

لخاد FMT مادختساب CDfmc ىلإ FDM لىحرت CDO

تايوتحملا

[عمدقملا](#)

[ةيساسالاب لطلتملا](#)

[تاب لطلتملا](#)

[عمدختسملا تانوكملا](#)

[ةيساسا تامولعم](#)

[نيوكتللا](#)

[قحصلا نم ققحتلا](#)

عمدقملا

ةرادا يف مكحتلا ءدحو ىلإ FirePOWER (FDM) ءزهجأ ري دم لىحرت ءيفيك دننتمسلا اذه حضوي FirePOWER لىحرت ءادا مادختساب (CDfmc) ءباحسلا ربع اهميلست متي يتلا (FMC) ءزهجالا CDO يف (FMT).

ةيساسالاب لطلتملا

تاب لطلتملا

- Firepower (FDM) 7.2+ زاهج ري دم
- ءباحسلا ءكبشلا هرفوت يذلا (CDfmc) ءيامحلا راج ءرادا زكرم
- CDO يف ءنمضملا Firepower (FMT) لىحرت ءادا

عمدختسملا تانوكملا

افنأ ءروكذملا تاب لطلتملا ىلإ اءانتسا ءقيلثولا هذو ءعضو دقو

- 7.4.1 رادصإلا ىلع Firepower (FDM) زاهج ري دم
- ءباحسلا ءكبشلا هرفوت يذلا (CDfmc) ءيامحلا راج ءرادا زكرم
- Cloud Defense Orchestrator (CDO)

ءصاخ ءيلمعم ءئيب يف ءدووملا ءزهجالا نم دننتمسلا اذه يف ءدراولا تامولعملا ءاشنإ مت تناك اذإ. (يضارتفا) حوسمم نيوكتب دننتمسلا اذه يف عمدختسملا ءزهجالا ءيمج ءأب رمأ يال لمحتملا ريثأتلل كمهف نم دكأف، ليغشتلا دي قكتكبش

ةيساسا تامولعم

يف مكحتلا ءدحو ىلإ مهب ءصاخلا ءزهجالا لىحرت تاي لعم ءارجإ CDO ءرادا يم دختسملا نكمي

يف. يلع رادصا و 7.2 رادصا يلع ؤزهألا نوكت ام دنع (CDfmc) ؤيساسألا ؤحوللا ؤرادا
CDO رجأتسم يلع لعلاب CDfmc نيكت مت ،دنتسمل اذه يف حضوملا ليحرتلا

نيوكتلا

1.- FDM يلع ؤيباحسلا Cisco تامدخ نيكت مت

تامدخ يلا ليحستلا و ؤقلعم رشن تاي لعم نودب FDM زاغ دوچو يرورضلا نم ،ليحرتلا ادب
تامدخ > ديزملا عجار > ماظنلا تاداعا يلا لقتنا ، ؤيباحسلا تامدخ يف ليحستلا . ؤيباحسلا
ؤيباحسلا

ليحستلا عارچا يرورضلا نم ،كلذل ، لچسم ريغ زاغلا نأ دجت ، ؤيباحسلا تامدخ مسق نمض
ليحستلا م ، ليحست حاتفم نيوكت بچي . CDO/نامألا باسح عون مادختساب

ليحستلا ؤيباحس تامدخ

ري فو تب مقو CDO باسح ليحست عون ددح . هليحست متي مل نأ رهظي ، ؤيباحسلا تامدخ رب
CDO نم ليحستلا حاتفم

ةباحسلا تامدخ ىلا لىجستلا

> نوزخملا ىلا لقتنا، CDO ىلا لقتنا. CDO لخاد لىجستلا حاتم ىلع روثعلا نكمي زمر ةفاضلا.

الوا، كيدل FDM راخ ني كمت بجي. FTD راخ دح. كيدل يذال زاخلا عون ديدحتل ةمئاق رهظت اذه في. لىجستلا مادختسا حاتم لىجستلا عون مدختسي. قباطملا لىجستلا عارجا نكمي ال FDM. في اهقصلو اهخسن بجي يتلاوا، 3 مقرر ةوطخلال في لىجستلا حاتم رهظي، راخلا

FDM ةحوللا ىلع راخ ةفاضلا

ةمدخ عون وا زاخ ديدحتل ةمئاق رهظت

Select a Device or Service Type

No Secure Device Connector found to communicate with some types of devices. [Set up a Secure Device Connector](#)



ASA

Adaptive Security Appliance
(8.4+)



Multiple ASAs

Adaptive Security Appliance
(8.4+)



FTD

Cisco Secure
Firewall Threat Defense

Meraki

Meraki

Meraki Security Appliance



Integrations

Enable basic CDO functionality for
integrations



VPC

AWS VPC

Amazon Virtual Private Cloud



Duo Admin

Duo Admin Panel

Umbrella

Umbrella Organization

View Umbrella Organization Policies
from CDO



Import

Import configuration for offline
management

مداخله وازجاله عون ديدت

دنتسمل اذهل ليجست حاتفم ديدت م

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.

ليجستال عون

ةقباسلا ةوطخلا يف بولطملا ليجستلا حاتفم ضرعي ،انه



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

ليجستلا ةيلمع

ليجست قوف رقناو FDM يف هقصلو حاتفملا خسنا ،ليجستلا حاتفم ىلع لوصحلا درجم بةروصللا يف حضوم وه امك نكمم وه امك هضرع متي ،ةباحسلا تامدخ لخاد FDM ليجست دعب

زاهجلا ليغشت درجمب زاهجلا ليجست متيس شيح "يكدللا صيخرتلا" يطخت مت

Device Summary

Cloud Services

✕ Not Registered

You can register the device with the Cisco cloud to use additional cloud-based services. If you want to use Cisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other security account registration key. You can alternatively auto-enroll with CDO or a Secure Firewall Management Center using the device serial number. If you want to use Secure Firewall device manager for management and are ready to license the device, then configure Smart Licensing, which automatically registers the device with the Cisco cloud. After you register with the cloud, you can enable or disable features as needed.

Enrollment Type

Security/CDO Account

Smart Licensing

Region

US Region

Registration Key

7a53c2

Service Enrollment

Cisco Defense Orchestrator

Cisco Defense Orchestrator is a cloud-based management tool used for managing network devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.

