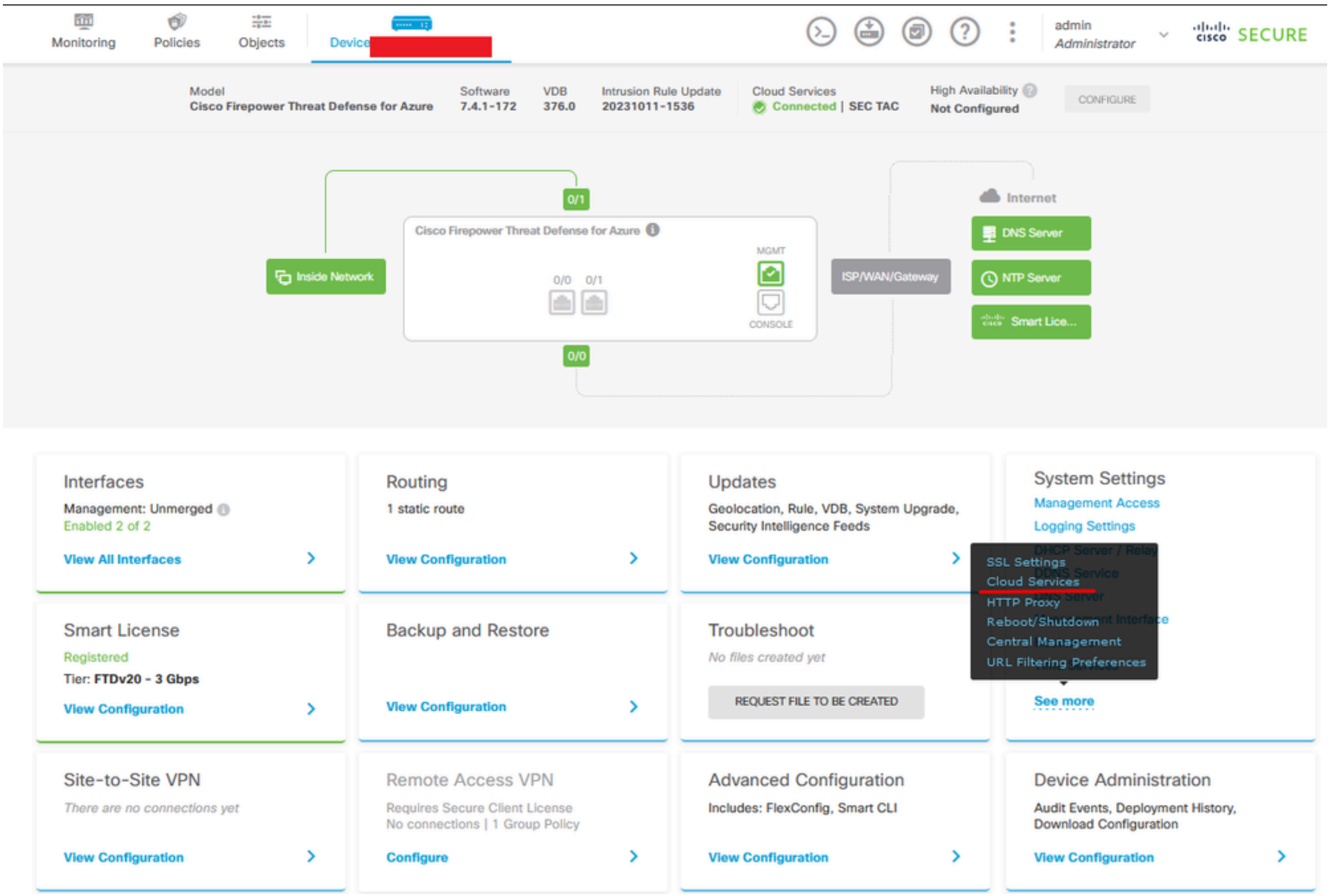
CDO管理者ユーザは、デバイスがバージョン7.2以降である場合に、そのデバイスをcdFMCに移行できます。このドキュメントで説明する移行では、cdFMCはすでにCDOテナントで有効になっています。

設定

1.- FDMでシスコクラウドサービスを有効にする

移行を開始するには、保留中の導入がないFDMデバイスを使用して、クラウドサービスに登録する必要があります。Cloud Servicesに登録するには、System Settings > See More > Cloud Servicesの順に移動します。

Cloud Servicesセクションで、デバイスが登録されていないことがわかりました。したがって、タイプSecurity/CDO Accountで登録を行う必要があります。登録キーを設定してから登録する必要があります。

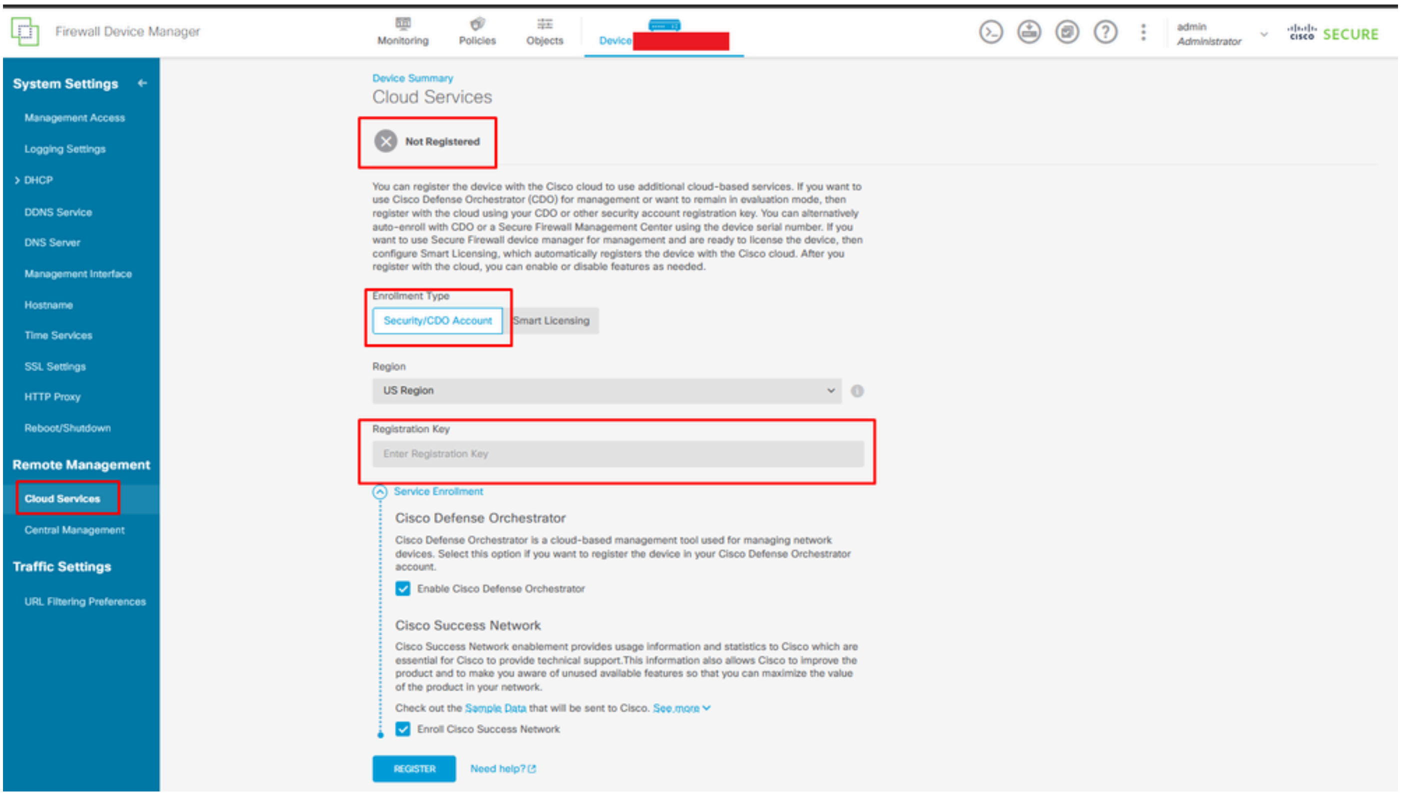


Device [redacted]

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

Registration Cloudサービス

クラウドサービスを介して、が登録されていないことが示されます。CDOアカウント登録タイプを選択し、CDOから登録キーを入力します。



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.

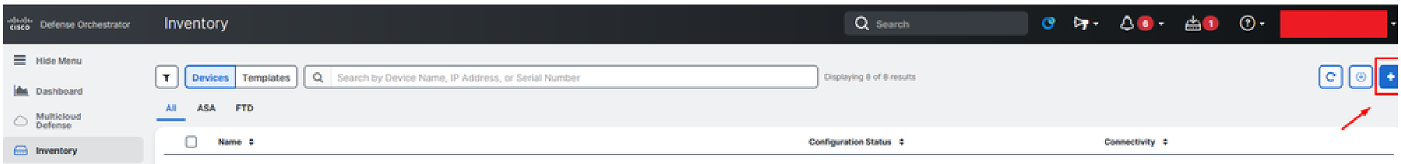
Check out the Sample Data that will be sent to Cisco. See more

☑ Enroll Cisco Success Network

クラウドサービスへの登録

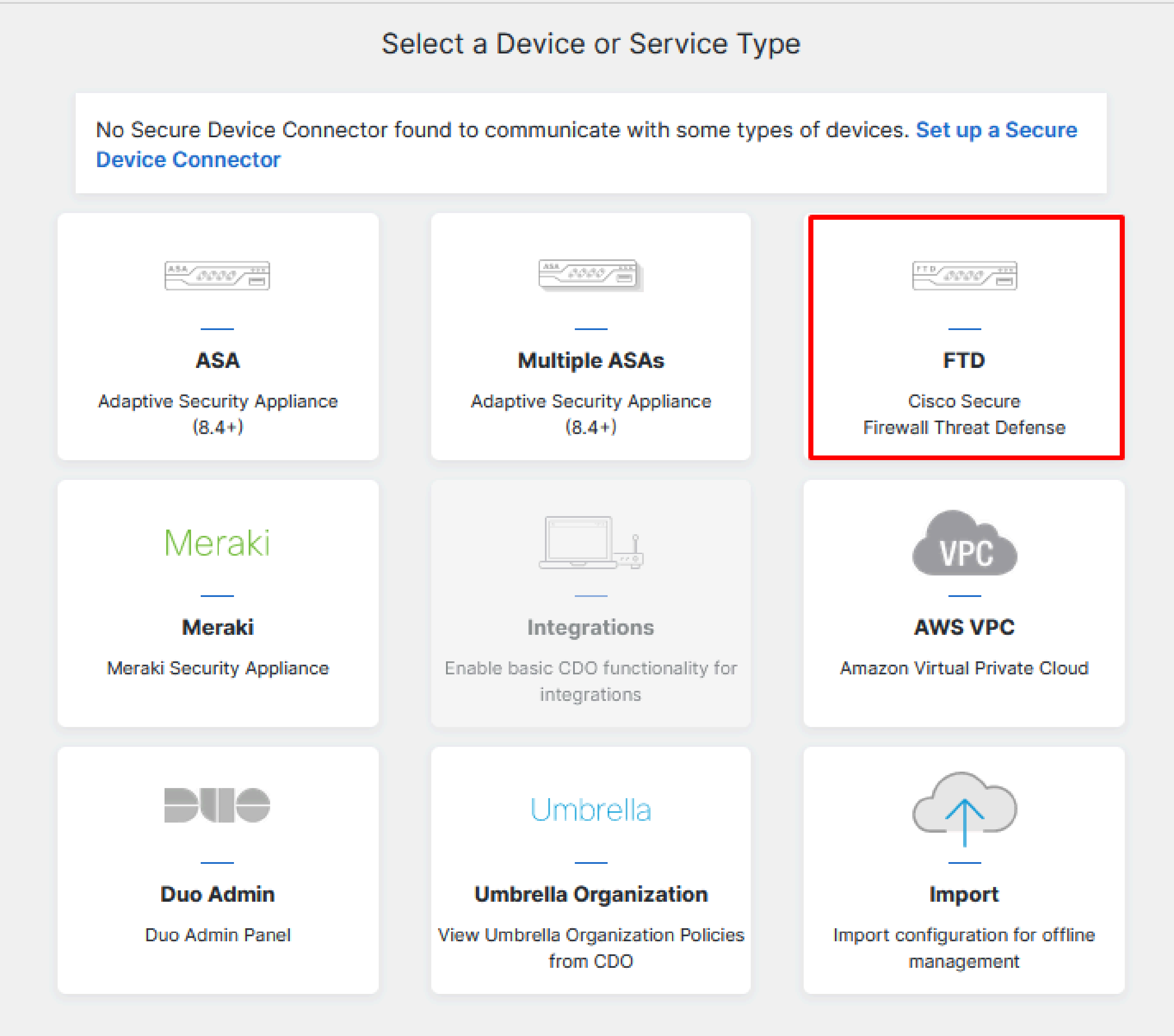
登録キーはCDO内にあります。CDOに移動し、Inventory > Add symbolに移動します。

メニューが表示され、使用しているデバイスのタイプを選択できます。FTDオプションを選択します。FDMオプションを使用可能にする必要があります。使用可能にしない場合、対応する移行は実行できません。登録のタイプは、登録キーの使用を使用します。このオプションでは、登録キーがステップ3に表示されます。このキーをコピーしてFDMに貼り付ける必要があります。



オンボードFDM、オプションの追加

[Select a Device or Service Type]（デバイスまたはサービスタイプの選択）メニューが表示されます。



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

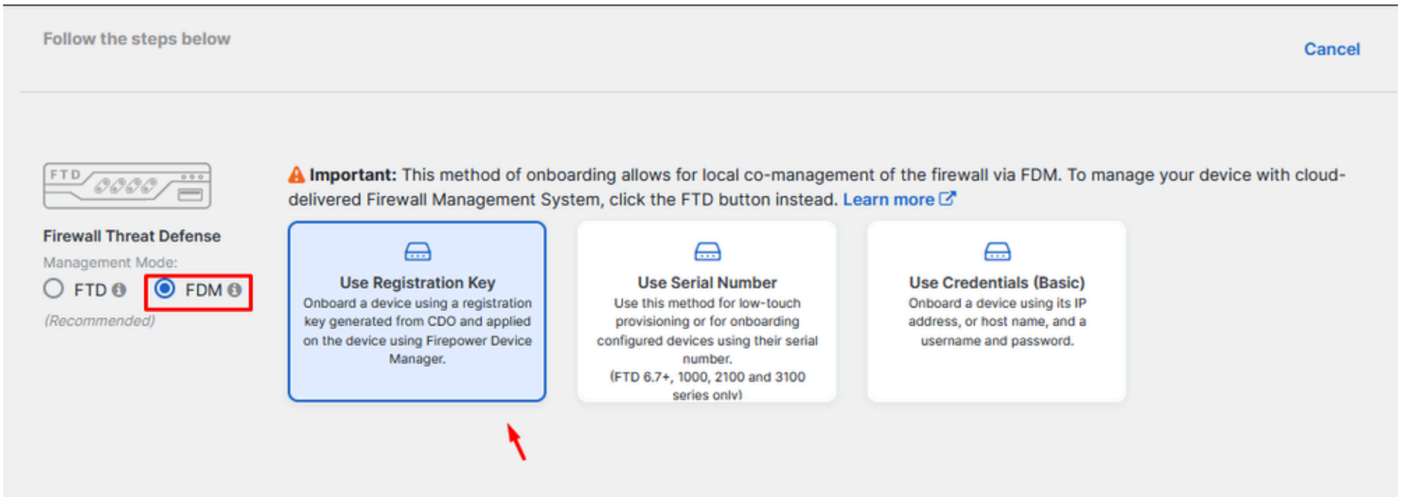
Duo Admin
Duo Admin Panel

Umbrella Organization
View Umbrella Organization Policies from CDO

Import
Import configuration for offline management

デバイスまたはサービスタイプの選択

このドキュメントでは、「Select Registration Key」が選択されています。



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

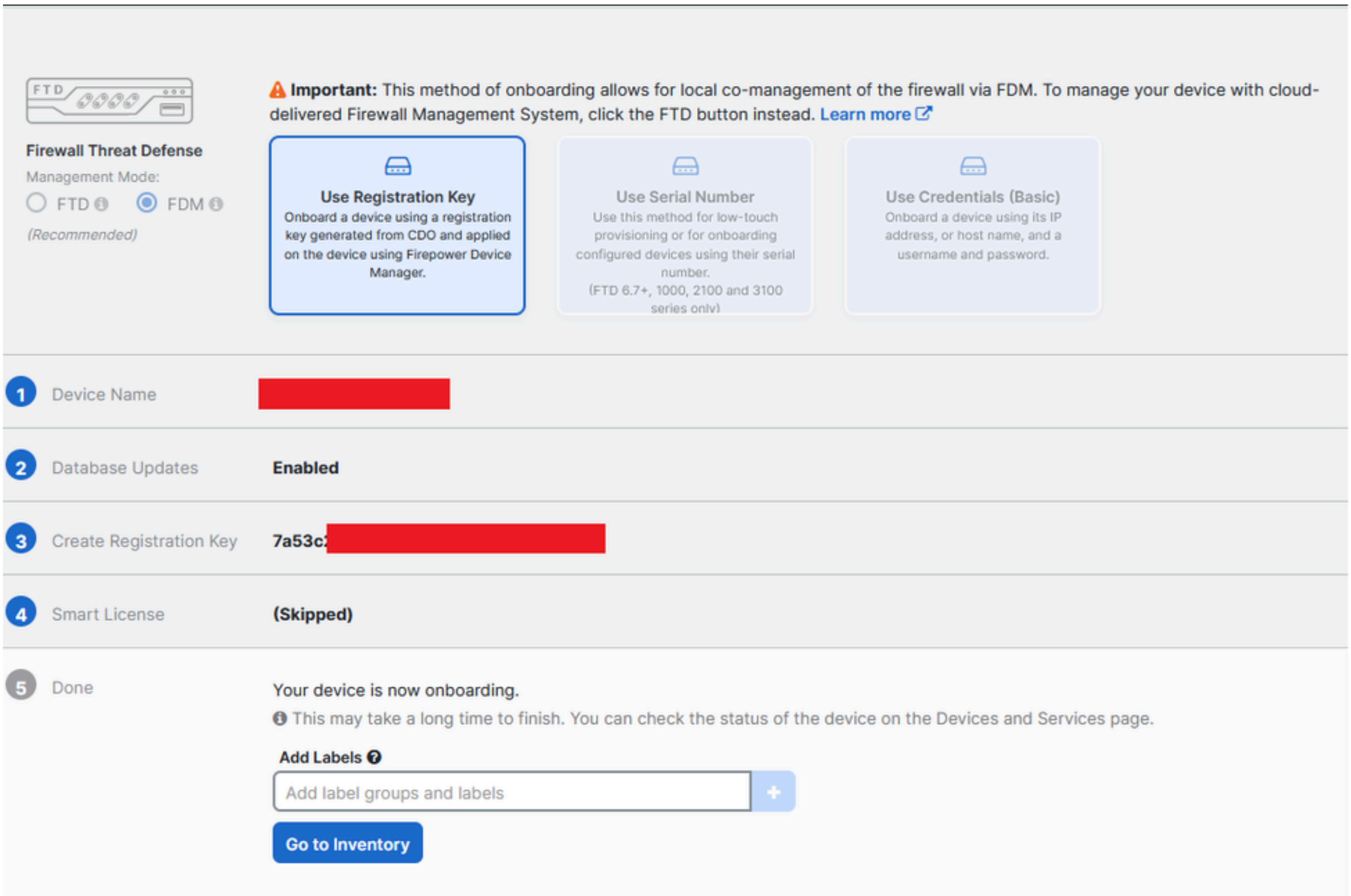
Use Registration Key
Onboard a device using a registration key generated from CDO and applied on the device using Firepower Device Manager.