Enable Cisco Defense Orchestrator

Cisco Success Network

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

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

Enroll Cisco Success Network

REGISTER

Need help? [?](#)

FDM ليحس ت

ةلجس مل او ةلص تم لة باحس ل ا تام دخ و را جي ال ا ضرعي هن ا ف، FDM ليحس ت دن ع

Device Summary
Cloud Services

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

Cisco Defense Orchestrator ENABLE
Enabled

Cisco Success Network ENABLE
Enabled

Send Events to the Cisco Cloud ENABLE
Disabled

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

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

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

FDM في ليجستل لامتك

عجول اليلع هونوك يلمع في FDM لعل روثعل انكمي، نوزخلم ةمئاق في CDO، نمض لملع ريس مام مسق لخاد اهق فدتو ةنمزلم هذه مدقت ةعجارم انكمي. ةنمزلماو

ةلصتمو ةنمزلماهنا لعل رهظت، ةلملعل هذه لامتك درجمب

Inventory

Search: [Redacted]

Name	Configuration Status	Connectivity
ASA	-	Unreachable
FDM	-	Serial Number Mismatch
FTD	Not Synced	Pending Setup
FTD	-	Pending Setup
FTD	-	Pending Setup
fdm	Syncing	Online
FTD	-	Online
FTD	-	Online
FTD	Not Synced	Unreachable

Device Details
Model: Cisco Firepower Threat Defense for Azure
Serial: [Redacted]
Version: 741-172
Onboarding Method: Registration Key
Smart Version: 3.153.100-56

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

نتم لعل دوجومل CDO FDM نوزخم

Online و Sync لثم رهظت اهنا، ةزهجال ةنمزلم دنع

Synced Online

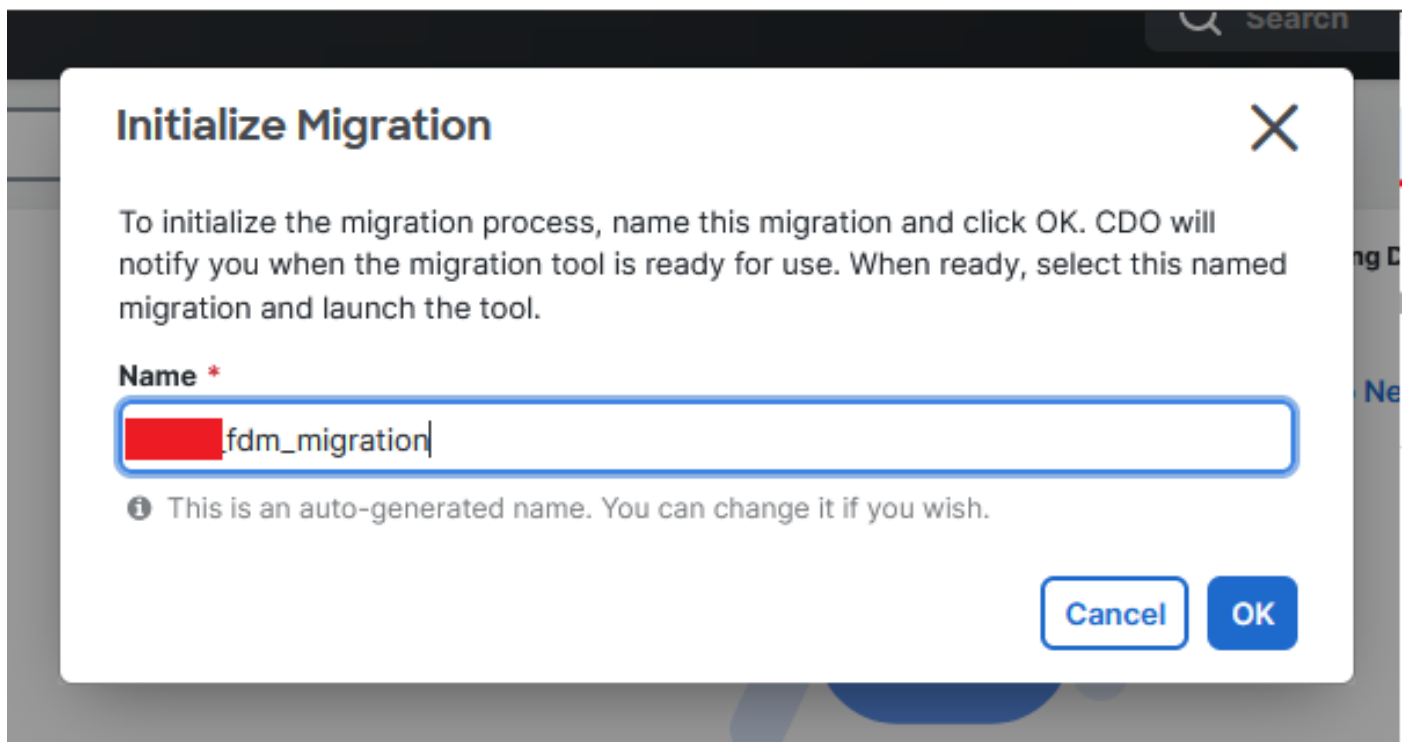
نم جورخلال ليجست دعب FDM نم جورخلال ليجست بجي، CDO ىلى حاجن ب FDM لوخد ليجست دنع
ةادأ > ليجرتال > تامدخل او تاولدال ىلى CDO لخد لقتنا، (FDM) لوحمال تاناي ب ةدعاق ةرادا
ةيامل رادج ليجرت



ةيمست ةداعل ىلى جاتحي مسالا نأ ىلى ريشي، يئاوشع مسا رهظيو، ةفاضل زم رىل ع رقنا
ليجرتال ةيلمع ادبل



ليجرتال ادبل ليجشت ىل ع رقنا، ةيمستال ةداعل دعب



ليجرتال ةيهت

ليجرتال نيوك ت ادبل ليجشت قوف رقنا

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

ليحترت الة لجمع قاطلطة لة لعمع

Cisco رايلال ديدحت متي شيح ليحترت الة لعمعل ذفان حت متيس، قاطلطة قوف رقلال دعب نم ة اءب رايلال اءه نيكت متي، اقباس ركذ امكو. Cisco Secure Firewall Device Manager (7.2+) رادصلال 7.2.



Firewall Migration Tool (Version 6.0.1)

Select Source Configuration (i)

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+)

ردصلال نيوك ت ديدحت ب FMT موقبي

طقف كرتشملال نيوك تالال: ةفلتخم ليحترت تارايل ةثال ث مي دقت متي، اء ديدحت درجمبو لى لكرتشملال تانيوك تالال و زاهال نمضت متي امك، ةكرتشملال تانيوك تالال و زاهال نمضت متي و ف TFD. ماطن في ة ديدجلال ةزهالال

FirePOWER Device Manager ليحترت وهو، يئثال رايلال ذي فنن متي، لالامل اءهل ةبسنلابل (كرتشملال نيوك تالال و زاهالال كلذ في امب).

How would you like to migrate from Firepower Device Manager :



Click on text below to get additional details on each of the migration options

Migrate Firepower Device Manager (Shared Configurations Only) >

Migrate Firepower Device Manager (Includes Device & Shared Configurations) v

- This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.
- **The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.**
- Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
- User should provide FDM credentials to fetch details.
- FDM Devices enrolled with the cloud management will lose access upon registration with FMC
- Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.
- It is highly recommended that a backup (export) of the FDM configuration is performed to restore the original state of the firewall managed by FDM if required.
- If the FTD devices are in a failover pair, failover needs to be disabled (break HA) before proceeding with moving manager from FDM to FMC.
- FDM with Universal PLR cannot be moved from FDM to FMC.
- FDM with flexConfig objects or flexconfig policies cannot be moved from FDM to FMC. The flexconfig objects and policies must be completely removed from FDM before migration.
- FMC should be registered to Smart Licensing Server.

Migrate Firepower Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware) >

Note :

ليحرتل تاراخي

ةرفوتل ةمئاقلا نم زاوجل ديحتل ةعباتملاب مق ، ليحرتل لبولسأ ديحت درجمب

Live Connect to FDM

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

Select FDM Managed Device

fdm - Available

Connect



FDM زاھج دېدھت

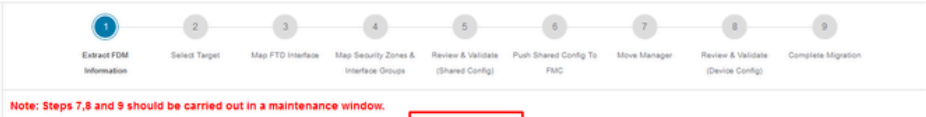
FDM device config extraction successful



100% Complete

نېوكتال جارختسا لم تكا

نھن یتال ةوطخل مھف و ةعجارمل لولعل اعزل ېف ةدوومال بېو بتال ةمالع حتف ب صوې
زاھجل دېدھت دنع اھلعل



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

ليحرت الة لملع تاوطخ

جهن مادختسا ديتر له رايلاب كتبلاطام دنع رمالاغل ددح، ةديجل ليحرت ة لملع كنوكل فمك على RAPN جهن و NAT، دوجوملا لوصولاب مكحتلا

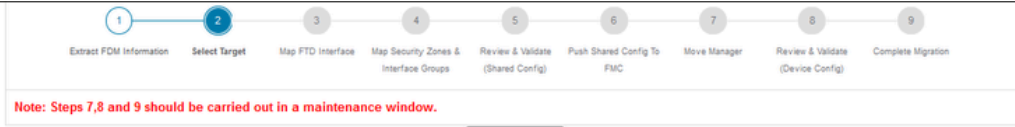
Do you want to use an Existing Access Control Policy, NAT or RAVPN Policy on FMC.

Yes No

Save Cancel

دوجوملا نيوكتلا رايلع اغل

يف حضورم وه امك اهليحرت م تيس يتلا تازيمل ديحتل تارايلع كانه نوكيس، كلذ دعب ةعباتم على رقنا. ةروصللا



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

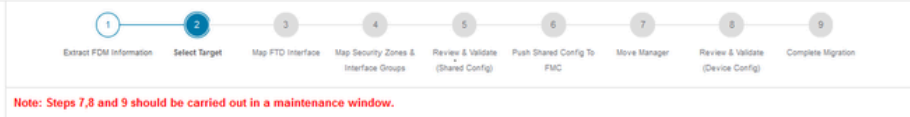
Proceed

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

اهد دخت متيس تال تازي مالا

لي وحتال ادبا مالا

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

لي وحتال ادب

ةعبات مودنتس مالا ليزنت: نيزرايخ مادختسا نكمي، لي وحتال اةي لمع يهتنت نا درجمب
يلال قوف رقنللا قيرط نع لي وحتال

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

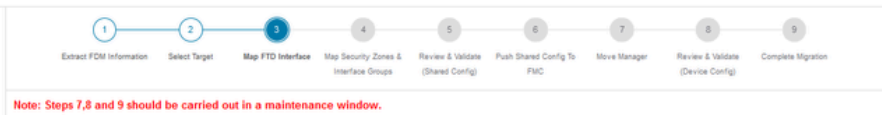
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPN/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)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

Back

Next

ريقرت ل ليزنت

ثي دحت قوف رقنللا نسحت سمللا نم، ةسرامم لصفأك. اهضرع متيل زاهجلا تاهجاو نييعت مت
يلالاتلا قوف رقنلاب ةعباتملا كنكمي، ةحصللا نم ققحتلا درجم. تاهجاو لثي دحتل



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

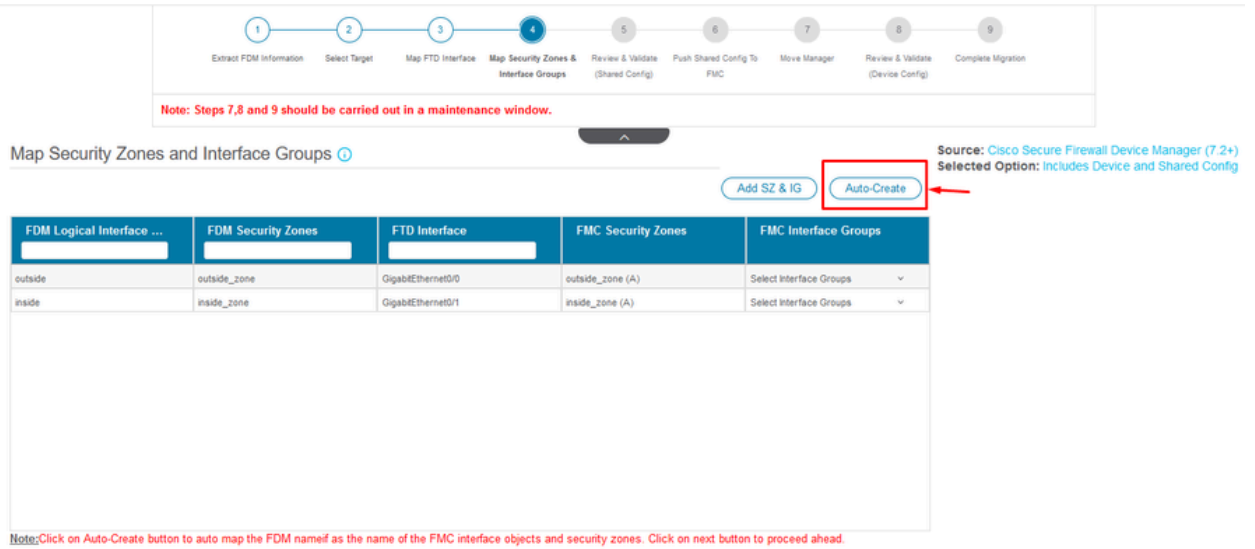
Next

ةضورعمل تاهجاو ل

مادختساب ايودي ةفاضلا ل لجاتحت ثيح، ةهجاو ل تاعومجمو نامأل قطانم مسق ل لقتنا
تاهجاو ل ءاشن ل ل دعاسي اذهو. يئاق ل لتلا ءاشن ل ل رايخ ل مت، لاثملا اذهل. SZ و IG ةفاضل

اهل لي حرت لابل موقت يتي ال (FMC) ةيساس ال ةحول ال ةراد ا في مكحت ال ةدحو ل خاد ائ اقل ت
يل ال رزل ال عل رقنا، ةاهت ال اءب

Firewall Migration Tool (Version 6.0.1)