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.

登録タイプ

ここでは、前の手順で必要な登録キーが示されています。



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

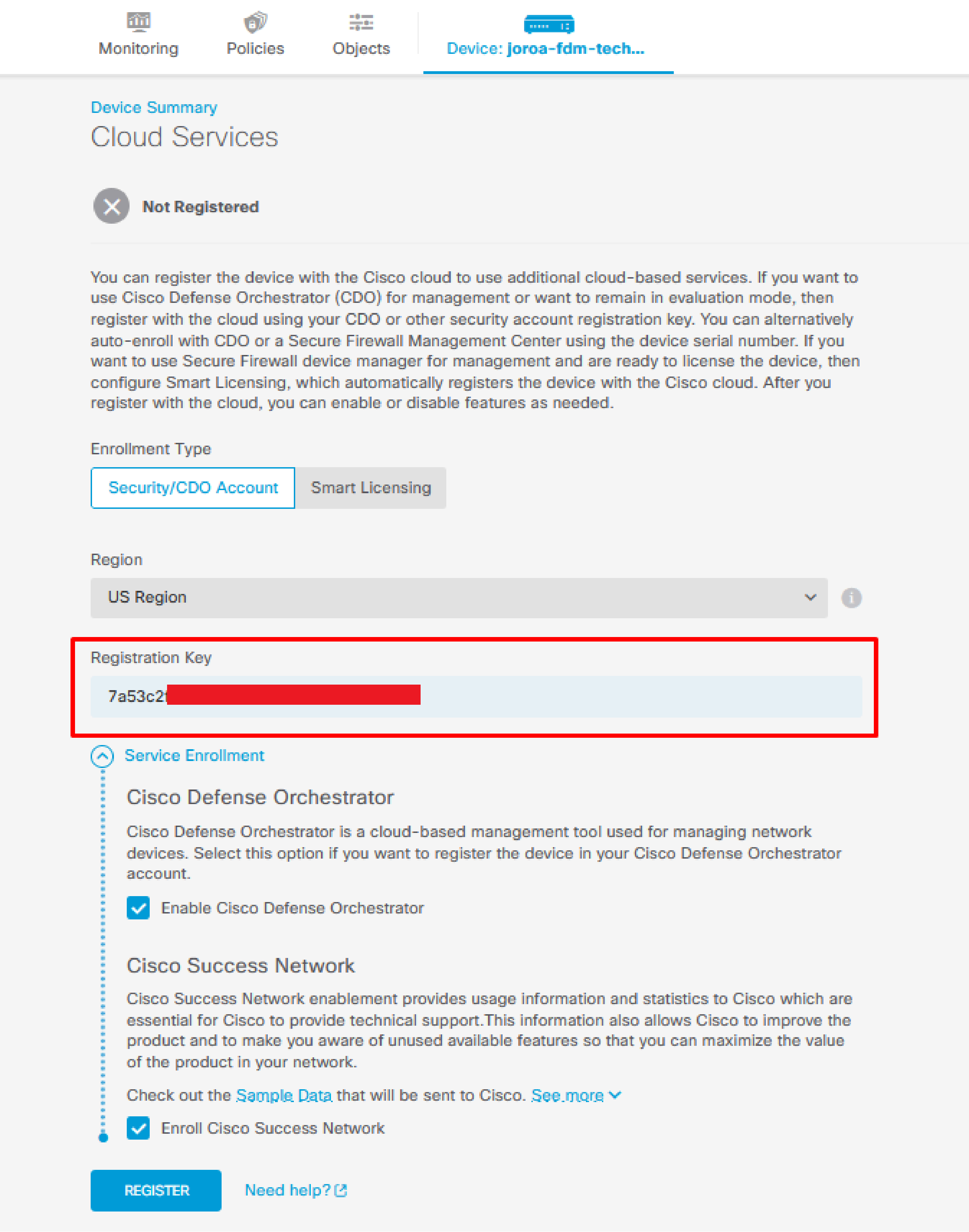
Add label groups and labels

Go to Inventory

登録プロセス

登録キーを取得したら、それをコピーしてFDMに貼り付け、登録をクリックします。クラウドサービス内にFDMを登録すると、図に示すようにEnabledと表示されます。

デバイスが起動して実行されるとデバイスが登録されるため、スマートライセンスはスキップされました。



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.

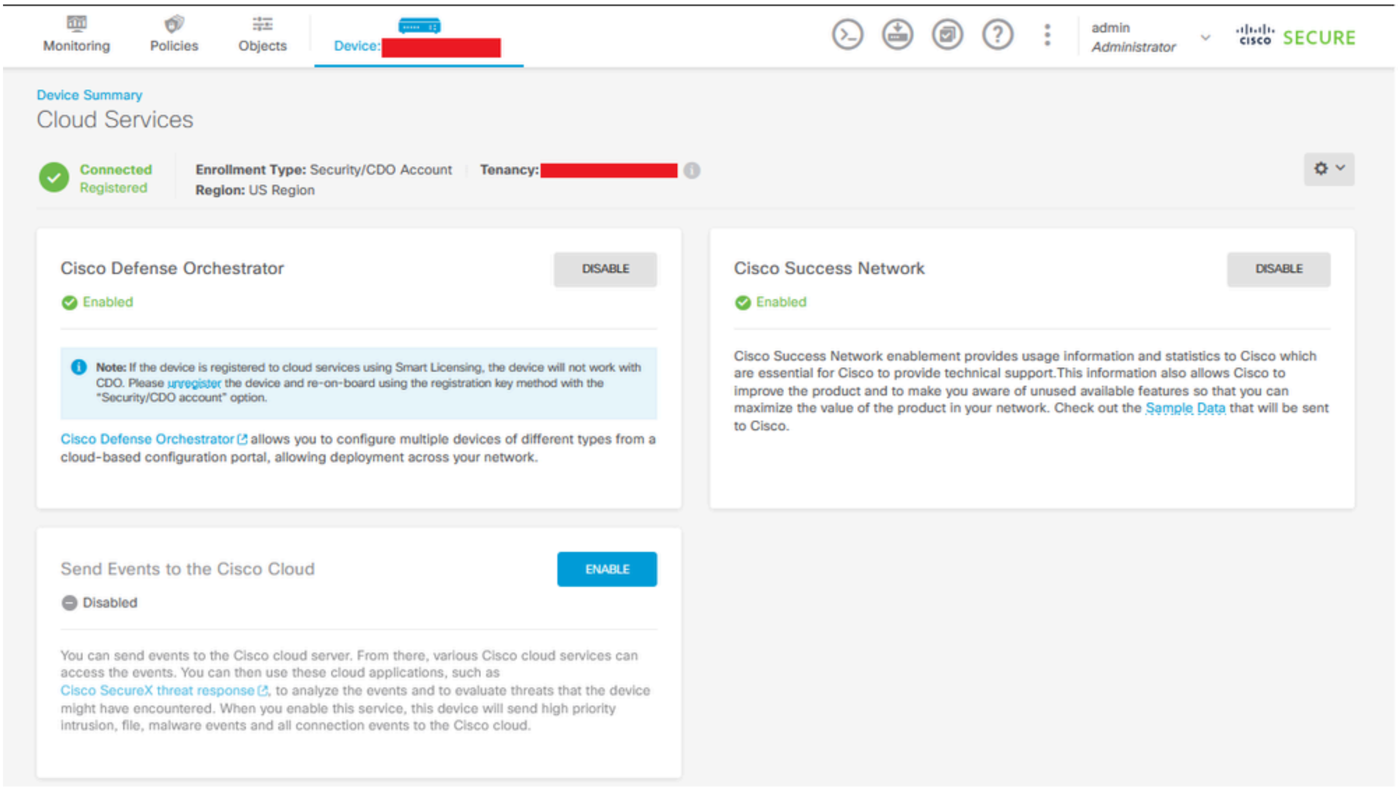
Check out the Sample Data that will be sent to Cisco. See more

☑ Enroll Cisco Success Network

REGISTER   Need help?

FDM登録

FDMを登録すると、テナント、接続されているクラウドサービス、および登録済みのクラウドサービスが表示されます。



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.

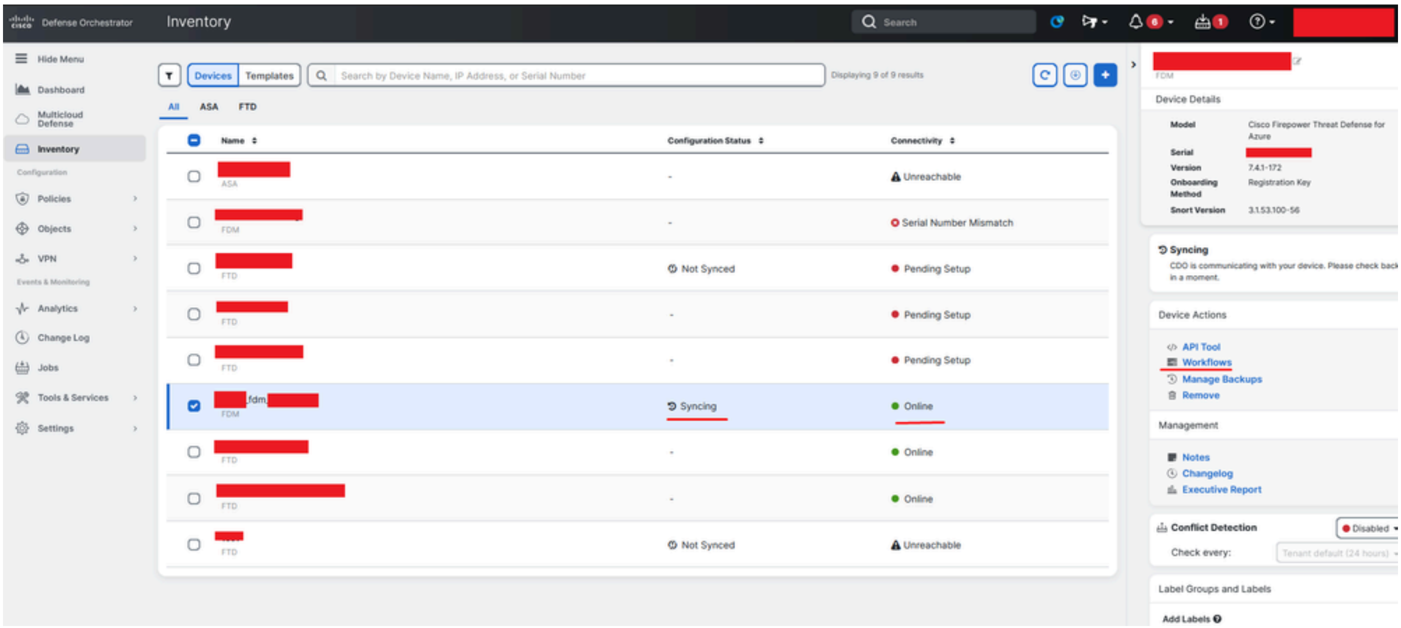
Send Events to the Cisco Cloud ENABLE
Disabled

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登録の完了

CDO内のインベントリメニューでは、FDMはオンボーディングおよび同期のプロセスにあります。この同期の進捗状況とフローは、「ワークフロー」セクションで確認できます。

このプロセスが完了すると、「Synced and Online」と表示されます。



Displaying 9 of 9 results

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

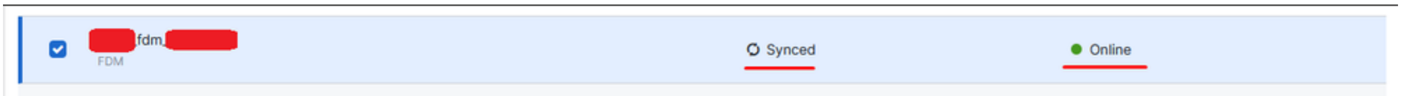
Management
Notes
Changelog
Executive Report

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

Label Groups and Labels
Add Labels

CDOインベントリFDMオンボーディング

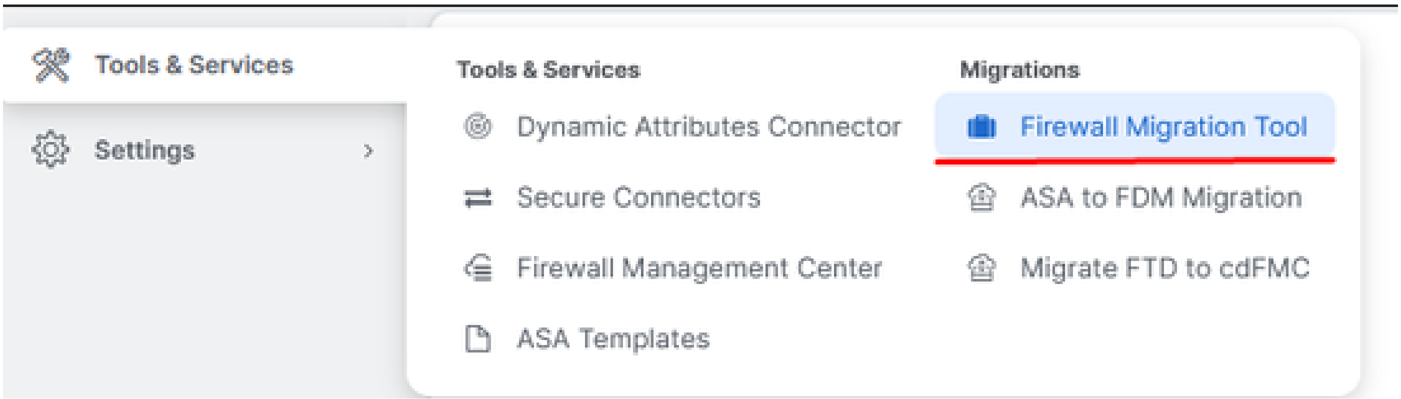
デバイスが同期されると、「Online」および「Synced」と表示されます。



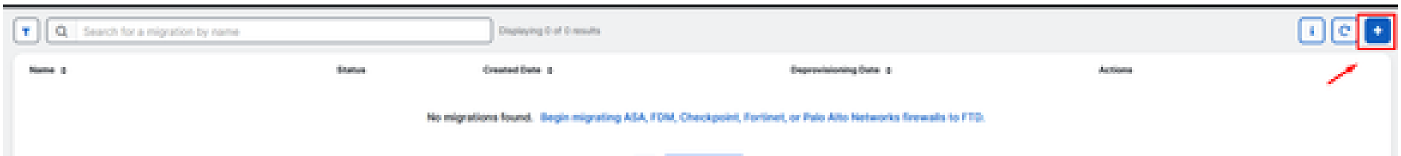
☑ [redacted]fdm[redacted]
FDM
Synced
Online

FDMオンボーディング

FDMがCDOに正常にオンボーディングされたら、FDMからログアウトする必要があります。FDMからログアウトした後、CDO内でTools & Services > Migration > Firewall Migration Toolの順に移動します。



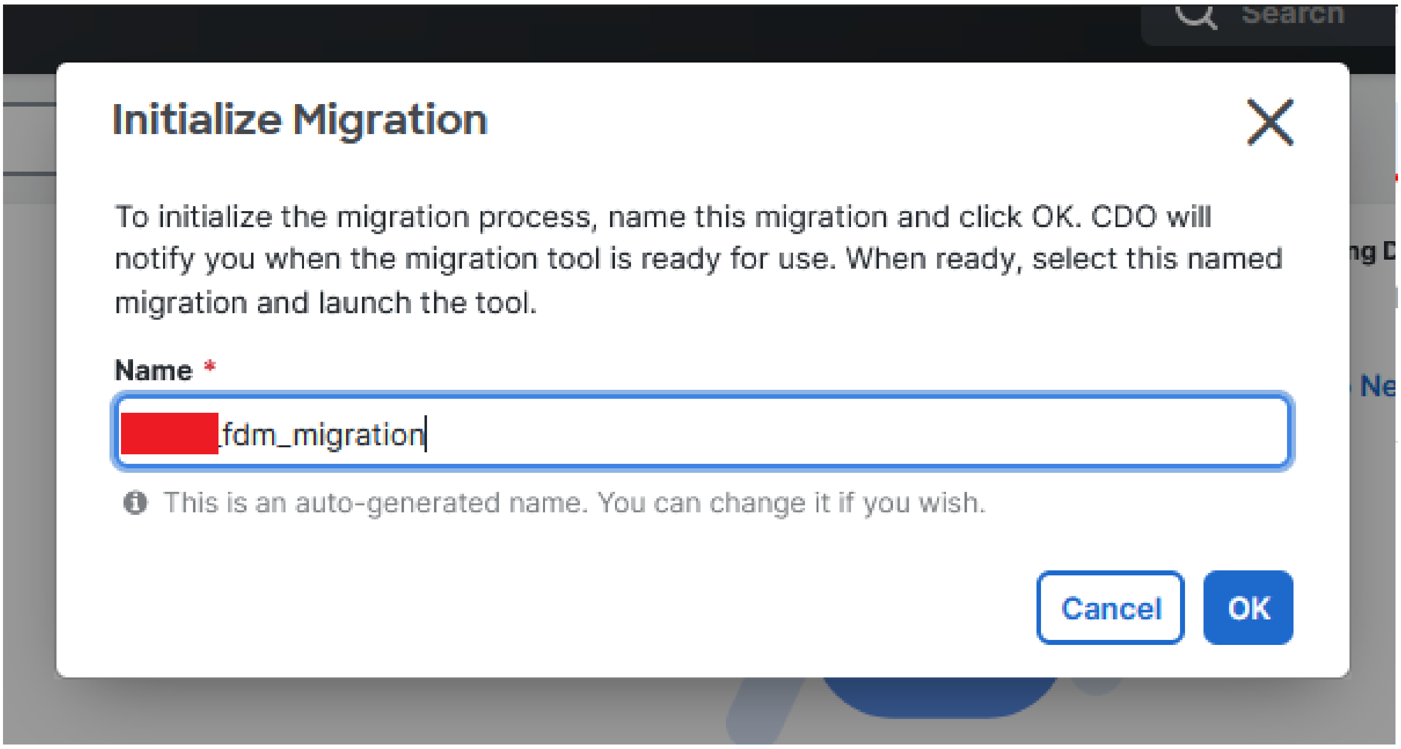
Addシンボルをクリックすると、名前がランダムに表示されます。これは、移行プロセスを開始するには名前を変更する必要があることを示します。



Name	Status	Created Date	Deprovisioning Date	Actions

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

名前を変更したら、Launchをクリックして移行を開始します。



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.