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

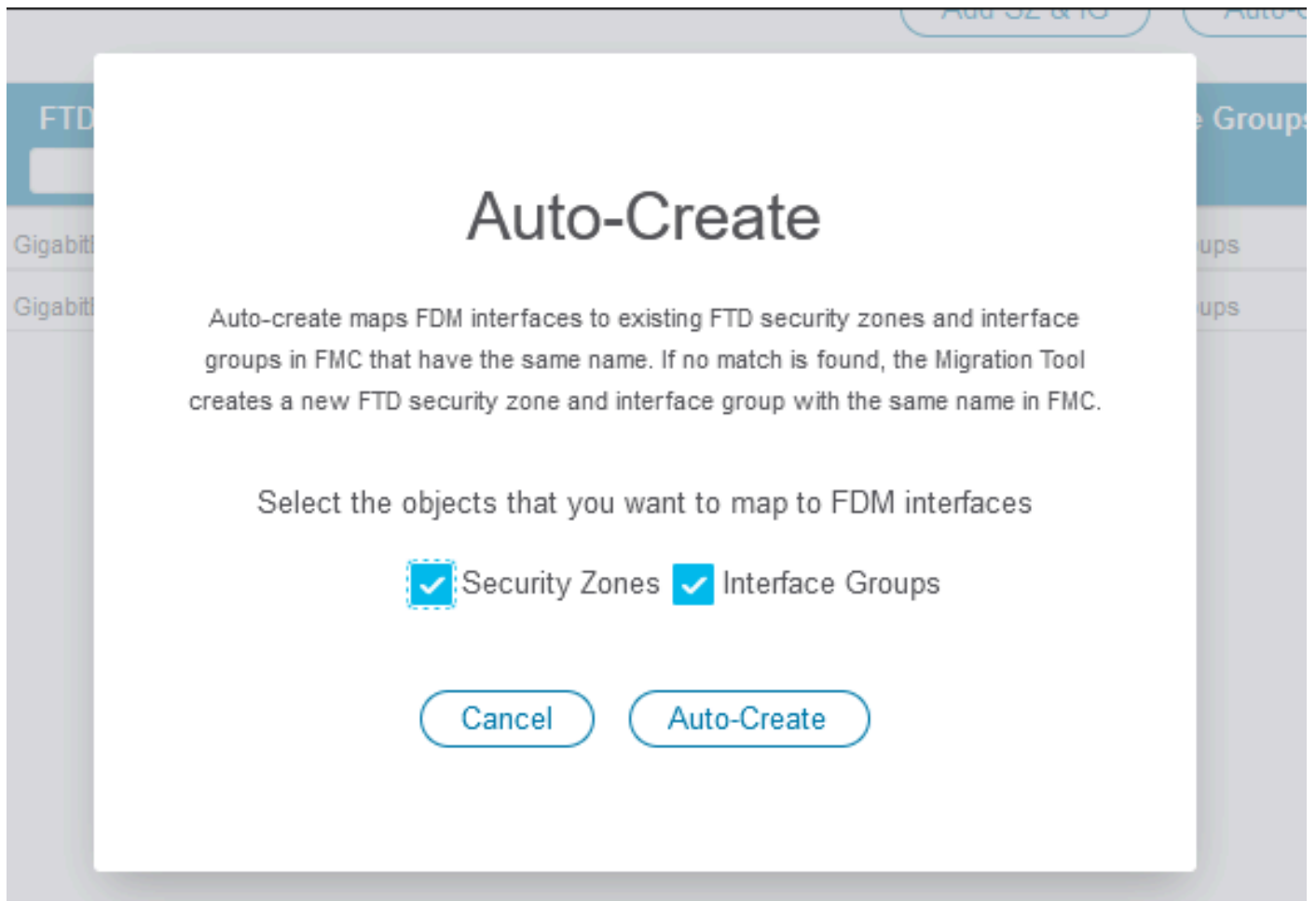
Source: Cisco Secure Firewall Device Manager (7.2+)
Selected Option: Includes Device and Shared Config

FDM Logical Interface ...	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	Select Interface Groups
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups

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

ةه اوال اءومءم ونام ال قءانم

ءاعومءم وءءوم ال FTD نام ا قءانم ال FDM اءءاو نئي عء ال ع ائ اقل ال ةاشن ال اءومءم ونام ال قءانم
مءس ال سفن اهل يتي ال FMC في اءء اوال



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

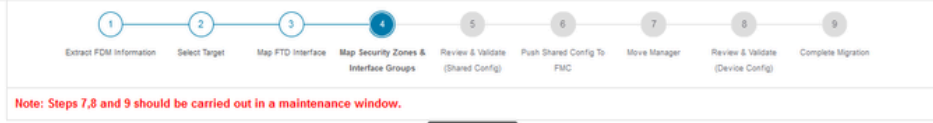
Security Zones Interface Groups

Cancel Auto-Create

يئاقلتل ءاشنإلإ راڤخ

ڤلالتل ددح مٲ

Firewall Migration Tool (Version 6.0.1)



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.

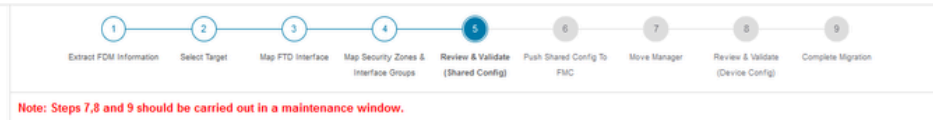
10 DEF.P938 2 Page 1 of 1

Back Next

يئاقلتل ءاشنإلإ راڤخ دعب

تاساڤس صرءفل ڤفالكلا تقولا صصرء، ڤولعل طرءشلا ڤف ءضوم وه امك، 5 ءوطءلا ڤف ءڤانعب رصنع لك ءعءارم قڤرط نع عبات nat ءعاوقو تانءالكلاو (ACP) لوصول ڤف مكءءلا تانڤوكءلا وأ ءامسألا ڤف لكاشم ءوءوم ءڤكأءل ءءاصل نم ققءءلا قوف رقنا مٲ

Firewall Migration Tool (Version 6.0.1)



Optimize, Review and Validate Shared Configuration Only

Source: Cisco Secure Firewall Device Manager (7.2+)

Selected Migration: Includes Device and Shared Config

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN SNMP DHCP

Access List Objects Network Objects Port Objects Access Control Policy Objects VPN Objects Dynamic-Route Objects