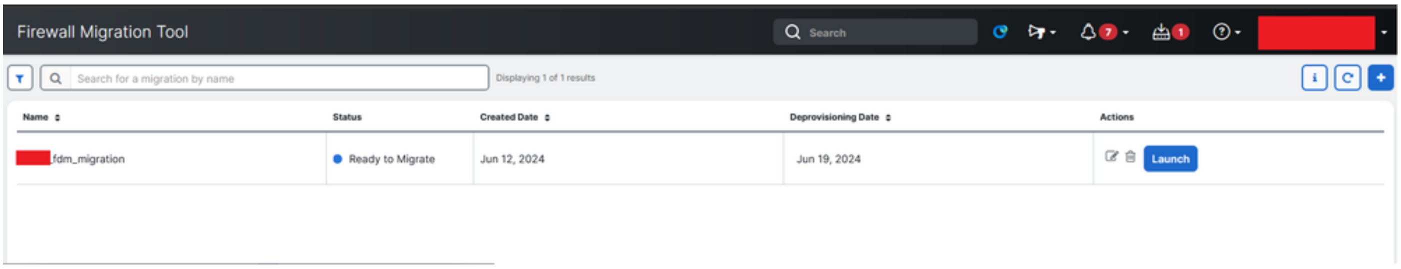
Name *

[redacted]fdm_migration

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

移行の初期化

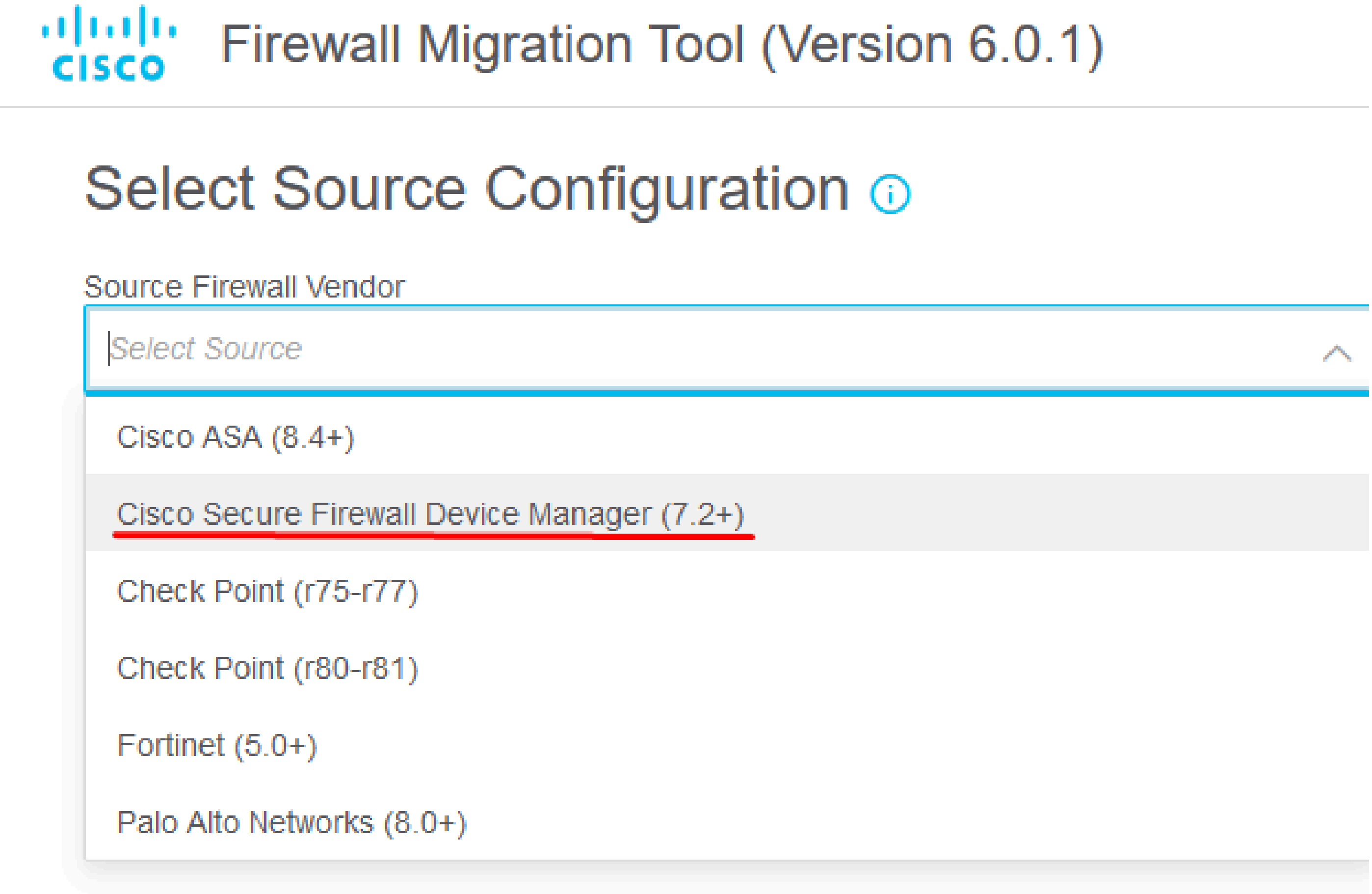
Launchをクリックして、移行の設定を開始します。



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

移行の開始プロセス

Launchをクリックすると、移行プロセスのためのウィンドウが開き、オプションのCisco Secure Firewall Device Manager(7.2+)が選択されます。前述したように、このオプションはバージョン7.2から有効になっています。

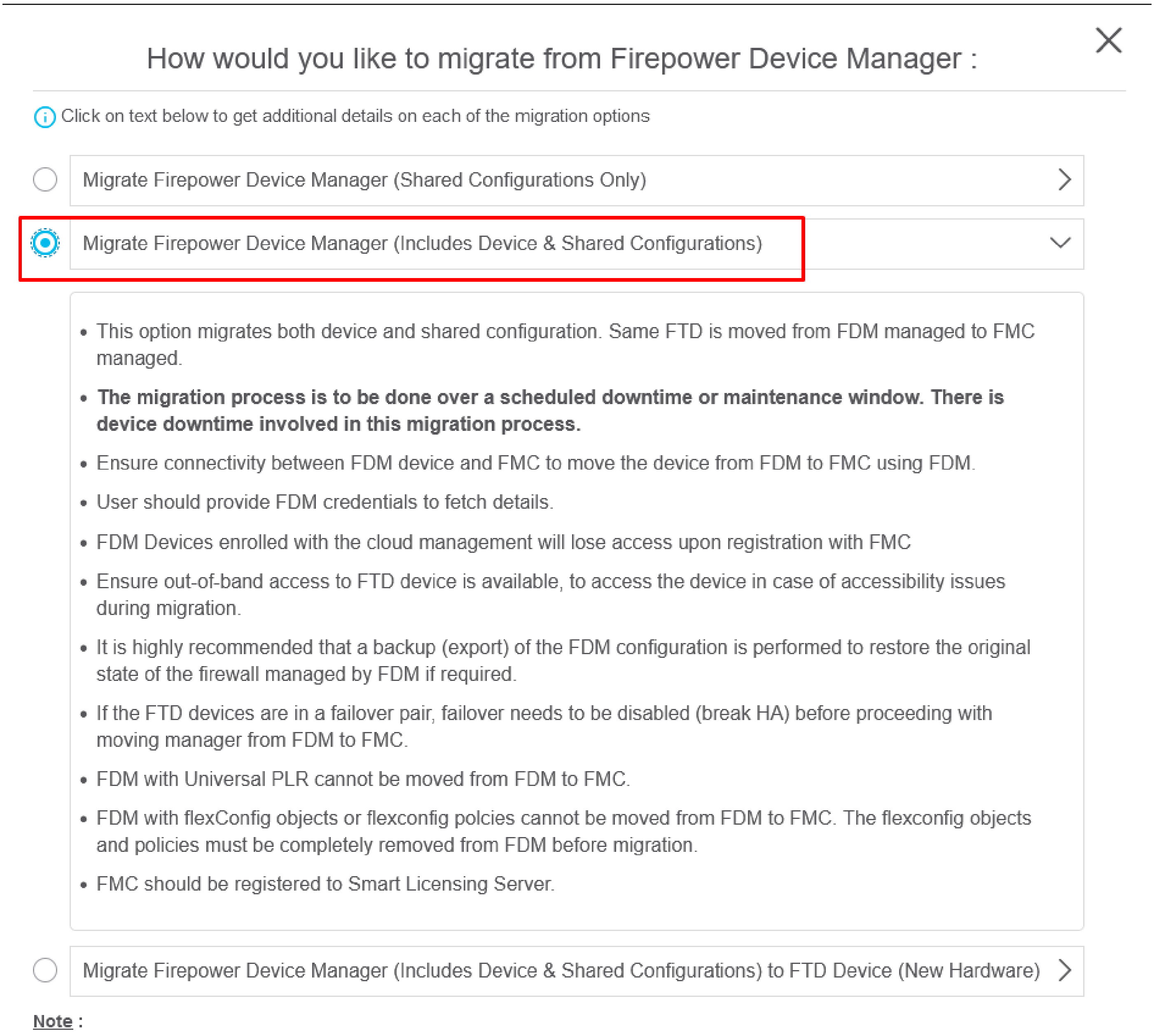


Firewall Migration Tool (Version 6.0.1)
Select Source Configuration
Source Firewall Vendor
Select Source
Cisco ASA (8.4+)
Cisco Secure Firewall Device Manager (7.2+)
Check Point (r75-r77)
Check Point (r80-r81)
Fortinet (5.0+)
Palo Alto Networks (8.0+)

FMTソース設定の選択

選択すると、3つの異なる移行オプションが表示されます。共有設定のみ、デバイスと共有設定を含む、デバイスと共有設定を含む、FTDの新しいハードウェアへの移行オプションです。

この例では、2番目のオプションであるMigrate Firepower Device Manager(Includes Device & Shared Configuration)が実行されます。



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)

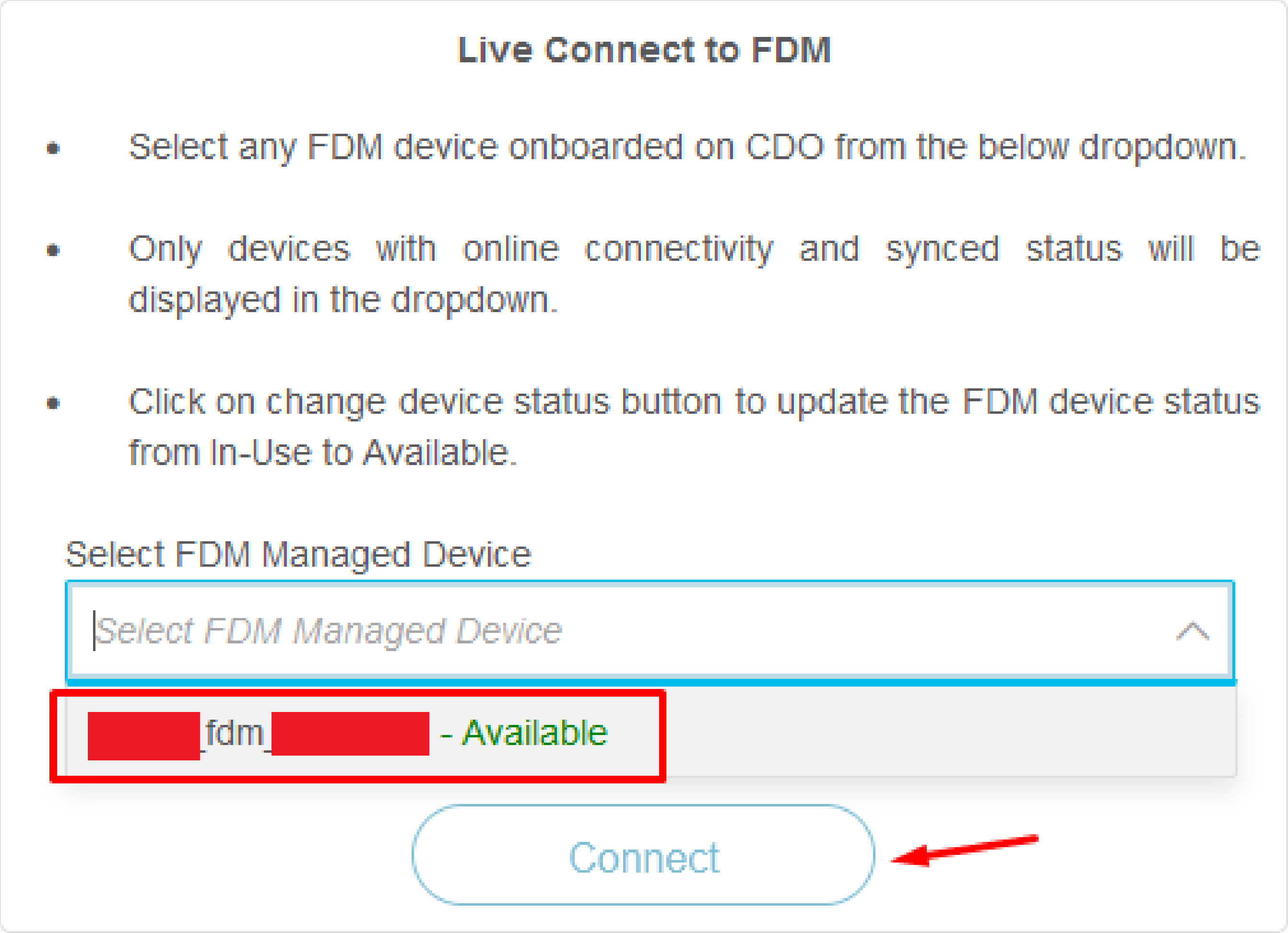
- This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
- **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
- Ensure connectivity between FDM device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

移行オプション

移行方法を選択したら、表示されたリストからデバイスを選択します。



Live Connect to FDM

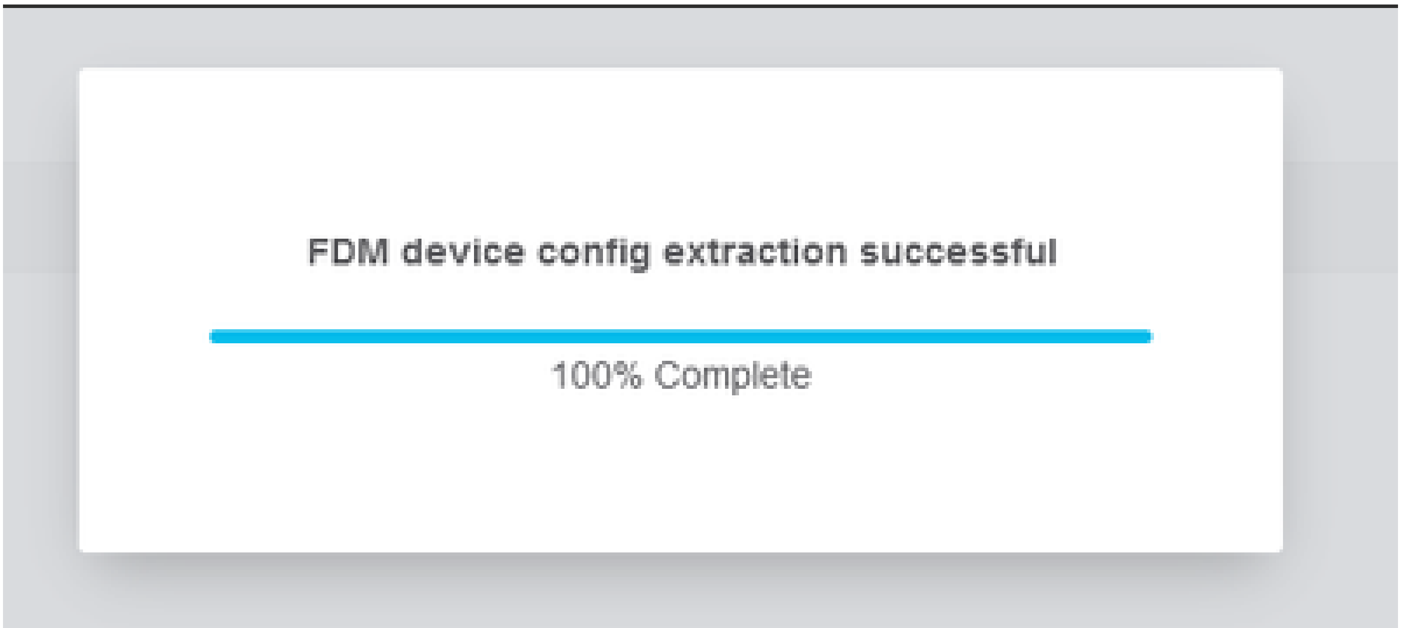
- Select any FDM device onboarded on CDO from the below dropdown.
- Only devices with online connectivity and synced status will be displayed in the dropdown.
- Click on change device status button to update the FDM device status from In-Use to Available.