Select all 3 entries Selected: 0/3 Actions Save

Search

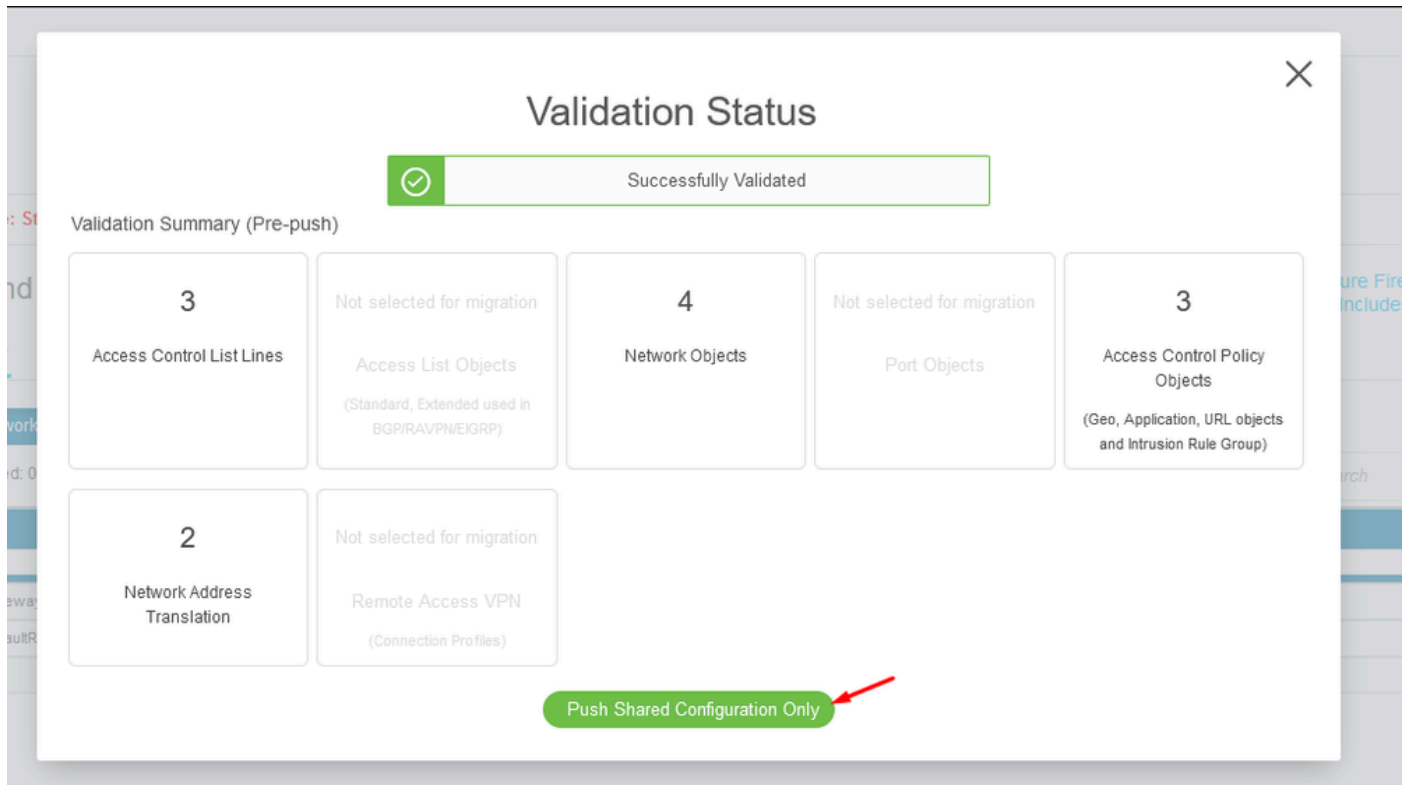
#	Name	Validation State	Type	Value
1	OutsidePv4Gateway	Validation pending	Network Object	172.16.1.1
2	OutsidePv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
3	Banned	Validation pending	Network Object	103.104.73.155

Page 1 to 3 of 3 Page 1 of 1

Validate

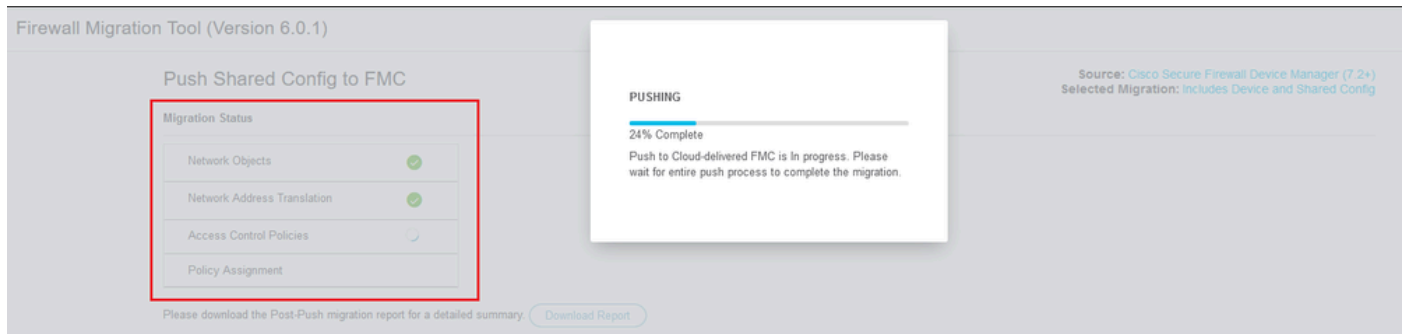
NAT تانويكوتو تانئالكلا، لوصولو في مكحتلا

طقف كرتشملا نيوكتلا لىل ع طغضا مث



طقف كرتشملا نيوكتلا ع ف د

اهي لىل ع لم ع ل ي رجي ي ت ل ا د د ح م ل ا م ه ل ا و ز ا ج ا ل ل ا ة ي و ئ م ل ا ة ب س ن ل ا ة ط ح ا ل م ن ك م ي و .



ع ف د ل ل ا ة ي و ئ م ل ا ة ب س ن ل ا

ث د ح ي ث ي ح ، ي و ل ع ل ا ط ي ر ش ل ا ي ف ض و ر ع م و ه ا م ك ، 6 ة و ط خ ل ا ل ا ل ق ت ن ا ، 5 ة و ط خ ل ا ل ا م ت ك ا د ع ب م د ق ت ل ل ي ل ا ت ل ا ر ز ل ا د د ح ، ك ل ذ د ن ع . FMC لىل كرتشملا نيوكتلا ع ف د



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, RAVNEGRP)	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, EIGRP)	Not selected for migration DHCP (Server, Relay, DDNS)

Next

FMC ىلى كرت شرمال نيوكتال عفد لامتك

ريدمال ليحرت عباتم ىلى يدؤي امم ،ديكأت ةلاس رليغشت ىلى راخال اذه يدؤي.

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.

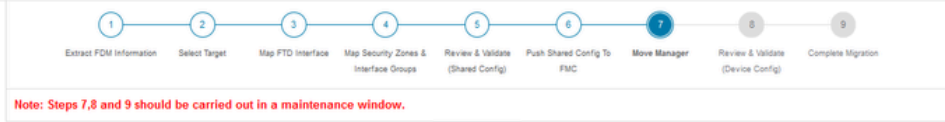
- Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.
 - FDM devices enrolled with the cloud management will lose access upon registration with FMC.
 - Ensure out-of-band access to the FTD device is available during migration.
 - It is highly recommended that 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

لقننلا قراد ديكأت

نكمي. يساسأ رمأ وهو، NAT فرعمو قرادإال زكرم فرعم رفوت ريديملا ليحرتة عباتم بلطتتة ذفانة ئيهتبا عارجإال اذه موقوي. ثيديحتلا ليصافات ديحتلالخ نم تا فرعملا هذه دادرستإظ فحبا ك لذ عبتي، cdFMC ل نمض FDM ليثمتل بوغرملا مسالا لاخدا متي شيح ققثب نم تاريخيغتللا.



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

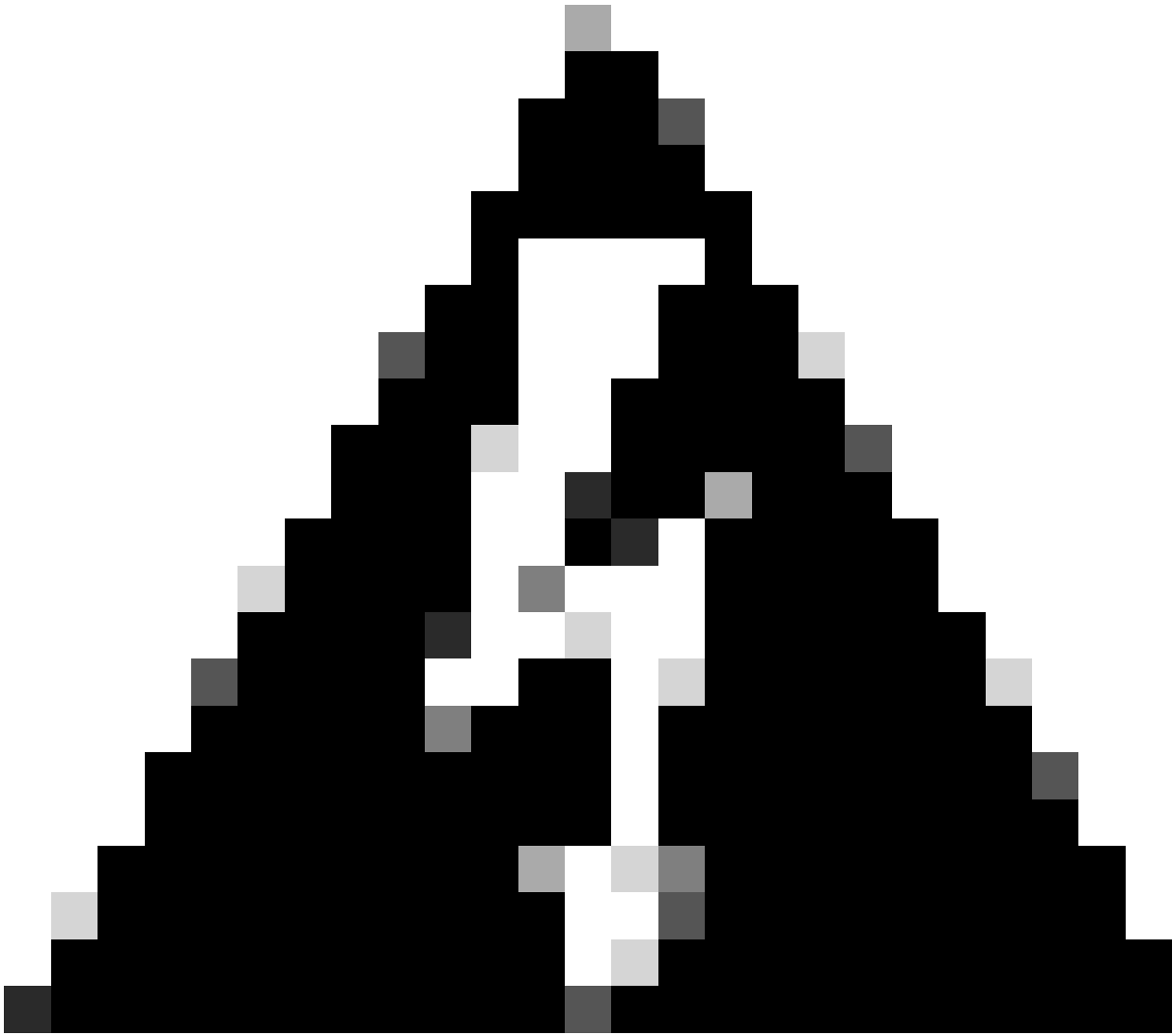
Save

Move Manager

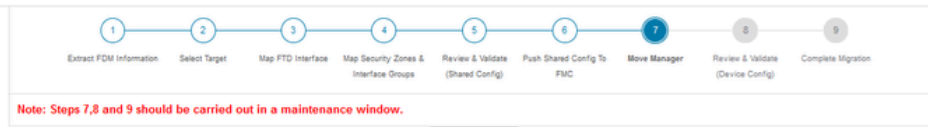
NAT فرع وة اذال زكرم فرع

ليجس ل زاهال مس ا ثي دت

ة. روك ذم ل لوقح ل ا فرع م ضرع م تي، ارحال اذه دعب



نوكي، يضارتفا لكش ب. ةرادإلا زكرم ةهجاو ىلع تارييغت يآ ءارجاب مقت ال :ريذحت
يضارتفا دادعإك راىخلا اذه كرتأ ،اددحم ةرادإلا راىخ



Move Manager

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

Update Details

This step is mandatory and should be performed during a downtime window. After you register the device with the management center or Cloud-delivered FMC, you can no longer use the device manager to manage it.

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco	us.cdo... ego	856GW 104v	26PM	fdm-Azure	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management Select Data interface

[Save](#)

[Move Manager](#)

NAT فرع ومو ة رادال زكرم فرعم

هت نمازم ادبب موقيس يذلا زاهج ل، لى صافات ل ثي دحت راى خ راى تخ ا دعب

FDM زاهج ة نمازم

DHCP تادادع و تاراسم ل و تاهج اول ص ح ف ي ة ي ل ال ة و ط خ ل ل ث م ت ، لى ح ر ت ل اء اء ن ا دعب ة ح ص ل ل ن م ق ق ح ت ل ا د ي د ح ت ل ل خ ن م (FDM) ل و ح م ل ا ن ا ي ب ة د ع ا ق ة ر ا د ا ي ف ا ه ن ي و ك ت م ت ي ت ل ل



Optimize, Review and Validate Device Configuration Page

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

Access Control Objects NAT Interfaces Routes Site-to-Site VPN Tunnels Remote Access VPN SNMP DHCP

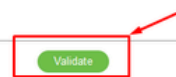
Static PPPoE

Select all 2 entries Selected: 0 / 2

Search

#	Interface	Zone	IP Address	State
1	GigabitEthernet0/0	outside_zone		Enabled
2	GigabitEthernet0/1	inside_zone	10.1.1.1	Enabled

Page 1 to 2 of 2 Page 1 of 1



FDM نيوكت تادادع| ةحص نم ققحتال

مرستستس يتلاو، نيوكتال عفد ةيلمع ادبل نيوكتال عفد رتخأ، ةحصلال نم ققحتال دعب م تي يتلا ماهمال ةبقارم نكمملا نم، كلذىل ةفاضلإاب. ليحرتال ةيلمع يهتنت ىتح اهذيفنت.