Select FDM Managed Device

Select FDM Managed Device

[redacted]_fdm_[redacted] - Available

FDMデバイスの選択

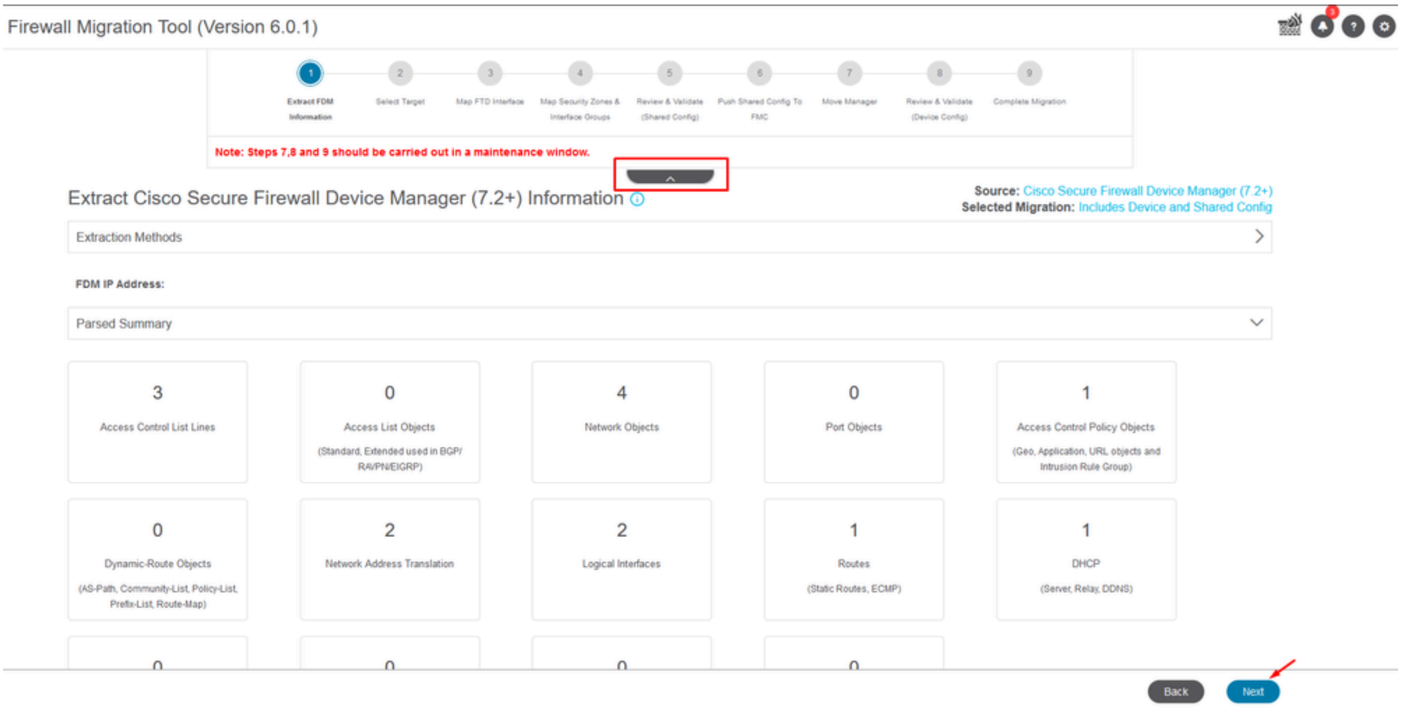


FDM device config extraction successful

100% Complete

構成の抽出が完了しました

デバイスを選択したときの手順を確認し、理解するために、上部にあるタブを開くことをお勧めします。



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

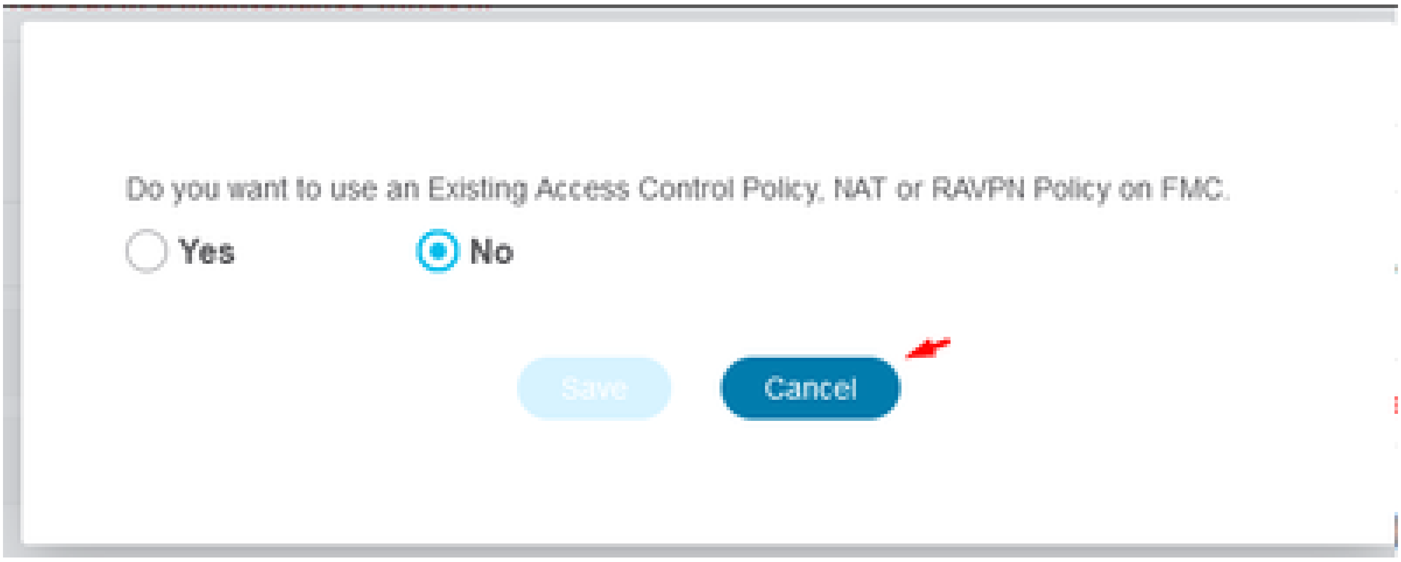
1 Routes (Static Routes, ECMP)

1 DHCP (Server, Relay, DDNS)

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
0
0
0
0
Back
Next

移行プロセスの手順

新しい移行であるため、「Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC?（FMCで既存のアクセスコントロールポリシー、NATまたはRAVPNポリシーを使用しますか？）」オプションの指示に従って、Cancelを選択します。

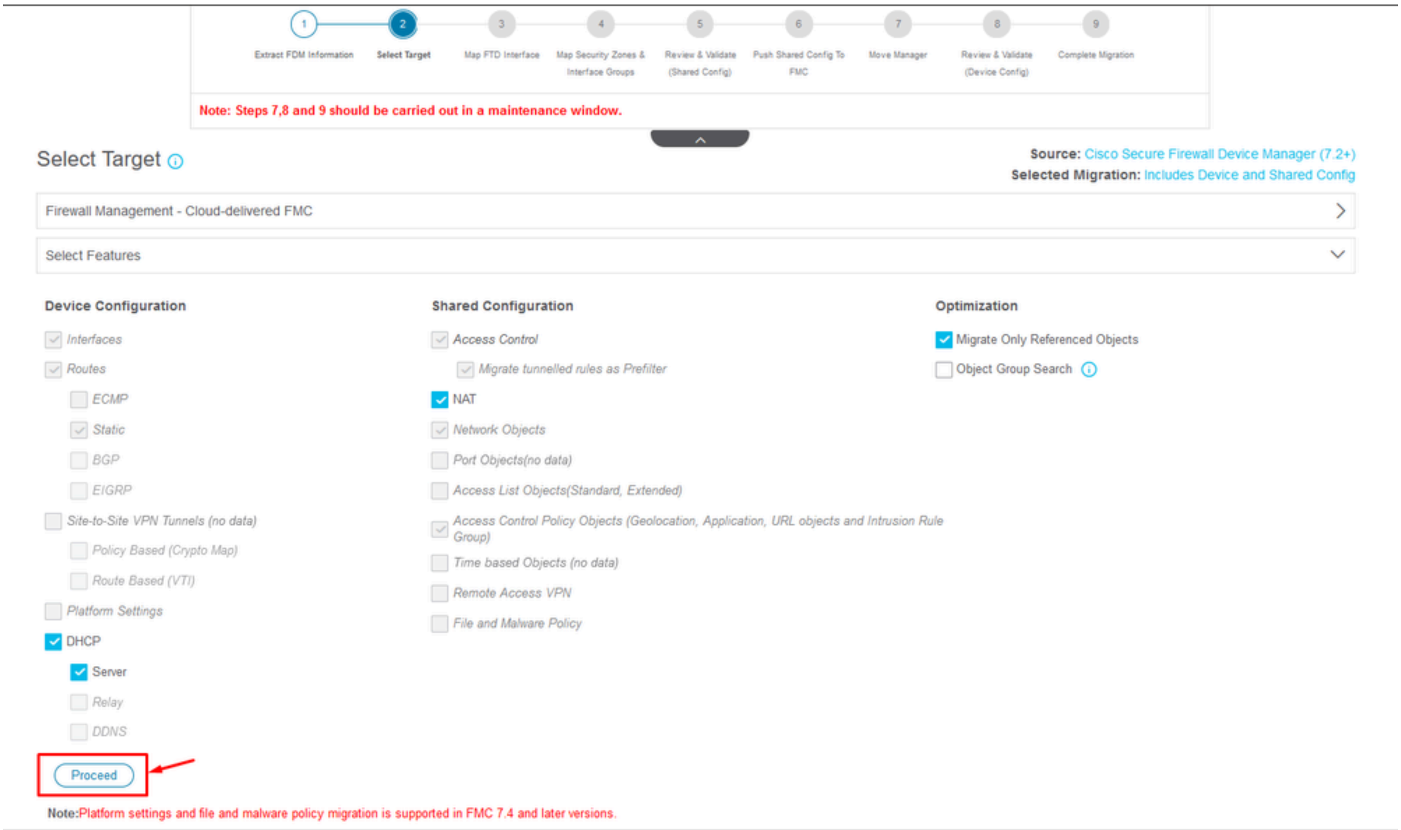


Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.

○ Yes ● No

既存の構成のキャンセルオプション

その後、図に示すように、移行する機能を選択するオプションが表示されます。[続行（Proceed）] をクリックします。



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

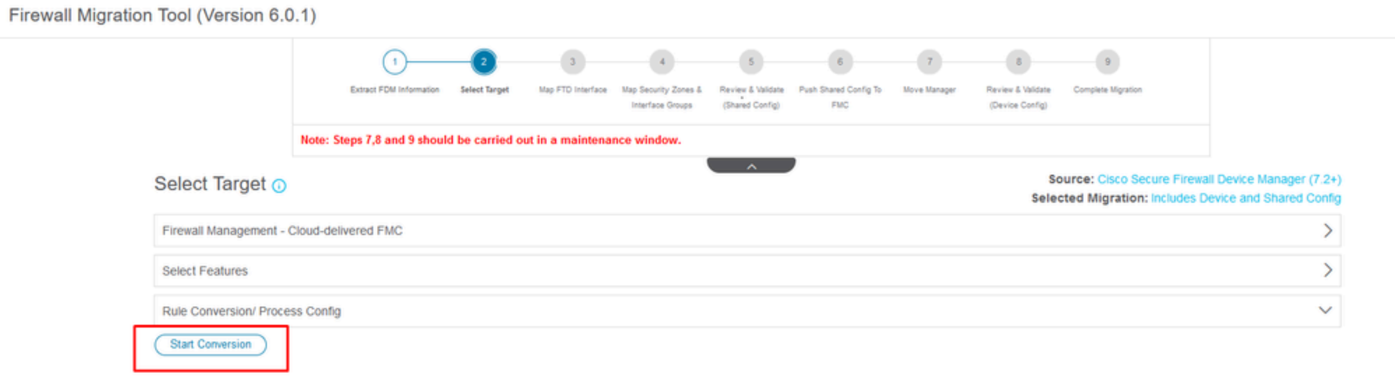
Optimization

- ☑ 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.

選択するフィーチャ

次に、変換を開始します。



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

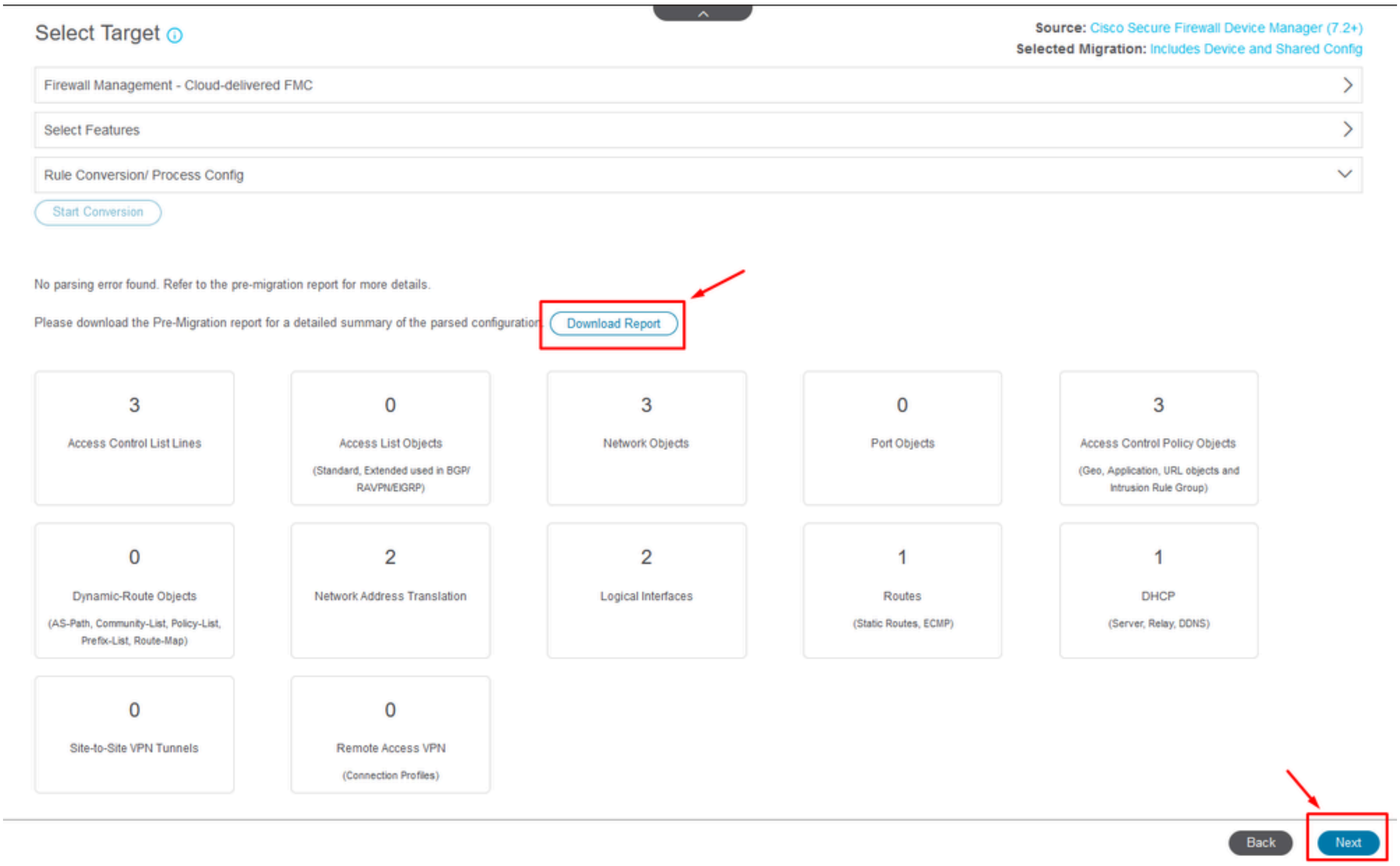
Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

変換を開始します。

解析プロセスが終了したら、次の2つのオプションが使用できます。ドキュメントをダウンロードし、Nextをクリックして移行を続行します。



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)

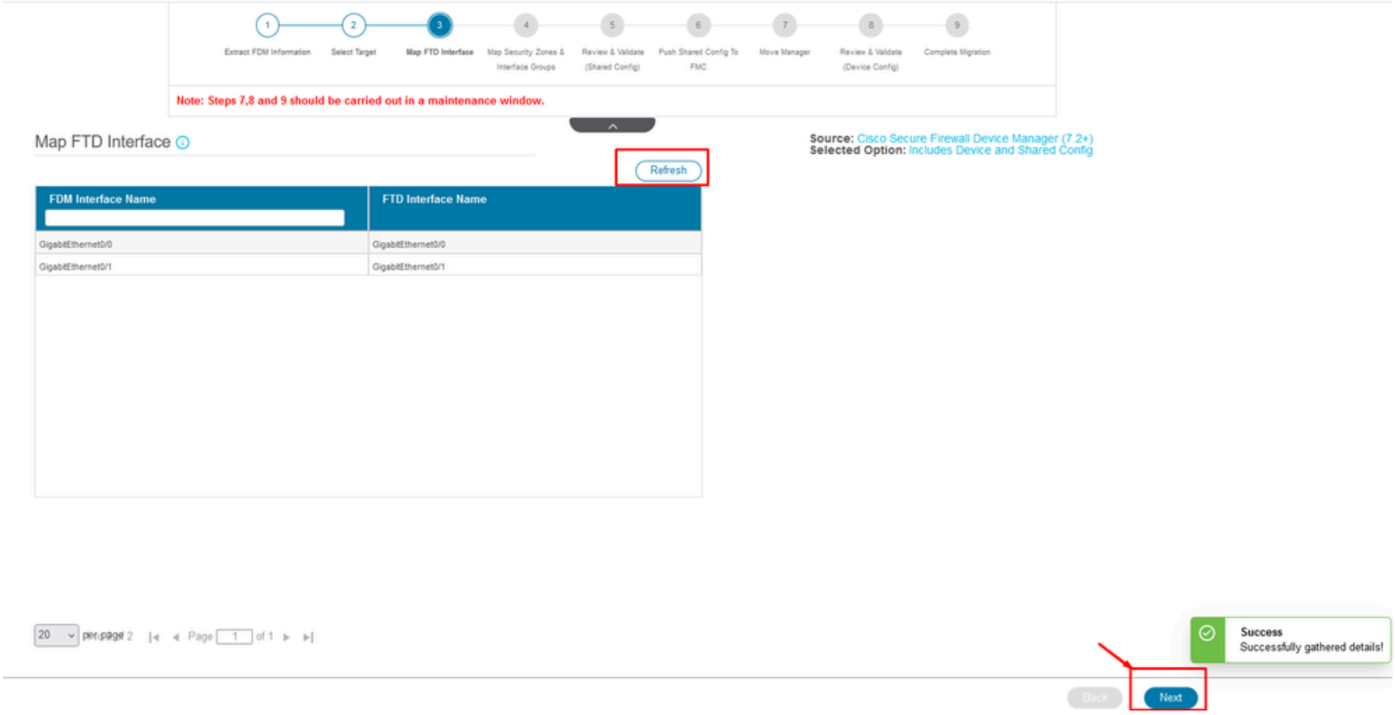
1
DHCP
(Server, Relay, DDNS)

0
Site-to-Site VPN Tunnels

0
Remote Access VPN
(Connection Profiles)

レポートのダウンロード

デバイスインターフェイスが表示されるように設定されています。ベストプラクティスとして、Refreshをクリックしてインターフェイスを更新することを推奨します。検証されたら、Nextをクリックして続行できます。



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 FTD Interface

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

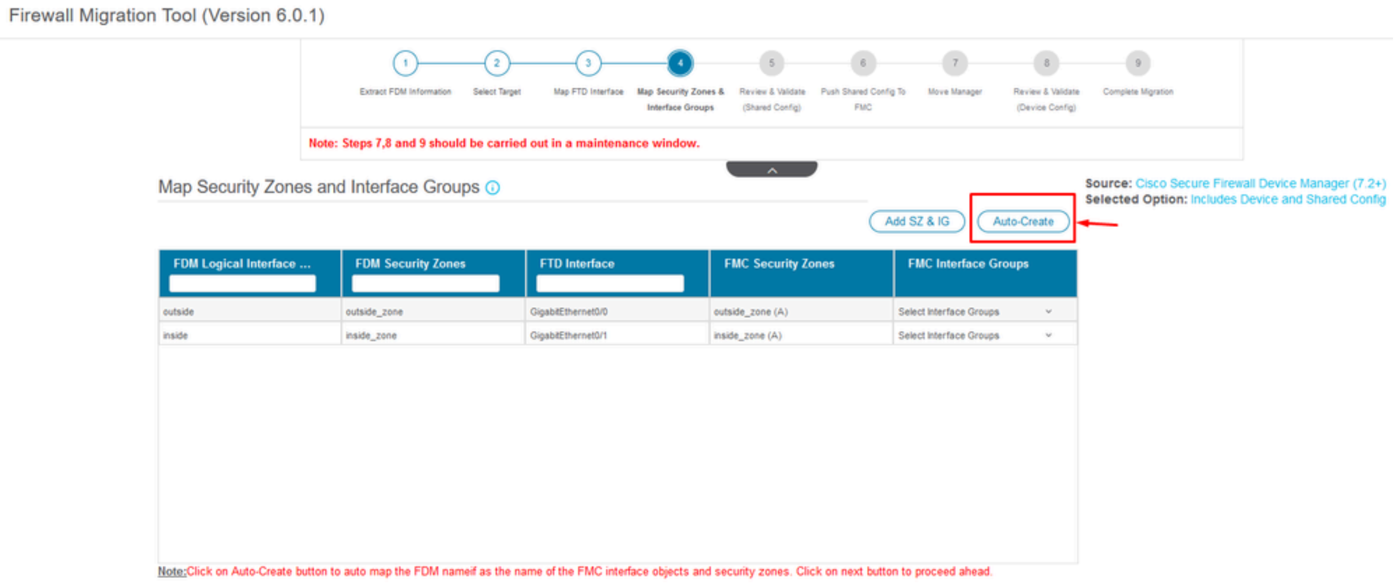
20 per page 2 Page 1 of 1

Success
Successfully gathered details!

表示されるインターフェイス

Security Zones and Interface Groupsセクションに移動します。このセクションで、Add SZ &

IGを使用して手動で追加する必要があります。 この例では「Auto-Create」が選択されています。これにより、移行先のFMC内でインターフェイスを自動的に生成できます。完了したら、Nextボタンをクリックします。


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

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

Map Security Zones and Interface Groups

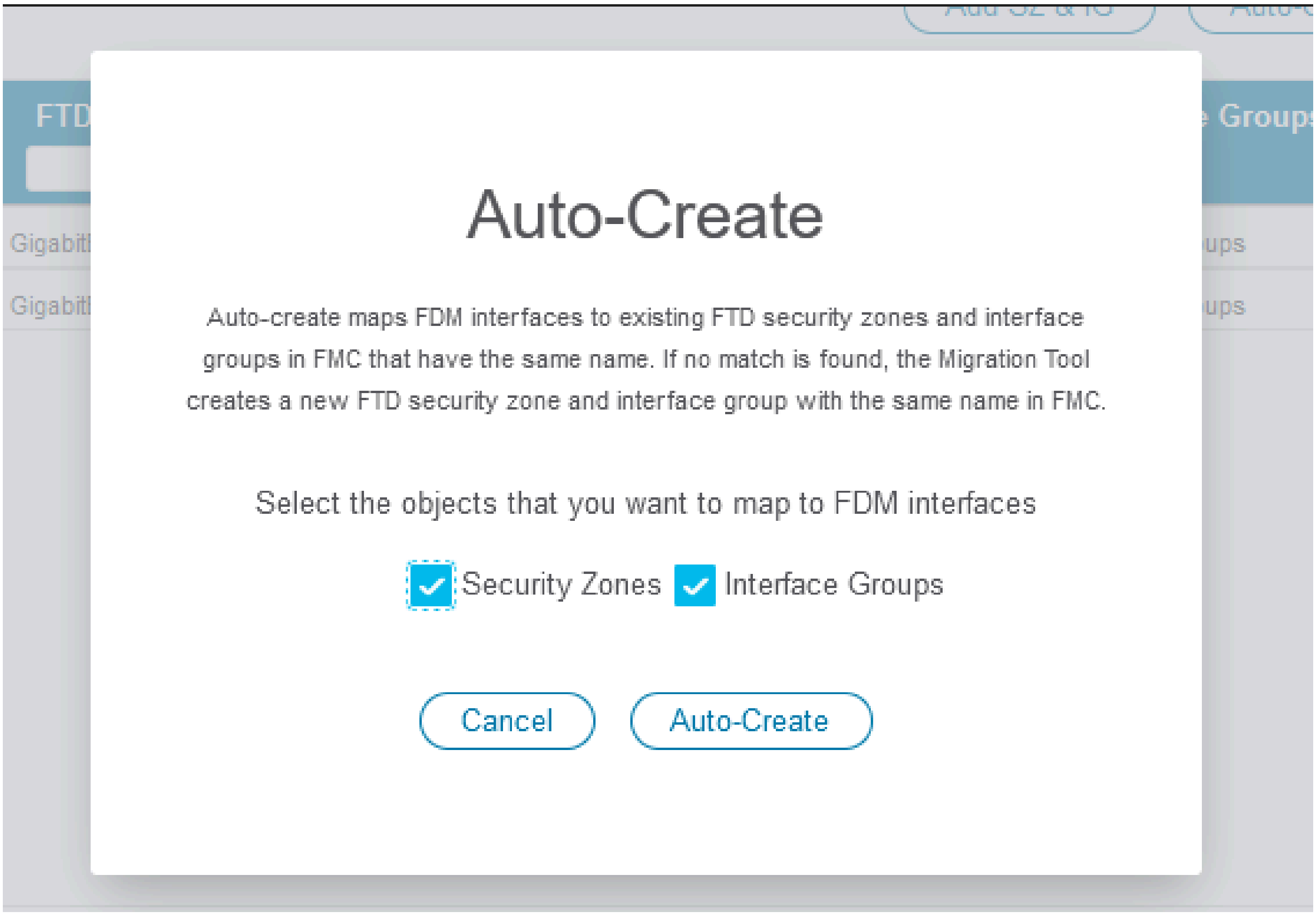
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

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.

セキュリティゾーンとインターフェイスグループ

自動作成オプションは、FDMインタフェースを既存のFTDセキュリティ・ ゾーンおよびFMC内の同じ名前のインタフェース・グループにマッピングします。



Auto-Create

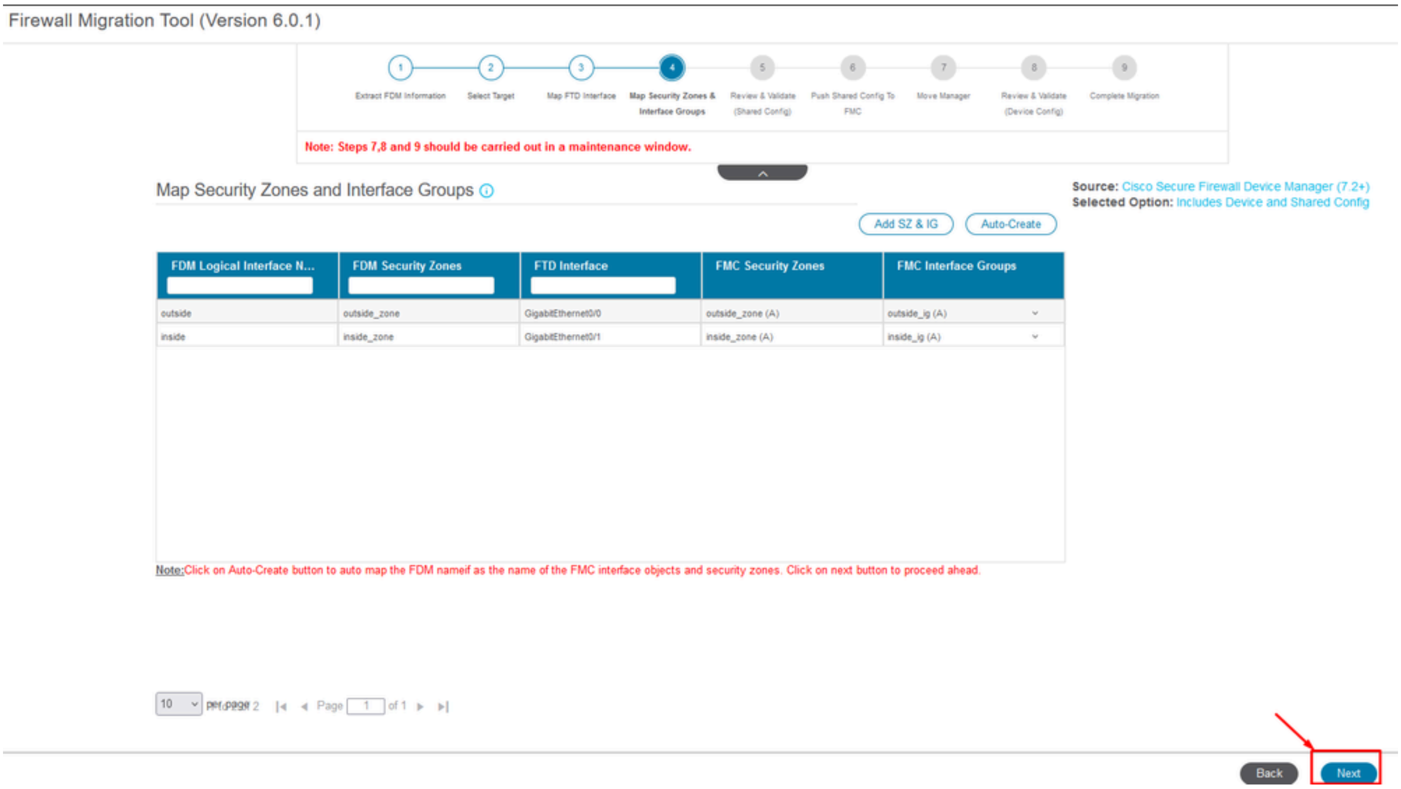
Auto-create maps FDM interfaces to existing FTD security zones and interface groups in FMC that have the same name. If no match is found, the Migration Tool creates a new FTD security zone and interface group with the same name in FMC.

Select the objects that you want to map to FDM interfaces

☑ Security Zones ☑ Interface Groups

Auto-Createオプション

次にNextを選択します。



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

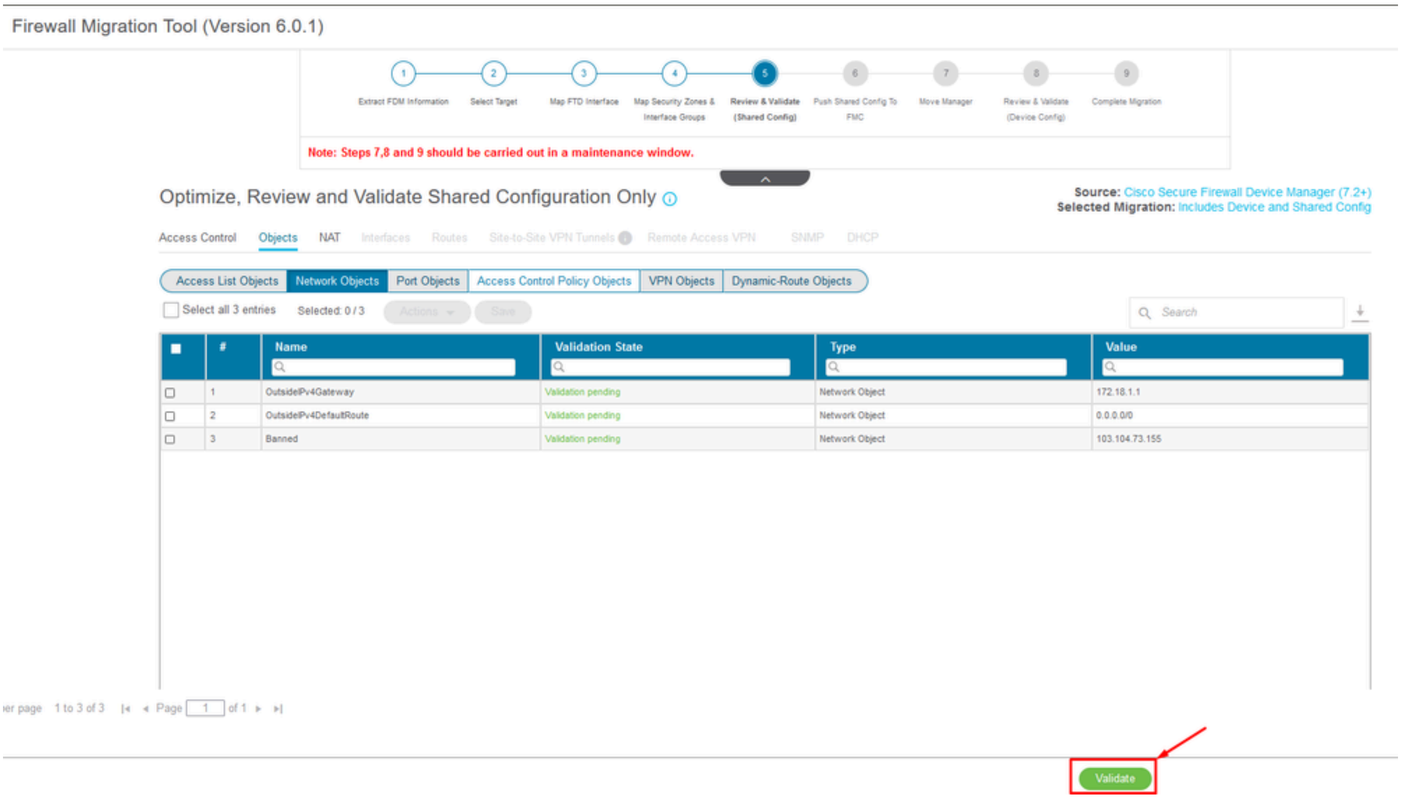
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Logical Interface 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 Auto-Creationオプション

手順5では、上部のバーに示されているように、時間をかけてアクセスコントロールポリシー(ACP)、オブジェクト、およびNATルールを調べます。各項目を注意深く確認して続行し、Validateをクリックして、名前や設定に問題がないことを確認します。



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.

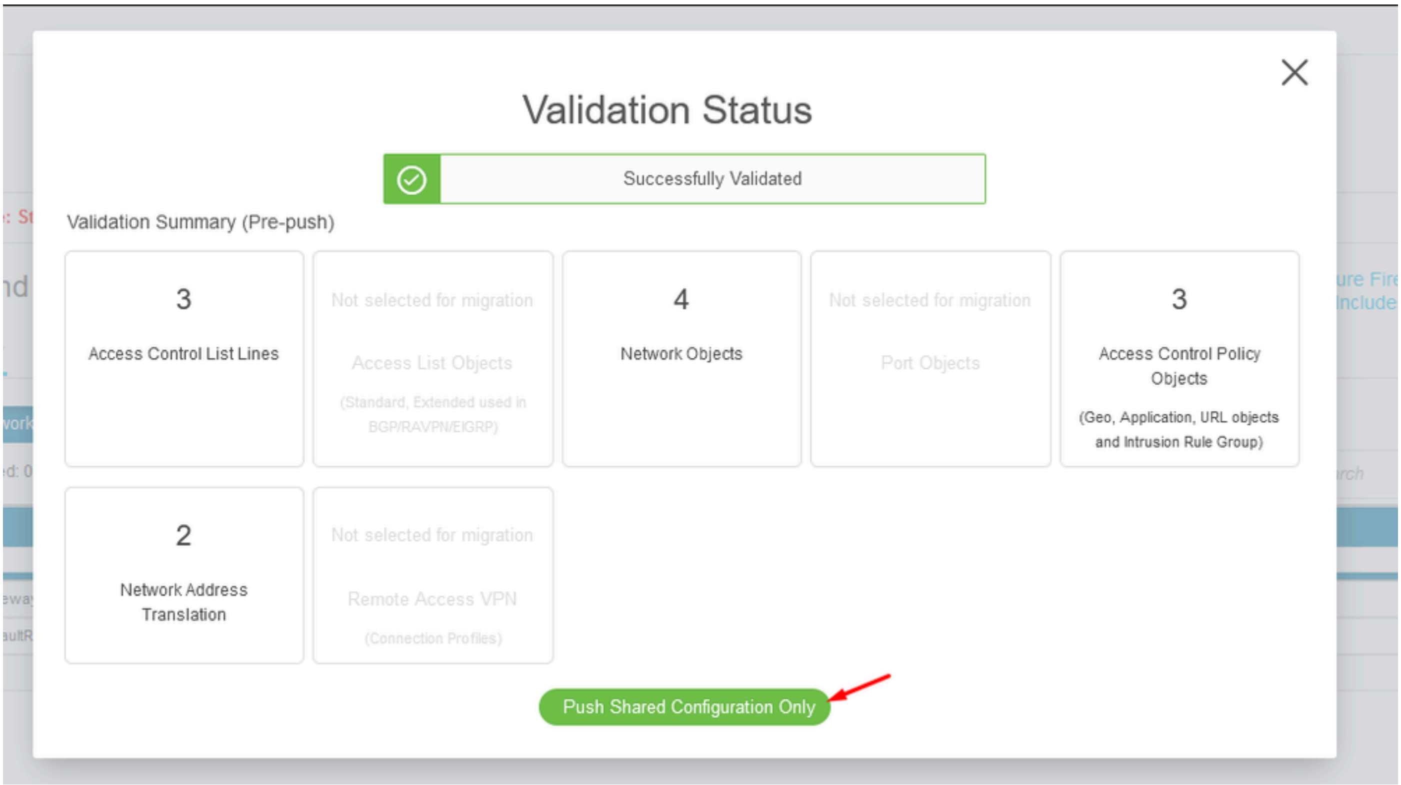
Optimize, Review and Validate Shared Configuration Only

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

■	#	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

アクセスコントロール、オブジェクト、およびNAT設定

次に、共有設定のみをプッシュします



Validation Status

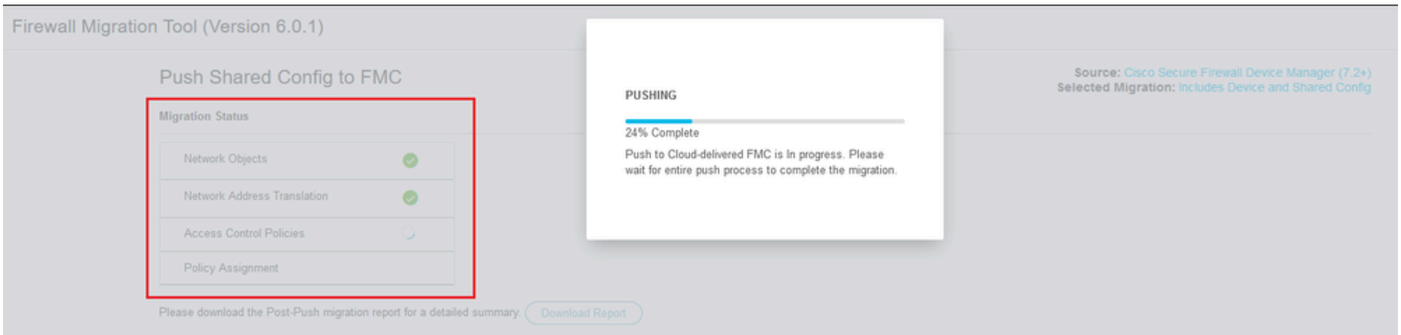
Successfully Validated

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)			

プッシュ共有構成のみ

完了の割合と作業している特定のタスクを確認できます。



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.

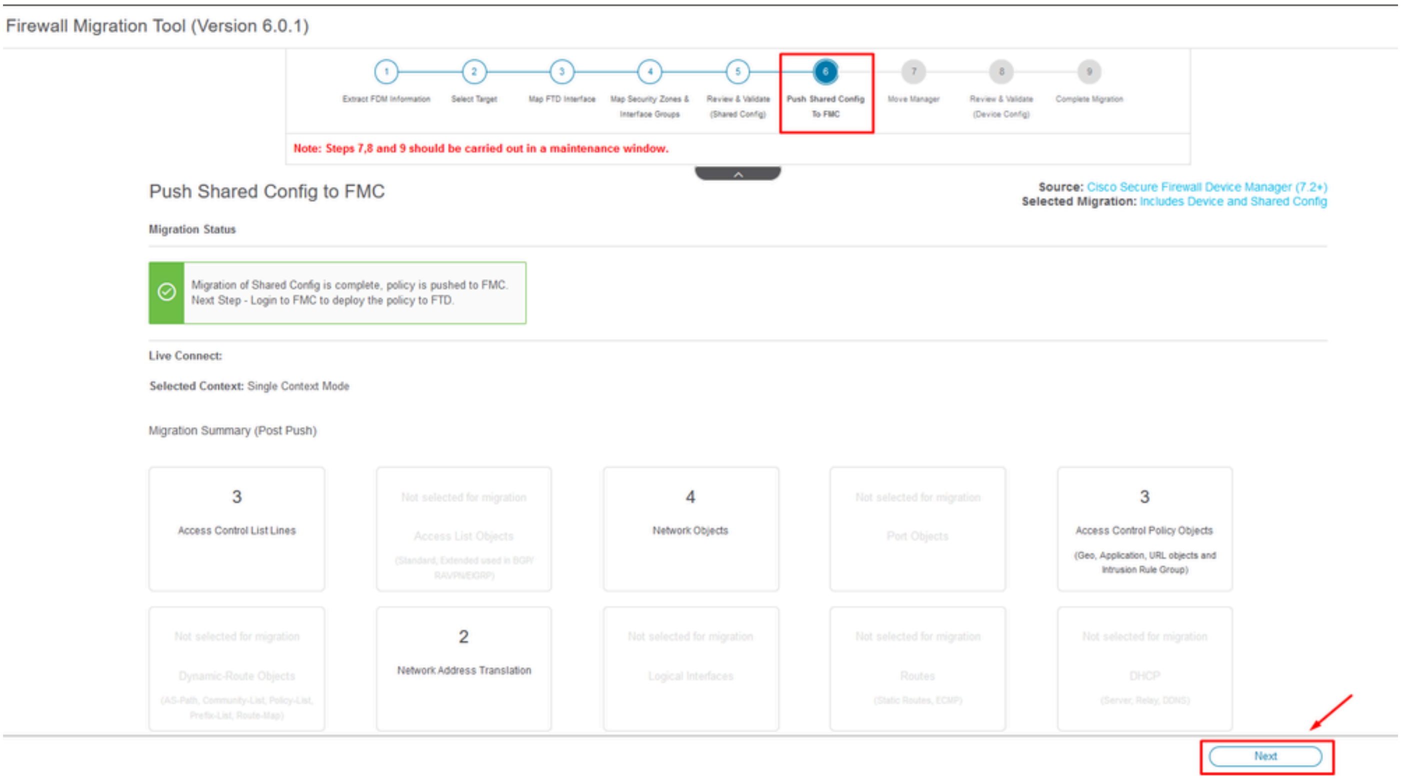
PUSHING

24% Complete

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

プッシュ率

手順5が完了したら、上部のバーに表示されている手順6に進みます。このバーで、共有設定をFMCにプッシュします。ここで、Nextボタンを選択して次に進みます。


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:

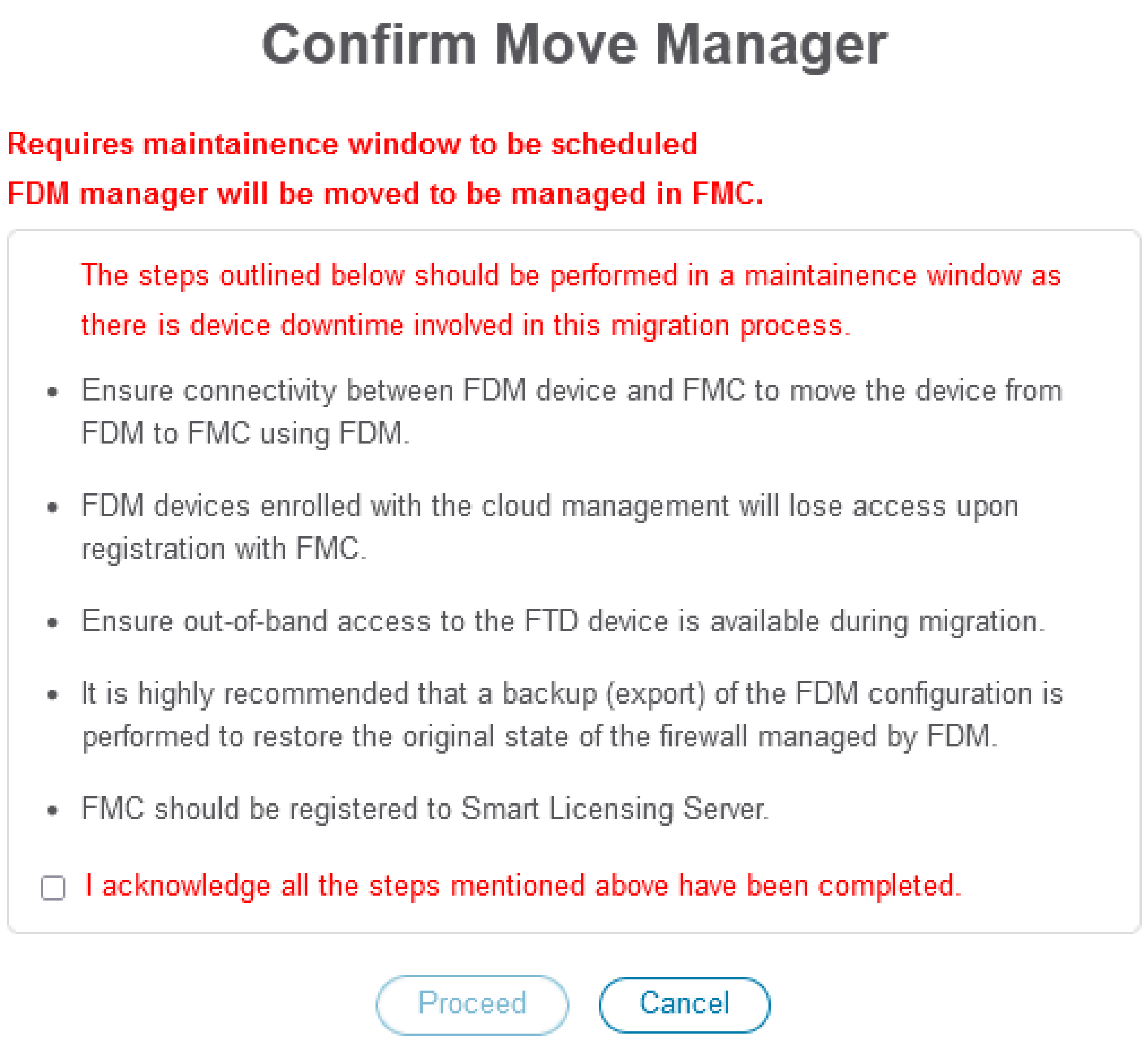
Selected Context: Single Context Mode

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)

共有構成のFMCへのプッシュが完了しました

このオプションを選択すると、確認メッセージが表示され、マネージャの移行の続行を促すメッセージが表示されます。


Confirm Move Manager

Requires maintainence window to be scheduled

FDM manager will be moved to be managed in FMC.

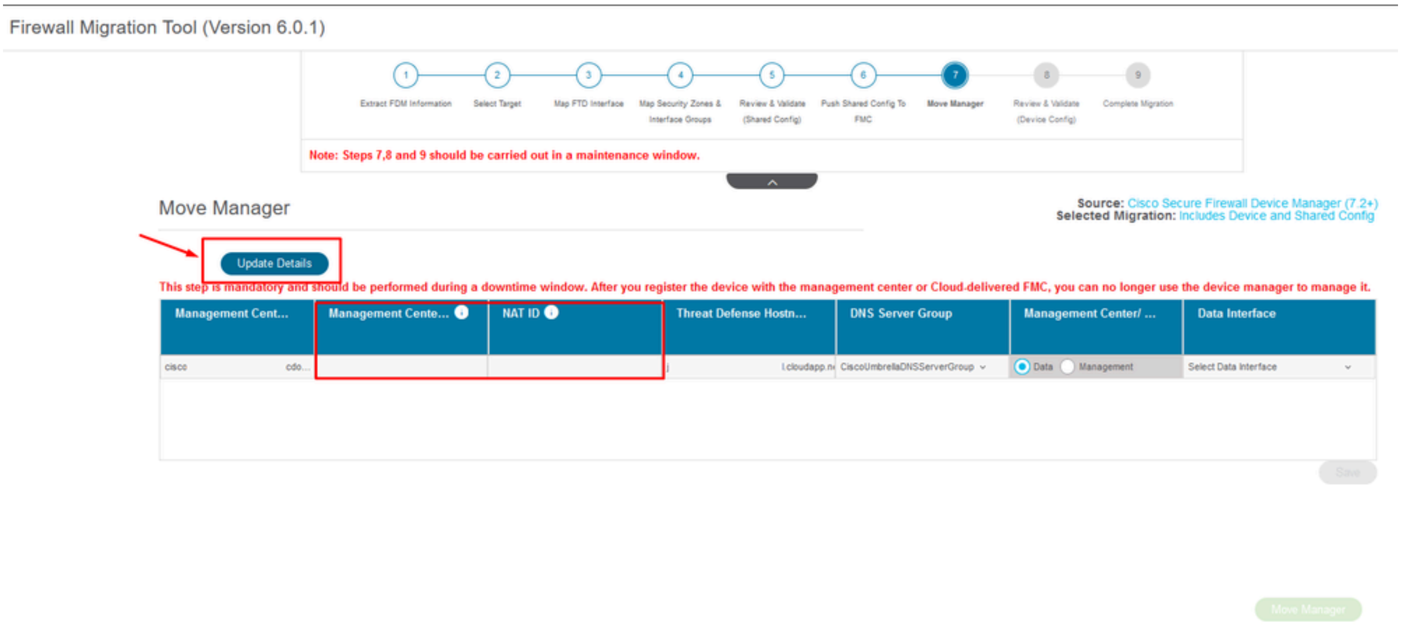
The steps outlined below should be performed in a maintainence window as there is device downtime involved in this migration process.

- 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.

移動マネージャの確認

マネージャの移行を進めるには、Management Center IDとNAT IDを手元に用意しておく必要があります。これは必須です。これらのIDは、Update Detailsを選択して取得できます。この操作によって、cdFMC内のFDM表現の目的の名前を入力するポップアップウィンドウが開始され、続いて変更が保存されます。



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.

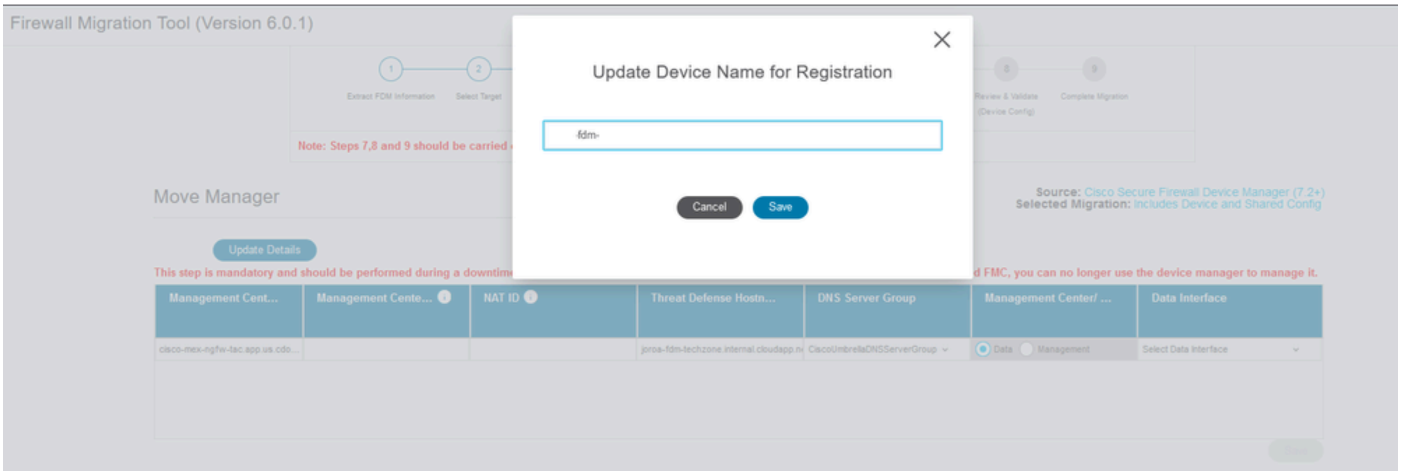
Move Manager

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

マネージャセンターIDとNAT ID



Firewall Migration Tool (Version 6.0.1)

Update Device Name for Registration

-fdm-

Move Manager

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

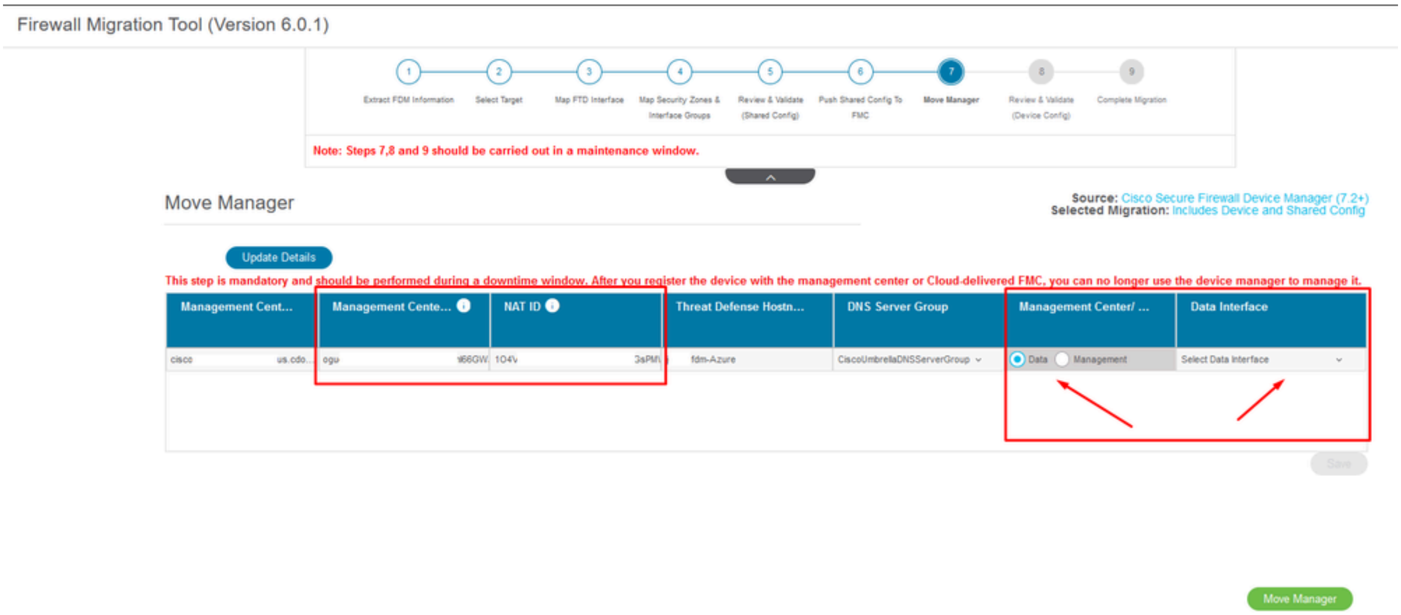
This step is mandatory and should be performed during a downtime ... d FMC, you can no longer use the device manager to manage it.

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

登録するデバイス名を更新します。

この操作の後、前述のフィールドのIDが表示されます。

警告: Management Centerインターフェイスは変更しないでください。デフォルトでは、[管理]オプションが選択され、このオプションはデフォルト設定のままになっています。



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.

Move Manager

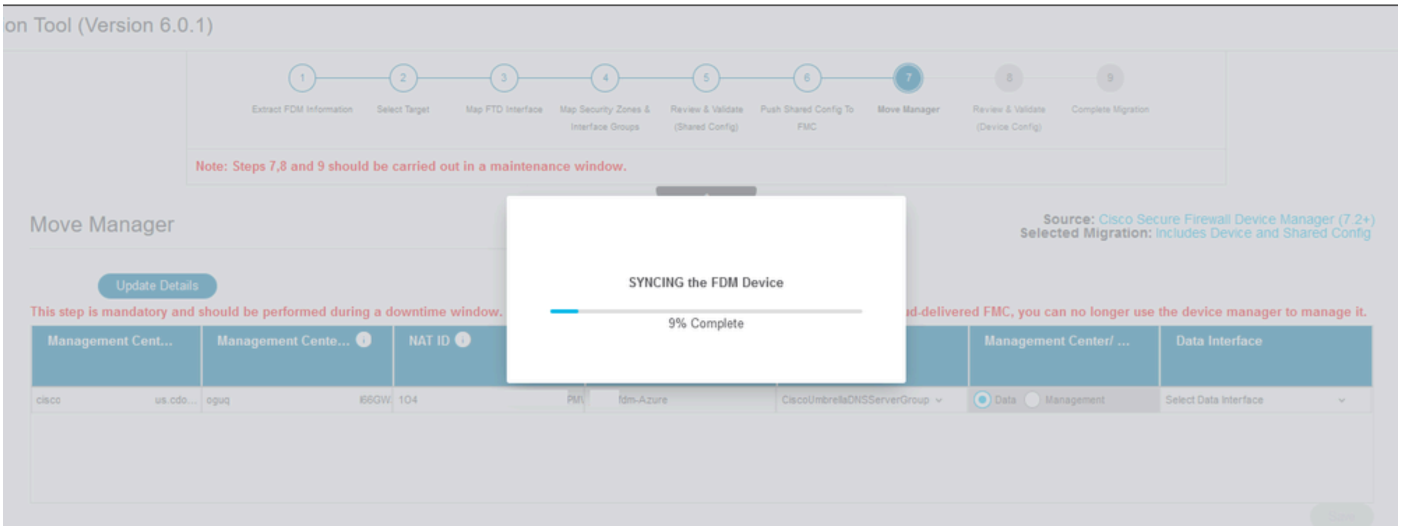
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Migration: Includes Device and Shared Config

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 166GW	104\ 3sPM	fdm-Azure	CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

管理センターIDとNAT ID。

Update Detailsオプションを選択した後、デバイスの同期が開始されます。



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

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. d-delivered FMC, you can no longer use the device manager to manage it.

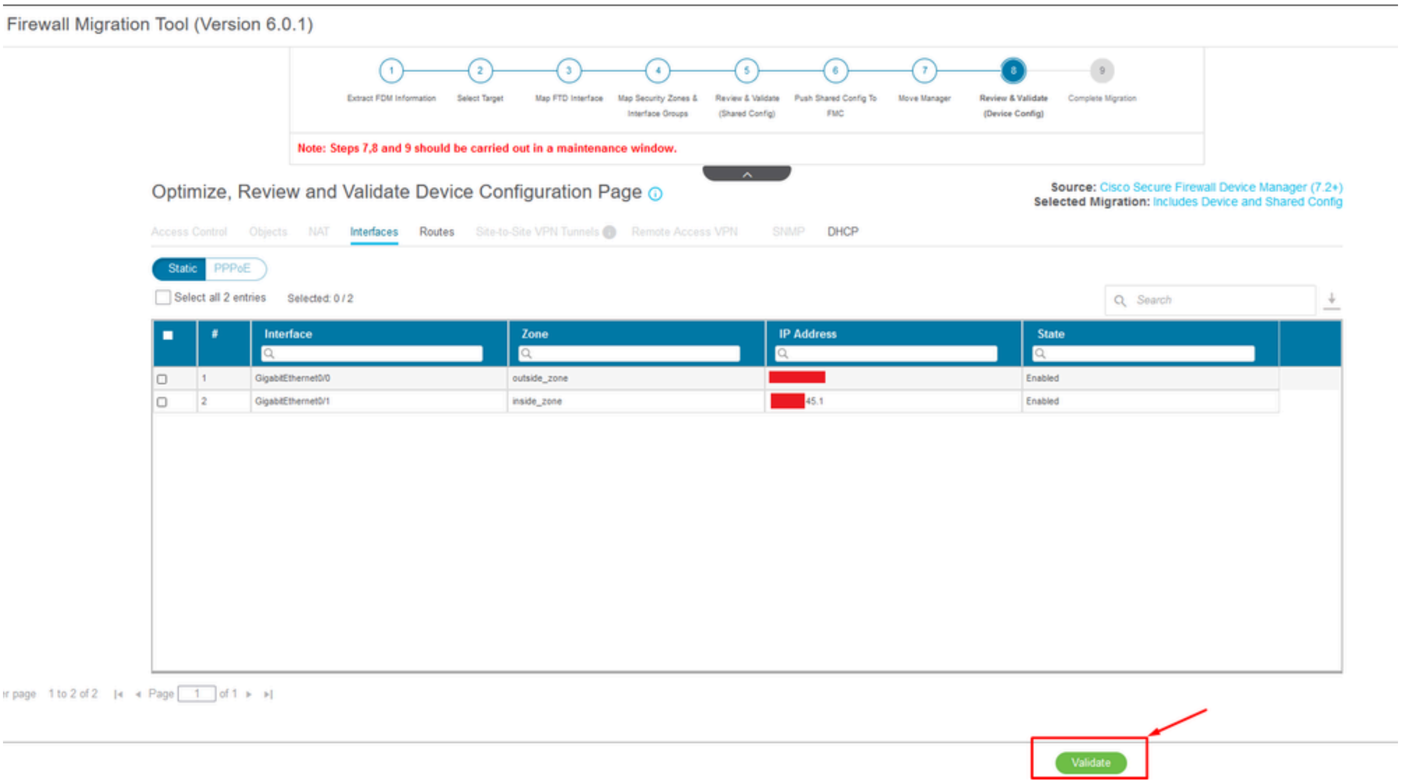
SYNCING the FDM Device

9% Complete

Management Cent...	Management Cente...	NAT ID			Management Center/ ...	Data Interface
cisco us.cdo...	oguq 166GW	104 PM	fdm-Azure	CiscoUmbrellaDNSServerGroup	● Data ○ Management	Select Data Interface

FDMデバイスの同期

移行が完了したら、次の手順として、検証を選択してFDMで構成されているインターフェイス、ルート、およびDHCP設定を確認します。



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

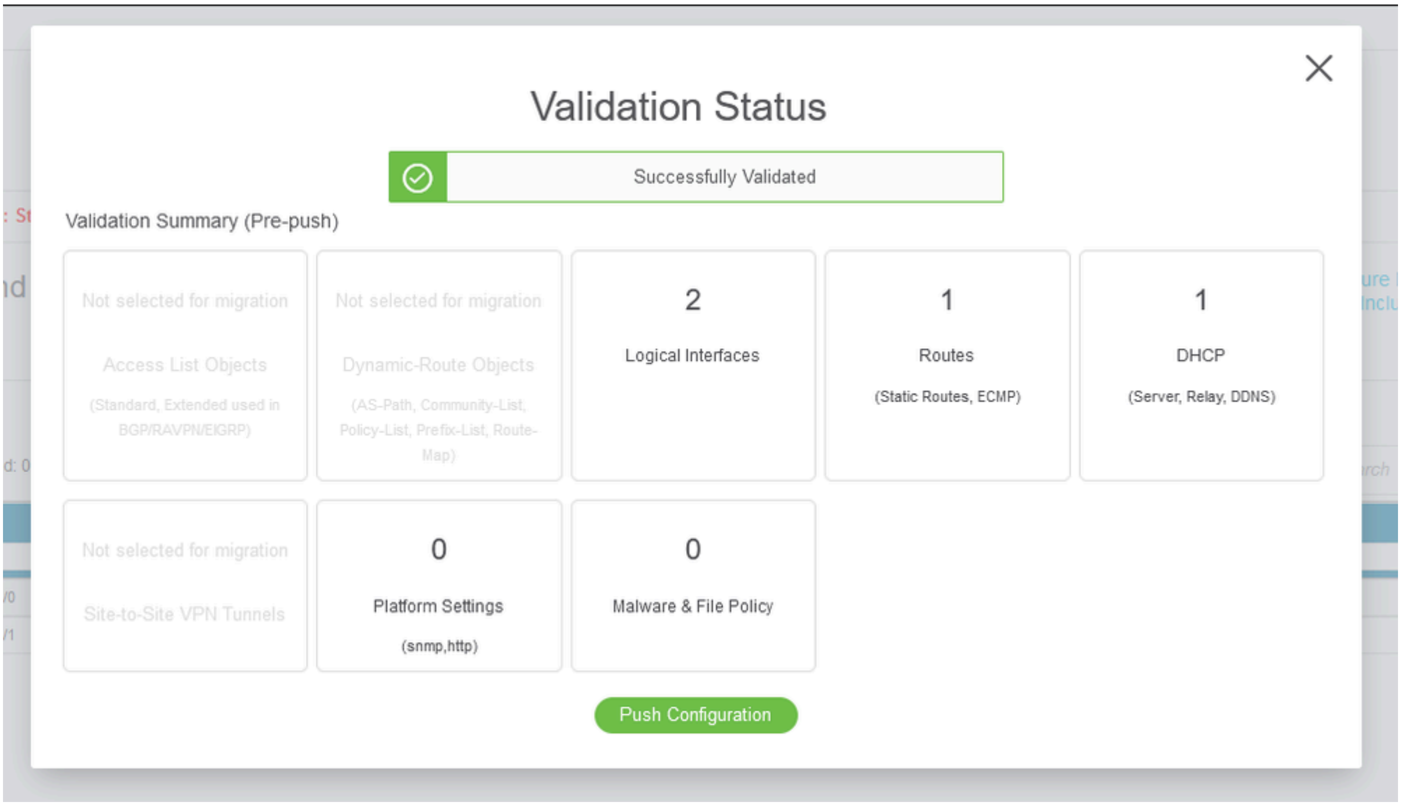
□ Select all 2 entries   Selected: 0 / 2

■	#	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 ▸ ▸|

FDM構成設定の検証

検証後、Push Configurationを選択して設定のプッシュプロセスを開始します。このプロセスは、移行が終了するまで続行されます。また、実行中のタスクを監視することもできます。



Validation Status

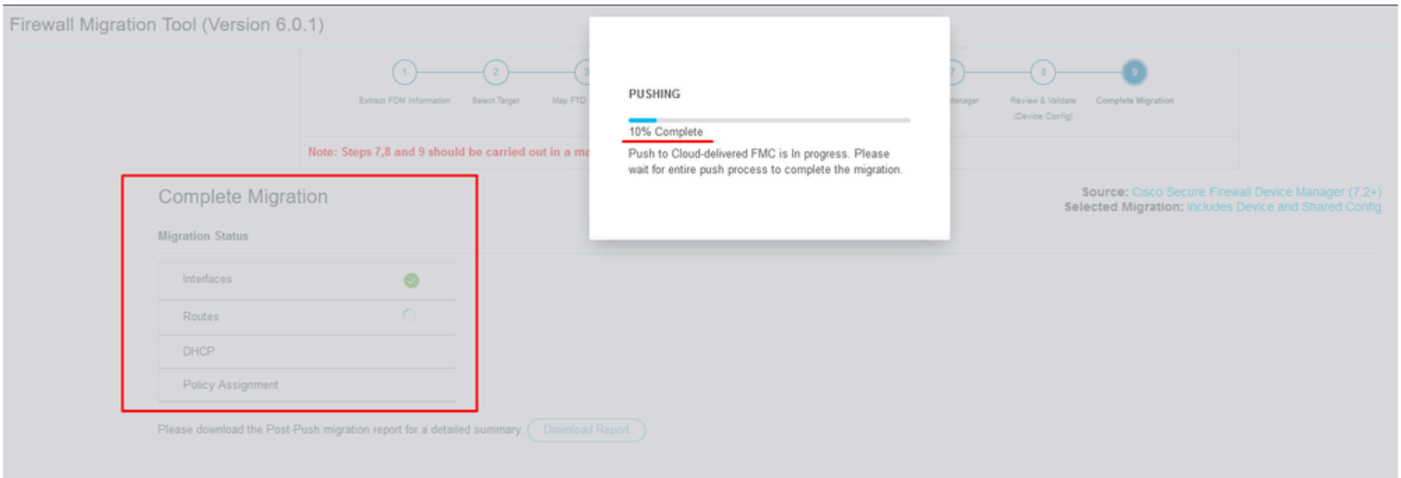
Successfully Validated

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		

検証ステータス：プッシュ設定。

プッシュ率の構成を示すポップアップウィンドウ。



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.

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

Complete Migration

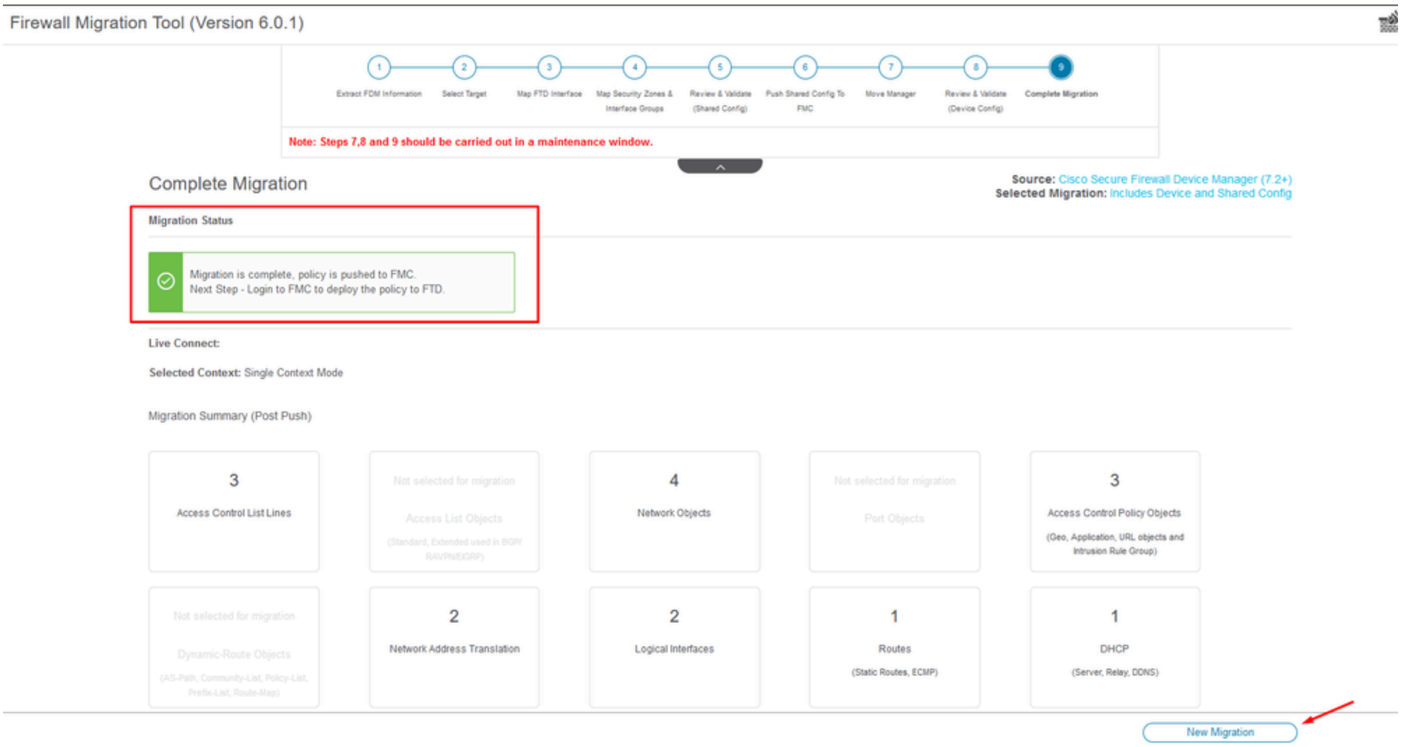
Migration Status

- Interfaces ✓
- Routes
- DHCP
- Policy Assignment

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

プッシュ率の完了

完了すると、新しい移行を開始するオプションが表示され、FDMからcdFMCへの移行プロセスが終了します。



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.

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)

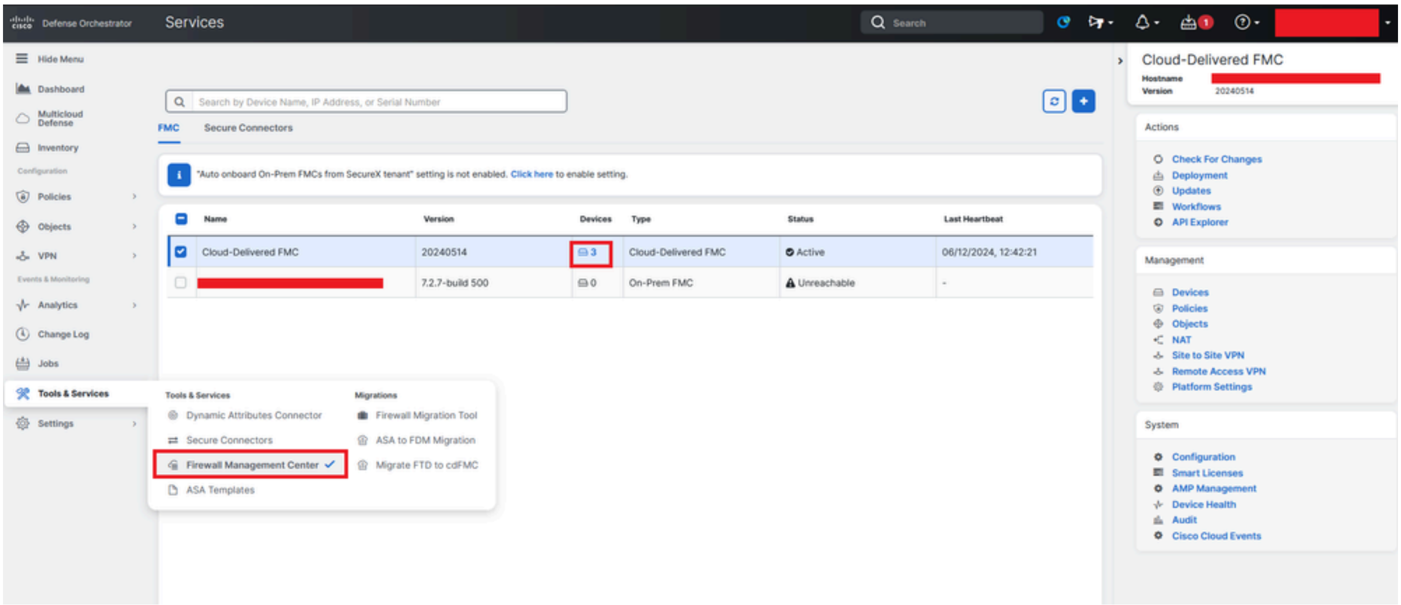
3 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Not selected for migration Dynamic-Route 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)

完全移行

確認

FDMがcdFMCに正常に移行されたことを確認します。

CDO > Tools & Services > Firepower Management Centerの順に移動します。そこに、登録されたデバイスの数が増えていることがわかります。



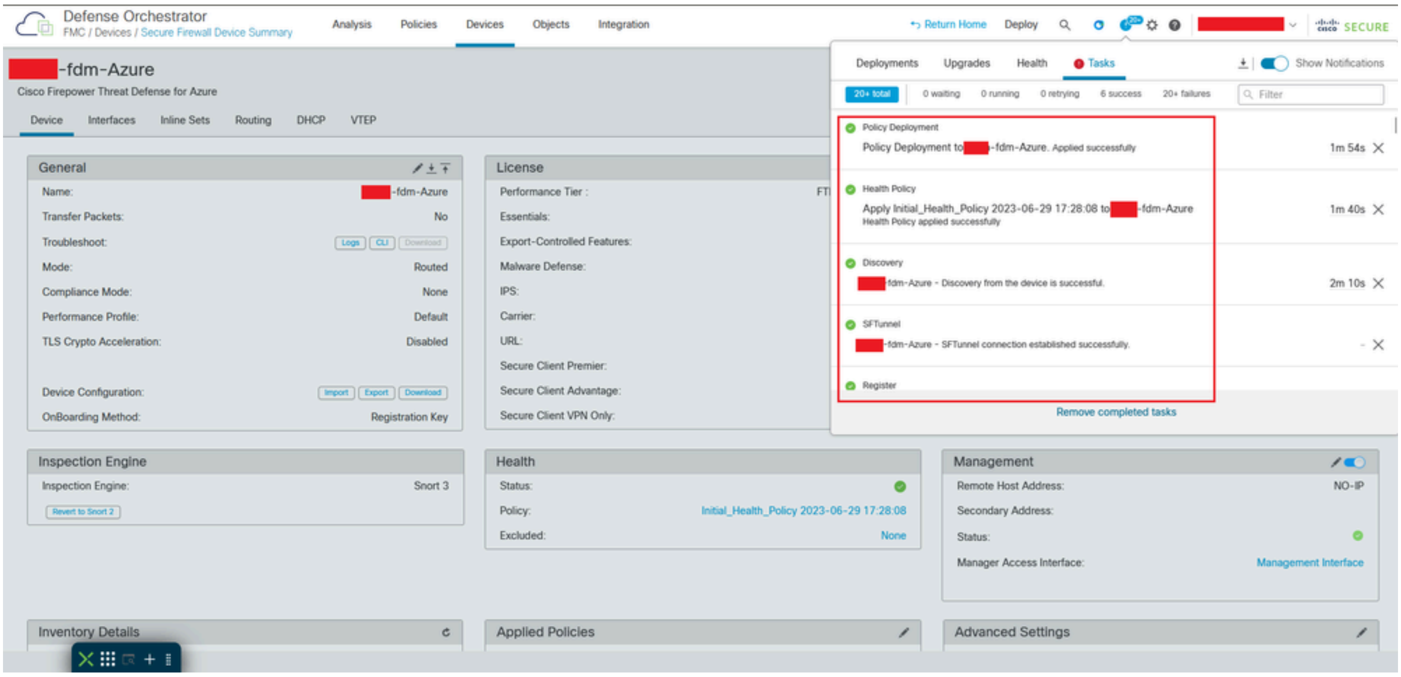
"Auto onboard On-Prem FMCs from SecureX tenant" setting is not enabled. Click here to enable setting.

	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	-

Hostname [redacted]
Version 20240514

cdFMCに登録されているデバイス

Devices > Device Management内でデバイスを確認します。また、FMCのタスクでは、デバイスが正常に登録され、最初の導入が正常に完了した時点を確認できます。



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

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

License
Performance Tier : FTI
Essentials:
Export-Controlled Features:
Malware Defense:
IPS:
Carrier:
URL:
Secure Client Premier:
Secure Client Advantage:
Secure Client VPN Only:

Inspection Engine
Inspection Engine: Snort 3

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

20+ total 0 waiting 0 running 0 retrying 6 success 20+ failures Filter

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

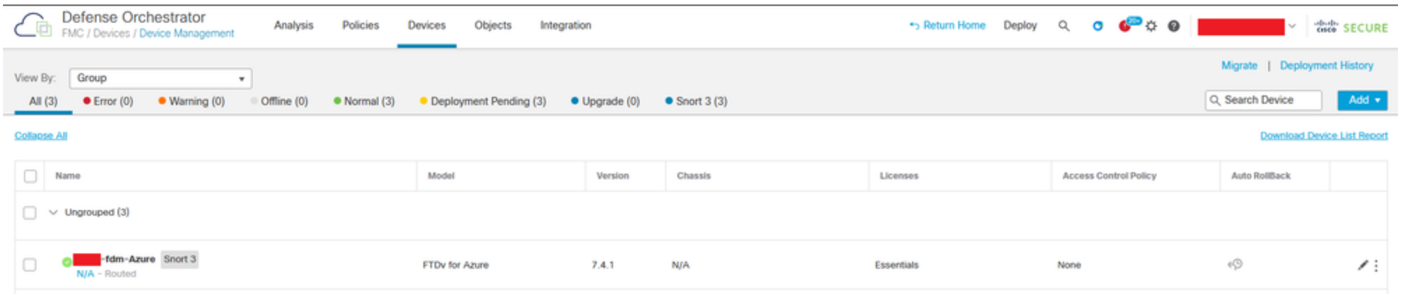
Discovery
[redacted]-fdm-Azure - Discovery from the device is successful. 2m 10s

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

Register

cdFMC登録タスクが完了しました。

デバイスはcdFMC > Device > Device Managementにあります。

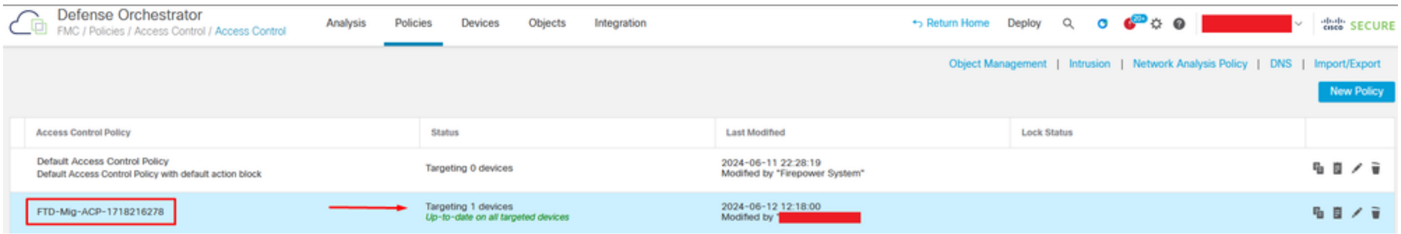


View By: Group
All (3) Error (0) Warning (0) Offline (0) Normal (3) Deployment Pending (3) Upgrade (0) Snort 3 (3)

	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	

cdFMCに登録されているデバイス

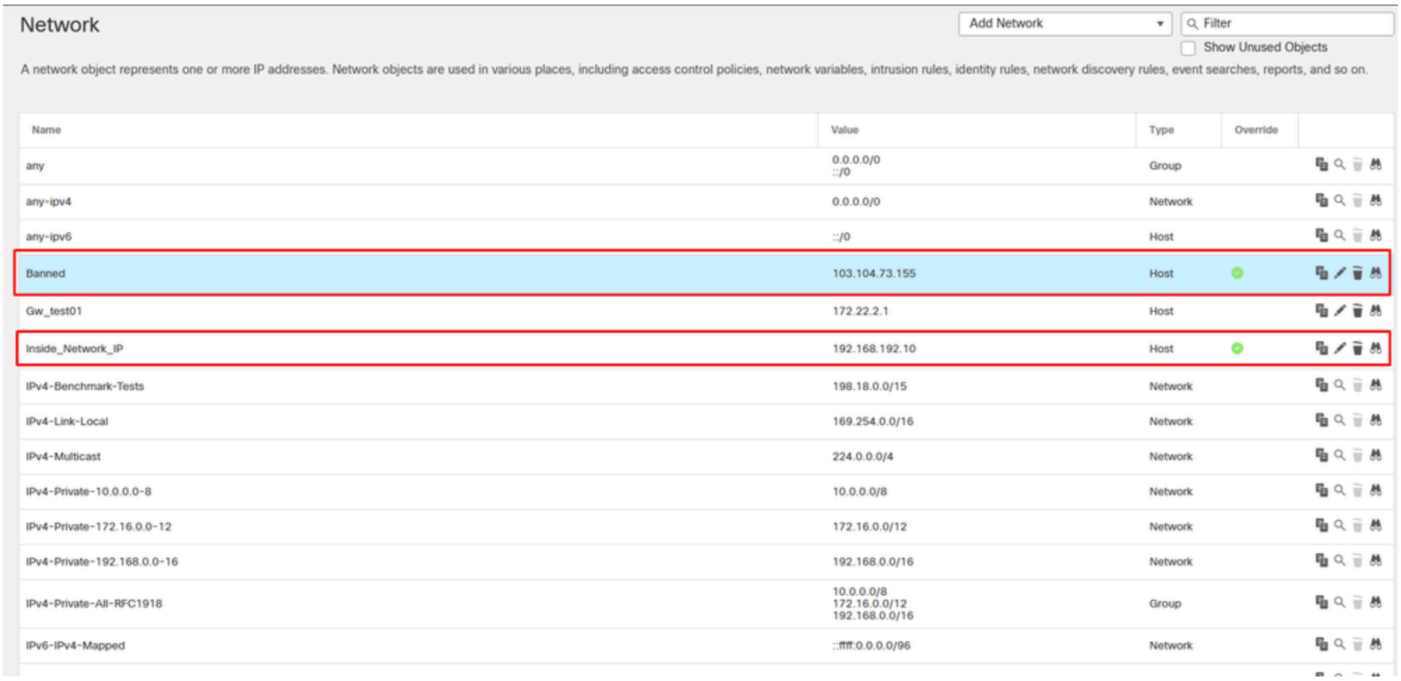
アクセスコントロールポリシーはPolicies > Access Controlで移行しました。


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]	

移行ポリシー

同様に、cdFMCに正しく移行されたFDMで作成されたオブジェクトを確認できます。

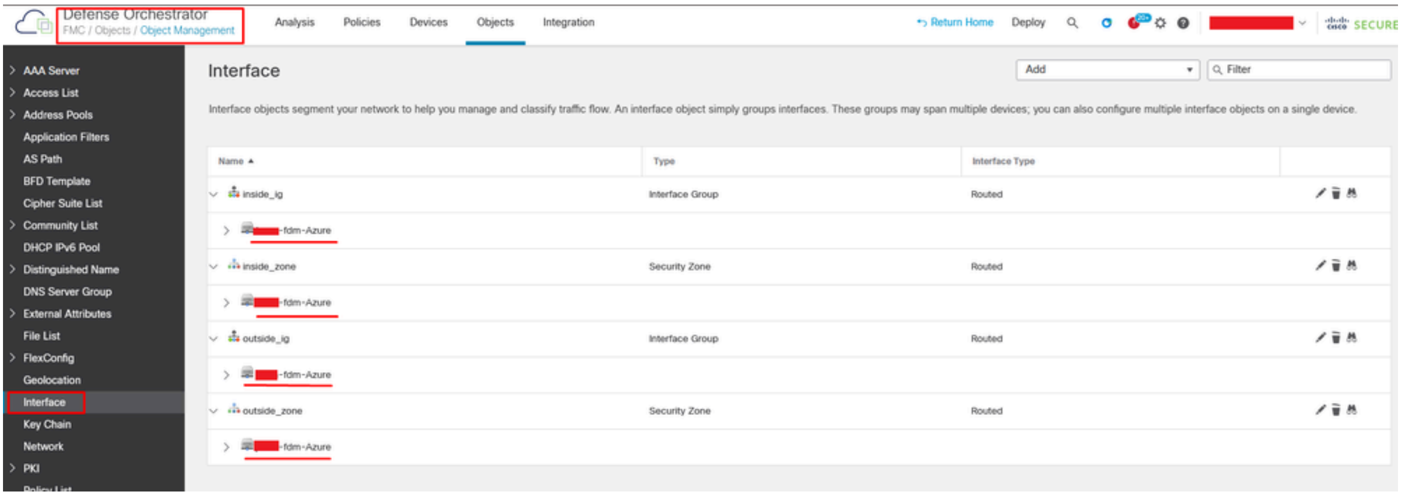


A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

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	

FDMからcdFMCに移行されたオブジェクト

オブジェクト管理インターフェイスが移行されました。



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
[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		

オブジェクト管理インターフェイスが移行されました。

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。