Validation Status

✔ Successfully Validated

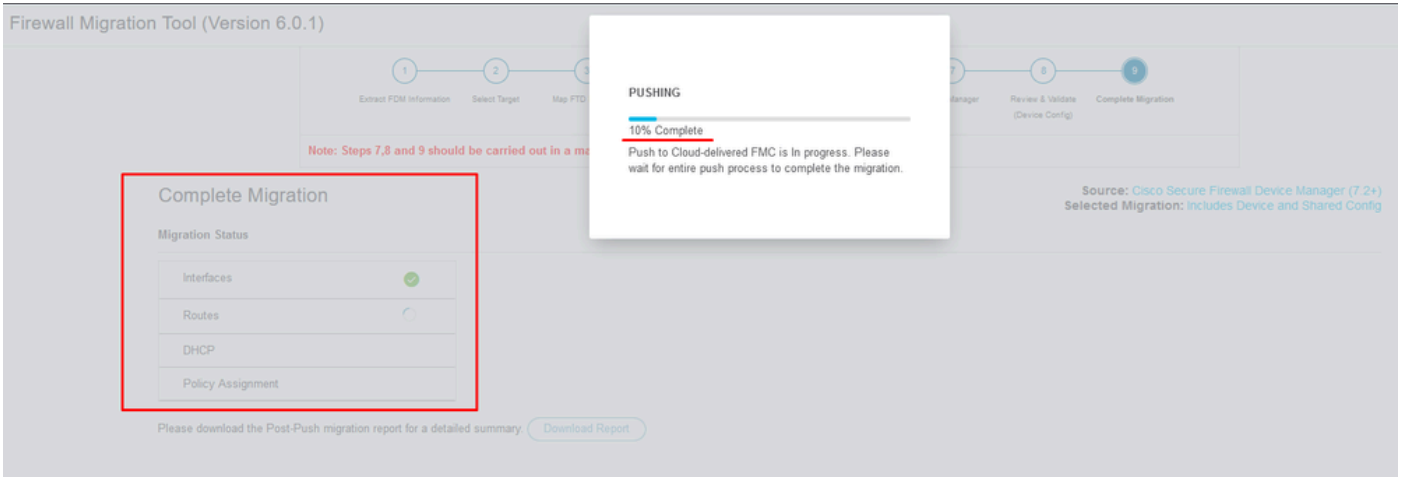
Validation Summary (Pre-push)

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

Push Configuration

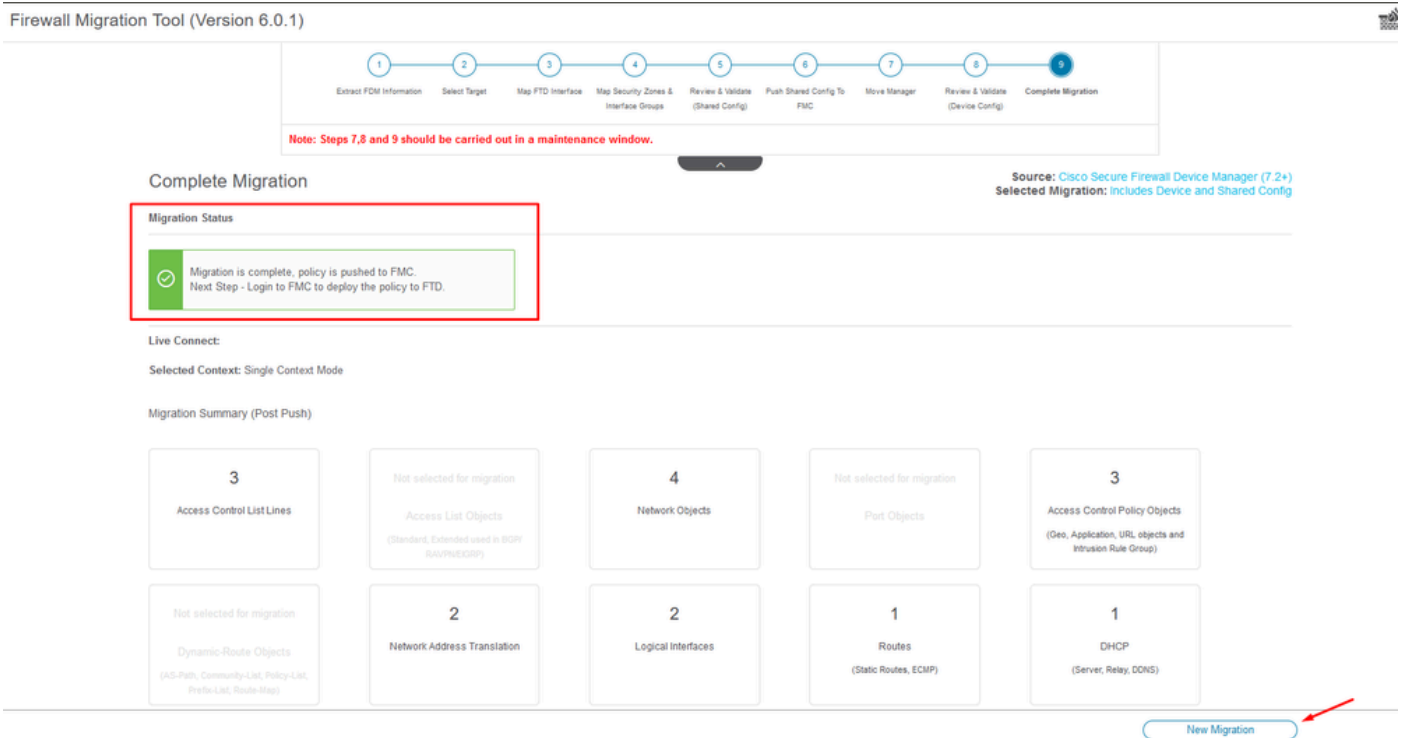
ع. فدل نيوكت - ةحصلال نم ققحتال ةلاح.

ةيوئمال ةبس نال عفد نيوكتب ققحتب نم راطإ.



ةلمتكم ال ع ف د ل ال ل ة ي و ة م ال ة بس ن ال

ة ي ل م ع ة ي ا ن ي ل ع ر ش و ي ا م ب ، ة د ي د ج ل ي ح ر ت ة ي ل م ع ا د ب ر ا ي خ م د ق ي ، ك ل ذ ن م ا ه ا ت ن ال د ن ع و ة ج م د م ال ا ت ا ف ل م ال ة ر ا د ا ة د و ي ال ف d m ة ر ا د ا ن م ل ي ح ر ت ال

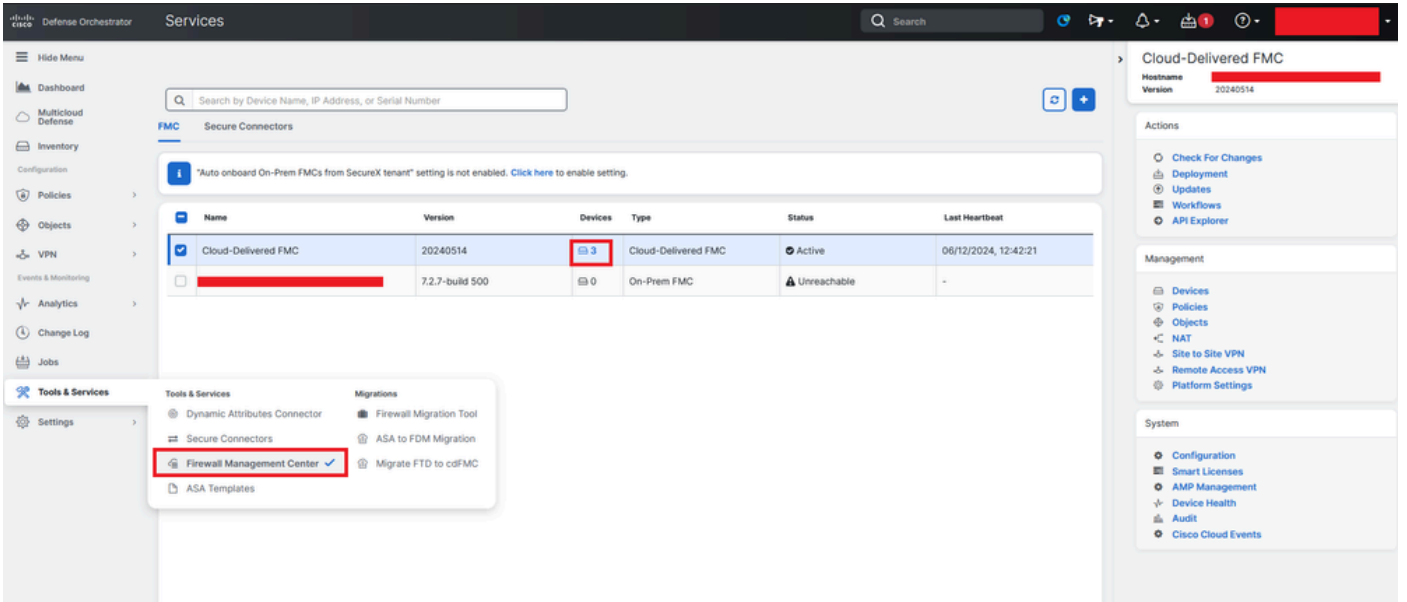


ل م ا ك ال ل ي ح ر ت ال

ة ح ص ال ن م ق ق ح ت ال

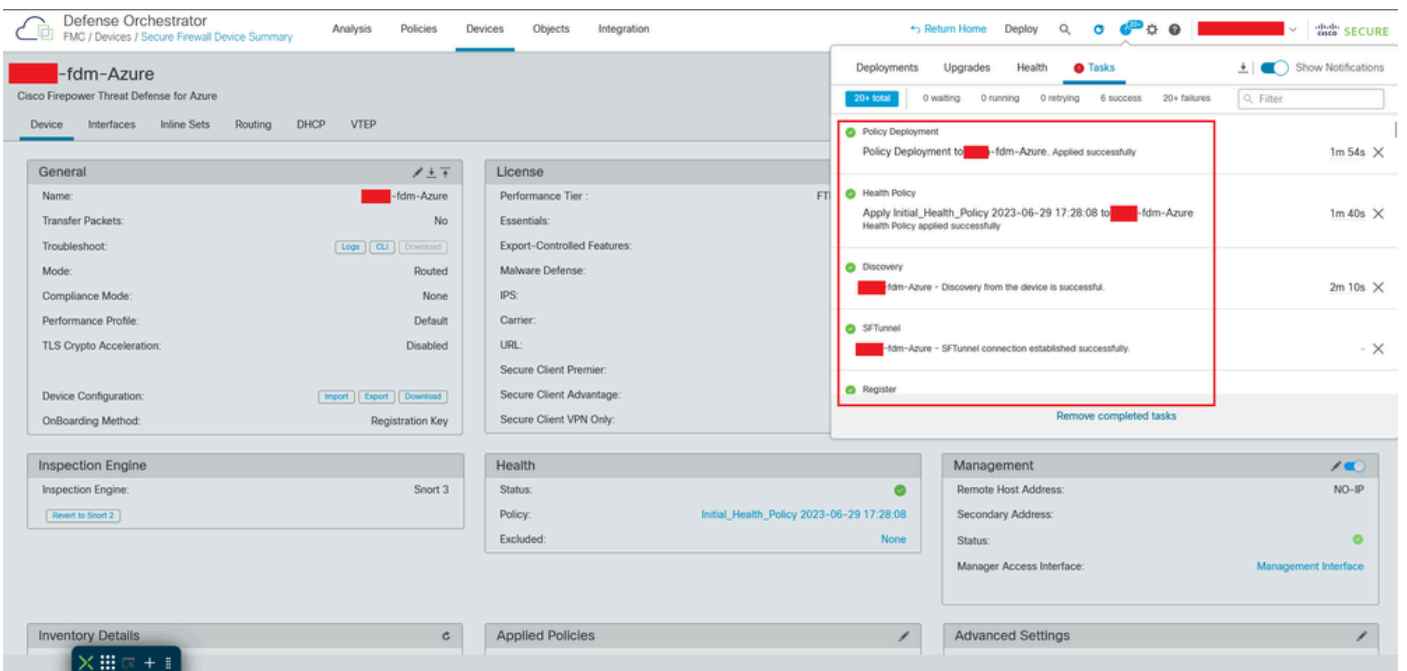
ل م ا ك ال ل ي ح ر ت ال ف D M ة ر ا د ا ن م ل ي ح ر ت ال c d F M C .

ة ل ج س م ال ة ز ه ا ل ا د د ع ن ا د ج ت ، ك ا ن ه . F i r e P O W E R . ة ر ا د ا ز ك ر م > ا م د خ ل ا و ا و د ا ل > C D O ي ل ل ق ت ن ا د ا ز د ق .



cdFMC في لاجسم الازجألا

ماهم نمض، روثعلا كنكمي، كلذلى لافاضالابو. ةزجألا ةرادا > ةزجألا نمض زاوجل نم ققحت متوحاجنبا زاوجل ليجست هي في مت يذلا تقولا لىع، (FMC) لكهال ةرادا في مكحتلا ةدحو حاجنبا لىلوالا رشنلا ةيلمع لامك



CDfmc في ليجستلا ةمه تلمتكا

ةزجألا ةرادا > زاوجل > cdFMC لىع زاوجل دجو

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

cdFMC لي لعسالم زاهل

لوصولو ل ف م ك ح ت ل > تاسايسال بحومب هلي حرت م ت ي ذللا لوصولو ل ف م ك ح ت ل جهن

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

ة رجهل ةسايس

لكشب اهلي حرت م ت ي ت لا و FDM في اهواشنن م ت ي ت لا تانئالكلا ةع جارم كنك مي ، لشم لا بو لى CDfmc لى ححص

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	

للى CDfmc لى FDM م اهلي حرت م ت ي ت لا تانئالكلا

تاتانئالكلا ةرادا تاهوا لى حرت م ت

Defense Orchestrator
FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration

Return Home Deploy Filter

Interface

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

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

نئال ءرادا تاهاوا لىحر ت

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامةرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل