

# CDO 내에서 FMT를 사용하여 FDM을 cdFMC로 마이그레이션

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[배경 정보](#)

[구성](#)

[다음을 확인합니다.](#)

---

## 소개

이 문서에서는 CDO의 FMT(Firepower 마이그레이션 도구)를 사용하여 FDM(Firepower 장치 관리자)을 cdFMC(클라우드 제공 FMC)로 마이그레이션하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

- Firepower 장치 관리자(FDM) 7.2+
- 클라우드 제공 방화벽 관리 센터(cdFMC)
- CDO에 포함된 FMT(firepower 마이그레이션 도구)

### 사용되는 구성 요소

이 문서는 앞서 언급한 요구 사항을 바탕으로 작성되었습니다.

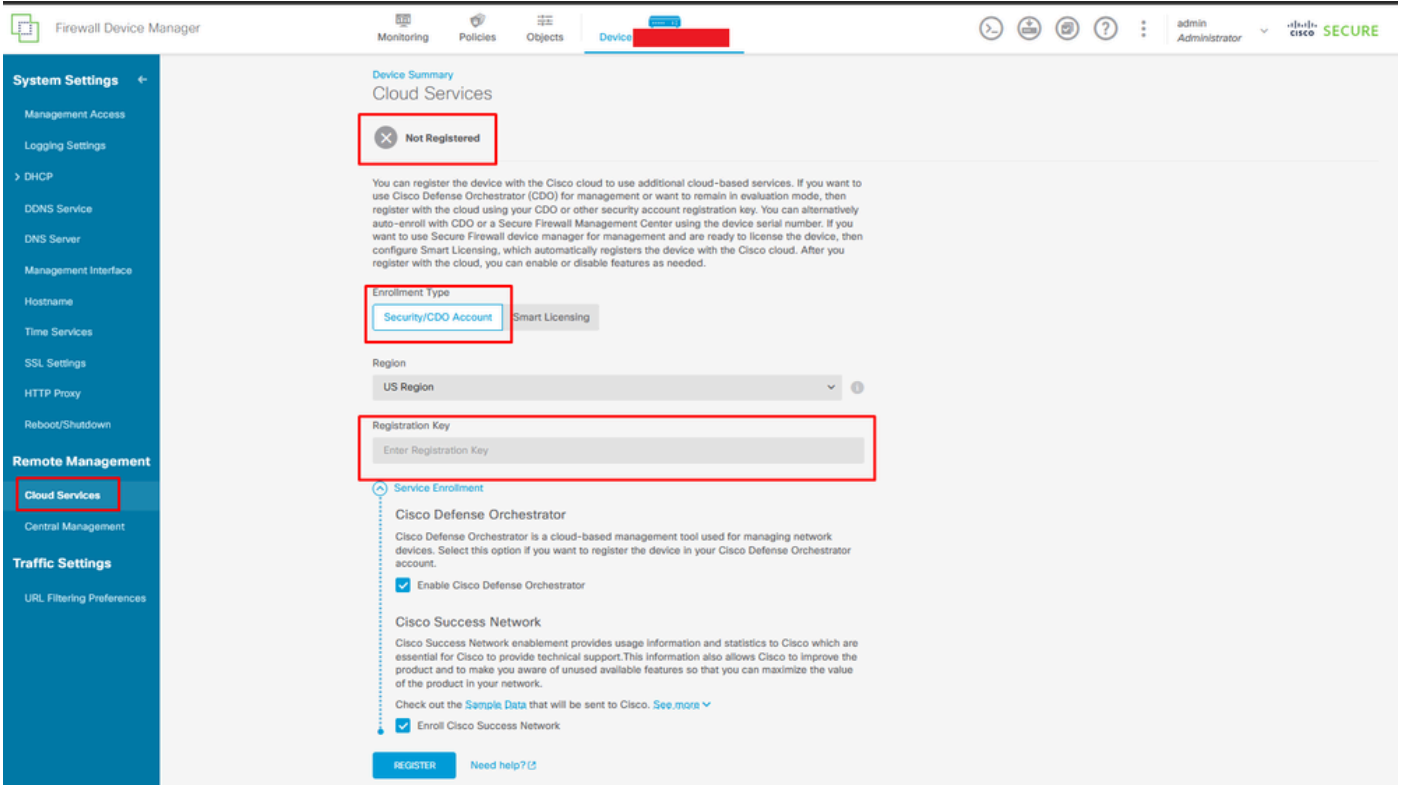
- 버전 7.4.1의 FDM(firepower 장치 관리자)
- 클라우드 제공 방화벽 관리 센터(cdFMC)
- CDO(Cloud Defence Orchestrator)

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 배경 정보

CDO 관리자 사용자는 디바이스가 버전 7.2 이상인 경우 디바이스를 cdFMC로 마이그레이션할 수 있습니다. 이 문서에 설명된 마이그레이션에서 cdFMC는 CDO 테넌트에서 이미 활성화되어 있습니

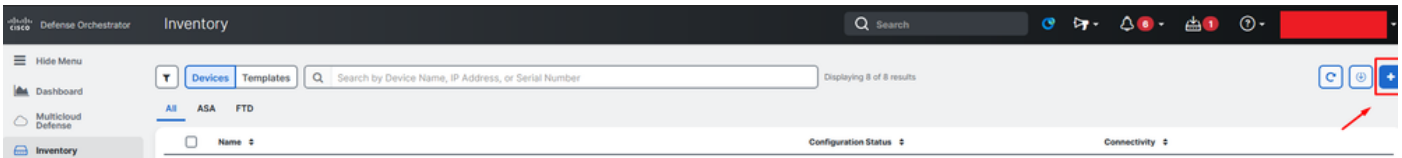




클라우드 서비스에 등록

등록 키는 CDO 내부에서 찾을 수 있습니다. CDO로 이동하고 Inventory(인벤토리) > Add symbol(기호 추가)로 이동합니다.

사용 중인 디바이스 유형을 선택하는 메뉴가 나타납니다. FTD 옵션을 선택합니다. FDM 옵션을 활성화해야 합니다. 그렇지 않으면 해당 마이그레이션을 수행할 수 없습니다. 등록 유형에서는 Use Registration Key를 사용합니다. 이 옵션에서는 3단계에 등록 키가 나타나며, 이를 복사하여 FDM에 붙여넣어야 합니다.



Onboard FDM, 추가 옵션

Select a Device or Service Type(디바이스 또는 서비스 유형 선택) 메뉴가 나타납니다.

## 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

장치 또는 서비스 유형 선택

이 문서에서는 Select Registration Key(등록 키 선택)를 선택했습니다.

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.

등록 유형

여기에는 이전 단계에서 필요한 등록 키가 표시됩니다.

**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**

등록 프로세스

등록 키를 가져온 후 FDM에 복사하여 붙여넣은 후 등록을 누릅니다. FDM을 Cloud Services 내에 등록하면 이미지에 표시된 것처럼 Enabled로 표시됩니다.

디바이스가 가동되어 실행되면 디바이스가 등록되므로 Smart 라이선스를 건너뛰었습니다.

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](#)

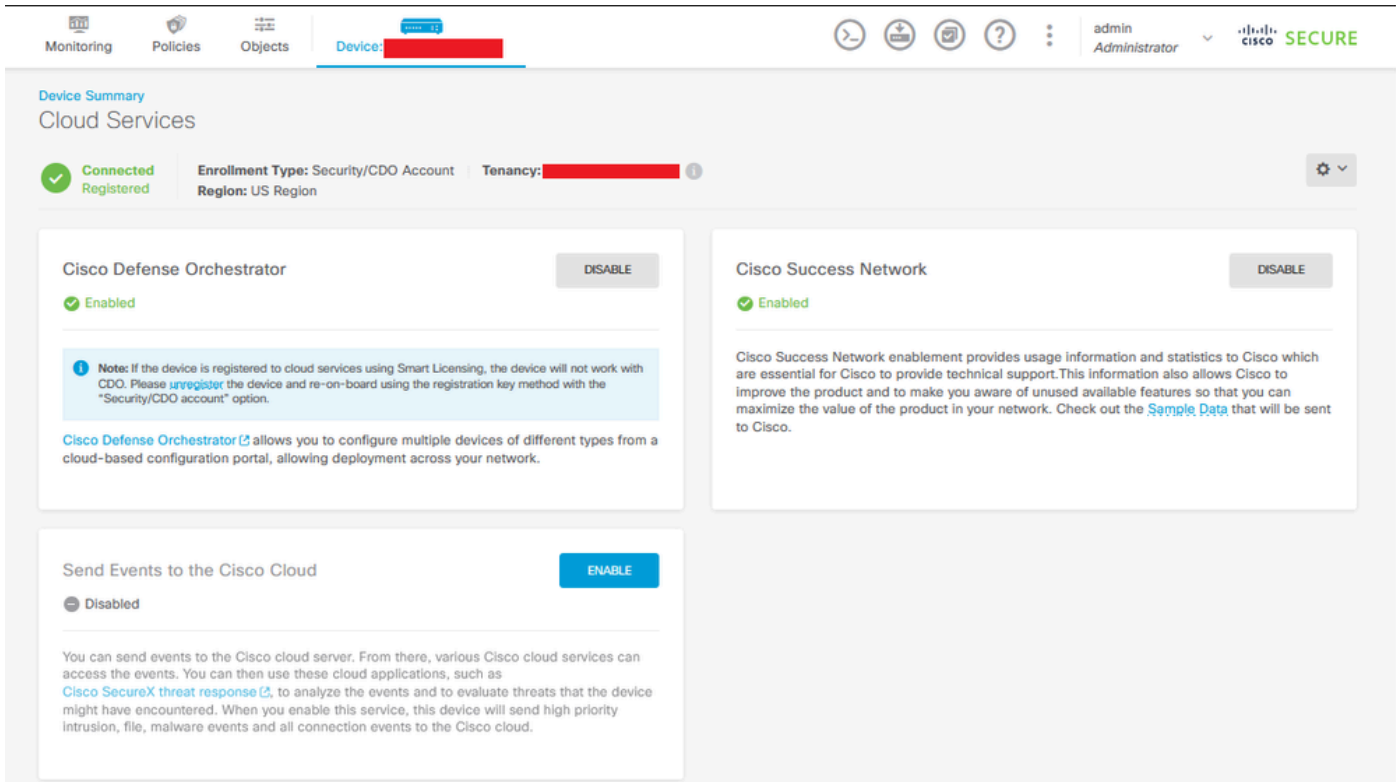
Enroll Cisco Success Network

REGISTER

[Need help?](#)

FDM 등록

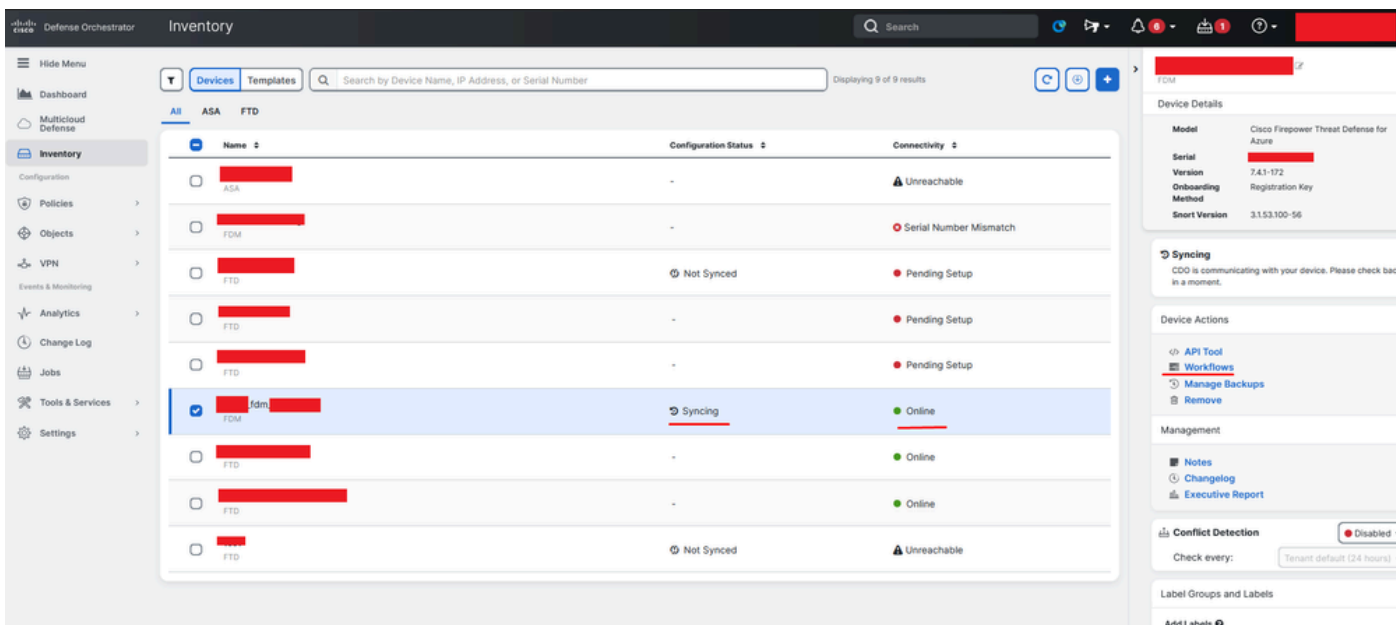
FDM을 등록하면 Tenancy, Cloud services connected 및 Registered가 표시됩니다.



FDM 등록 완료

CDO의 Inventory(인벤토리) 메뉴에서 FDM을 온보딩 및 동기화 과정에서 찾을 수 있습니다. 이 동기화의 진행률과 흐름은 Workflows(워크플로) 섹션에서 검토할 수 있습니다.

이 프로세스가 완료되면 동기화 및 온라인으로 표시됩니다.

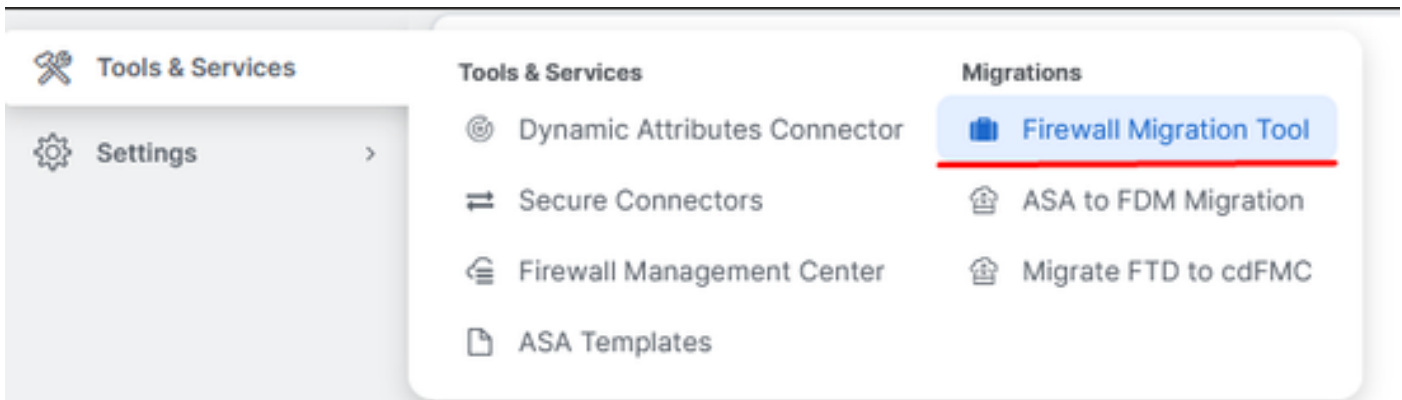


FDM 온보딩된 CDO 인벤토리

디바이스가 동기화되면 Online(온라인) 및 Synced(동기화됨)로 표시됩니다.



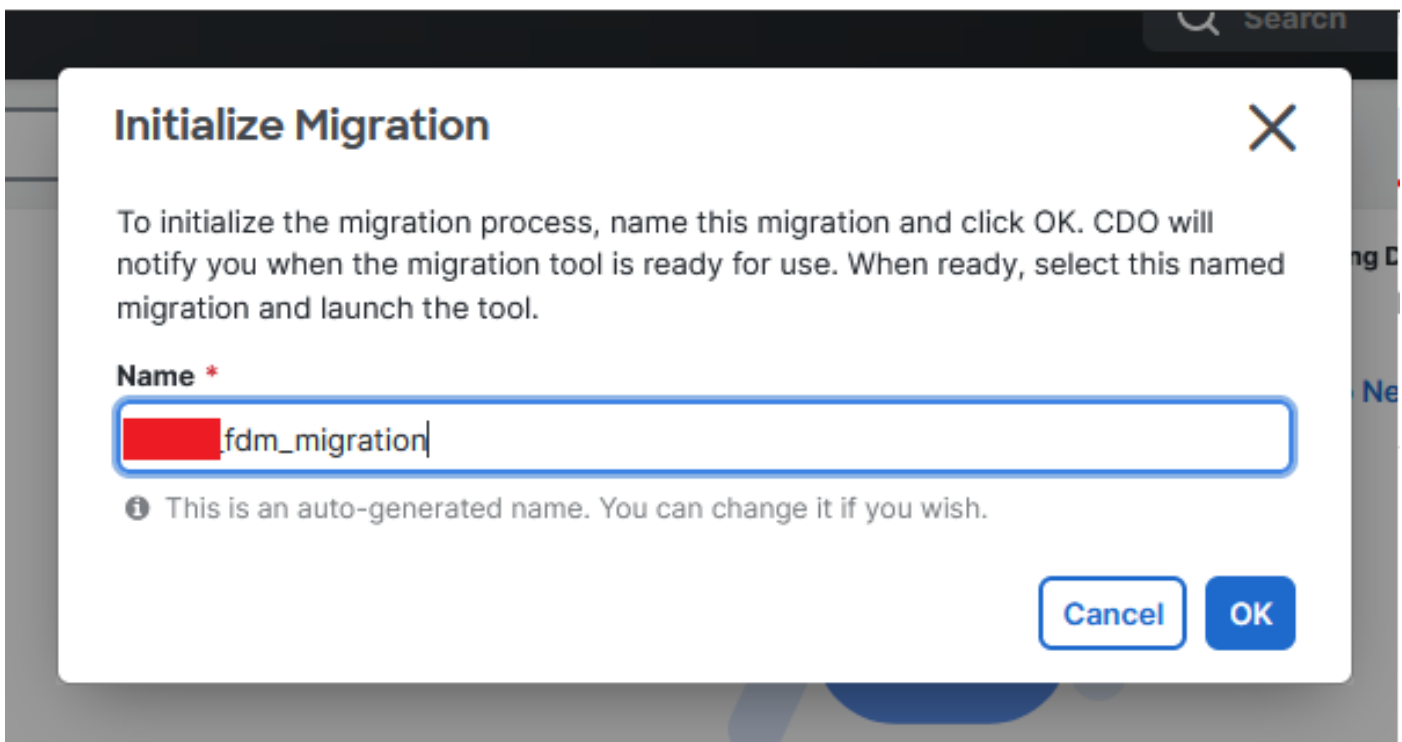
FDM이 CDO에 성공적으로 온보딩되면 FDM에서 로그아웃해야 합니다. FDM에서 로그아웃한 후 CDO 내에서 Tools & Services(툴 및 서비스) > Migration(마이그레이션) > Firewall Migration Tool(방화벽 마이그레이션 도구)로 이동합니다.



Add(추가) 기호를 클릭하면 임의의 이름이 나타나며, 이는 마이그레이션 프로세스를 시작하기 위해 이름을 변경해야 함을 나타냅니다.



이름을 바꾼 후 Launch(실행)를 클릭하여 마이그레이션을 시작합니다.



마이그레이션 초기화

Launch(실행)를 클릭하여 마이그레이션 컨피그레이션을 시작합니다.



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

마이그레이션 시작 프로세스

Launch(실행)를 클릭하면 마이그레이션 프로세스를 위한 창이 열립니다. 여기서 Cisco Secure Firewall Device Manager(7.2+) 옵션이 선택됩니다. 앞에서 설명한 대로 이 옵션은 버전 7.2부터 활성화됩니다.

## 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 소스 선택 컨피그레이션

선택하면 세 가지 마이그레이션 옵션이 표시됩니다. 공유 구성 전용, 장치 및 공유 구성 포함, 장치 및 공유 구성을 FTD 새 하드웨어에 포함.

이 경우 두 번째 옵션인 Migrate Firepower Device Manager(Migrate Device Manager)(Includes Device & Shared Configuration(디바이스 및 공유 컨피그레이션 포함)가 수행됩니다.

## 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 :**

마이그레이션 옵션

마이그레이션 방법을 선택한 후 제공된 목록에서 디바이스를 선택합니다.

### 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

fdm - Available

Connect

FDM 장치 선택

FDM device config extraction successful

100% Complete

구성 추출 완료

맨 위에 있는 탭을 열어 디바이스를 선택한 시점의 단계를 검토하고 이해하는 것이 좋습니다.



### 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:

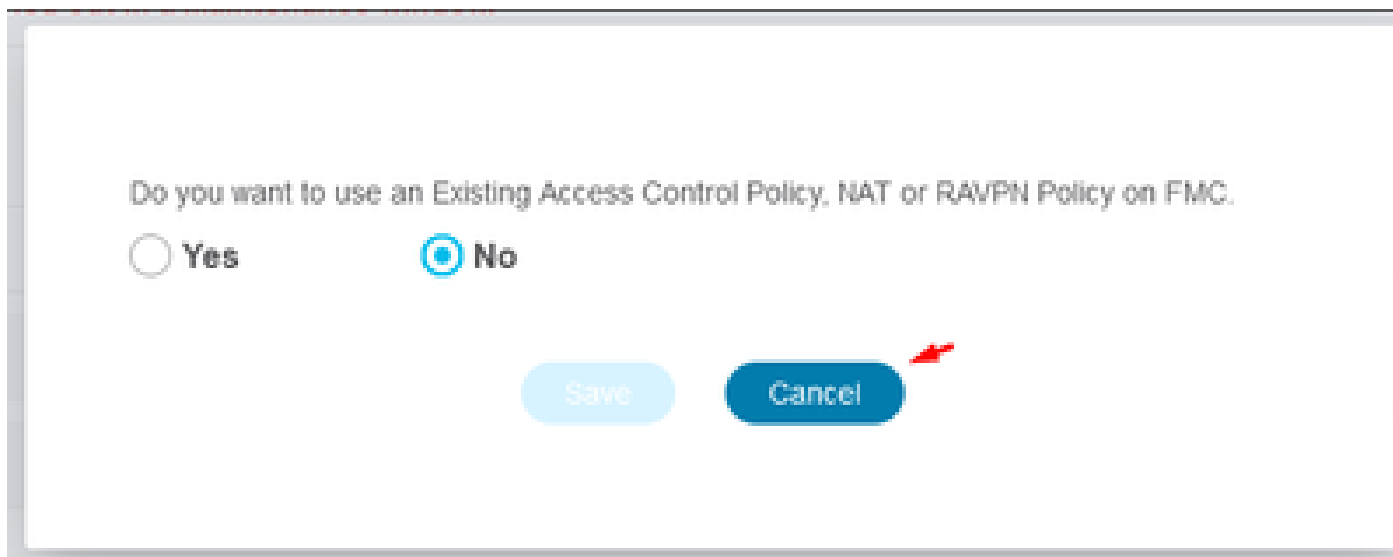
Parsed Summary

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

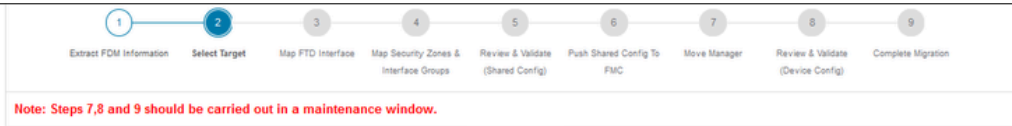
### 마이그레이션 프로세스 단계

새 마이그레이션인 경우 "FMC에서 기존 액세스 제어 정책, NAT 또는 RAVPN 정책을 사용하시겠습니까?" 옵션이 표시되면 Cancel(취소)을 선택합니다.



### 기존 구성에 대한 취소 옵션

그런 다음 이미지에 표시된 대로 마이그레이션할 피처를 선택하는 옵션이 있습니다. Proceed(진행)를 클릭합니다.



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

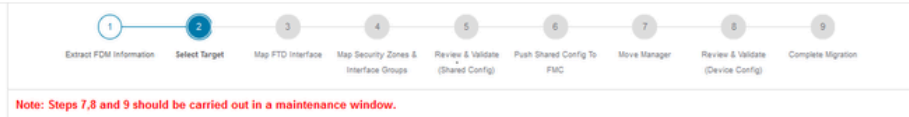
Proceed

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

선택할 기능

그런 다음 변환을 시작합니다.

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

변환을 시작합니다.

구문 분석 프로세스가 완료되면 문서를 다운로드하고 다음을 클릭하여 마이그레이션을 계속하는 두 가지 옵션을 사용할 수 있습니다.

## 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

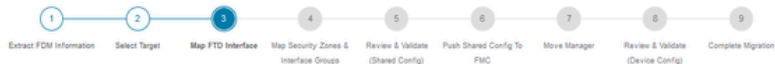
3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPI/EIGRP)	3 Network Objects	0 Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
0 Dynamic-Route Objects (AS-Path, Community-List, Policy-List, Prefix-List, Route-Map)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

보고서 다운로드.

디바이스 인터페이스가 표시되도록 설정됩니다. 모범 사례로서, Refresh를 클릭하여 인터페이스를 업데이트하는 것이 좋습니다. 검증이 완료되면 Next(다음)를 클릭하여 계속할 수 있습니다.



## 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

표시되는 인터페이스

Security Zones and Interface Groups(보안 영역 및 인터페이스 그룹) 섹션으로 이동합니다. 여기서 Add SZ & IG(SZ 및 IG 추가)를 사용하여 수동으로 추가해야 합니다. 이 예에서는 자동 생성이 선택

되었습니다. 이렇게 하면 마이그레이션할 FMC 내에서 인터페이스를 자동으로 생성할 수 있습니다. 작업을 마치면 Next(다음) 버튼을 클릭합니다.

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

보안 영역 및 인터페이스 그룹

[자동 생성] 옵션은 FDM 인터페이스를 동일한 이름을 가진 FMC의 기존 FTD 보안 영역 및 인터페이스 그룹에 매핑합니다.

## 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

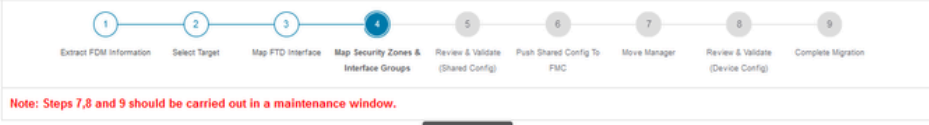
Security Zones  Interface Groups

Cancel Auto-Create

자동 생성 옵션.

그런 다음 다음을 선택합니다.

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.

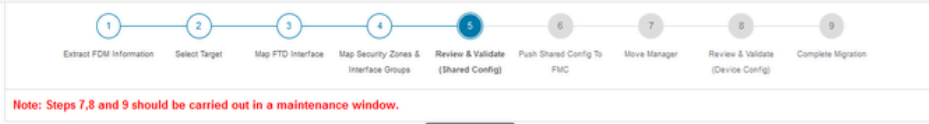
10 DEF.P93# 2 |< < Page 1 of 1 > >|

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

자동 생성 후 옵션

5단계에서는 위쪽 막대에 표시된 것처럼 시간을 두고 ACP(Access Control Policies), Objects 및 NAT 규칙을 검토합니다. 각 항목을 신중하게 검토한 다음 Validate(검증)를 클릭하여 이름 또는 구성에 문제가 없음을 확인합니다.

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](#) [Clear](#)

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

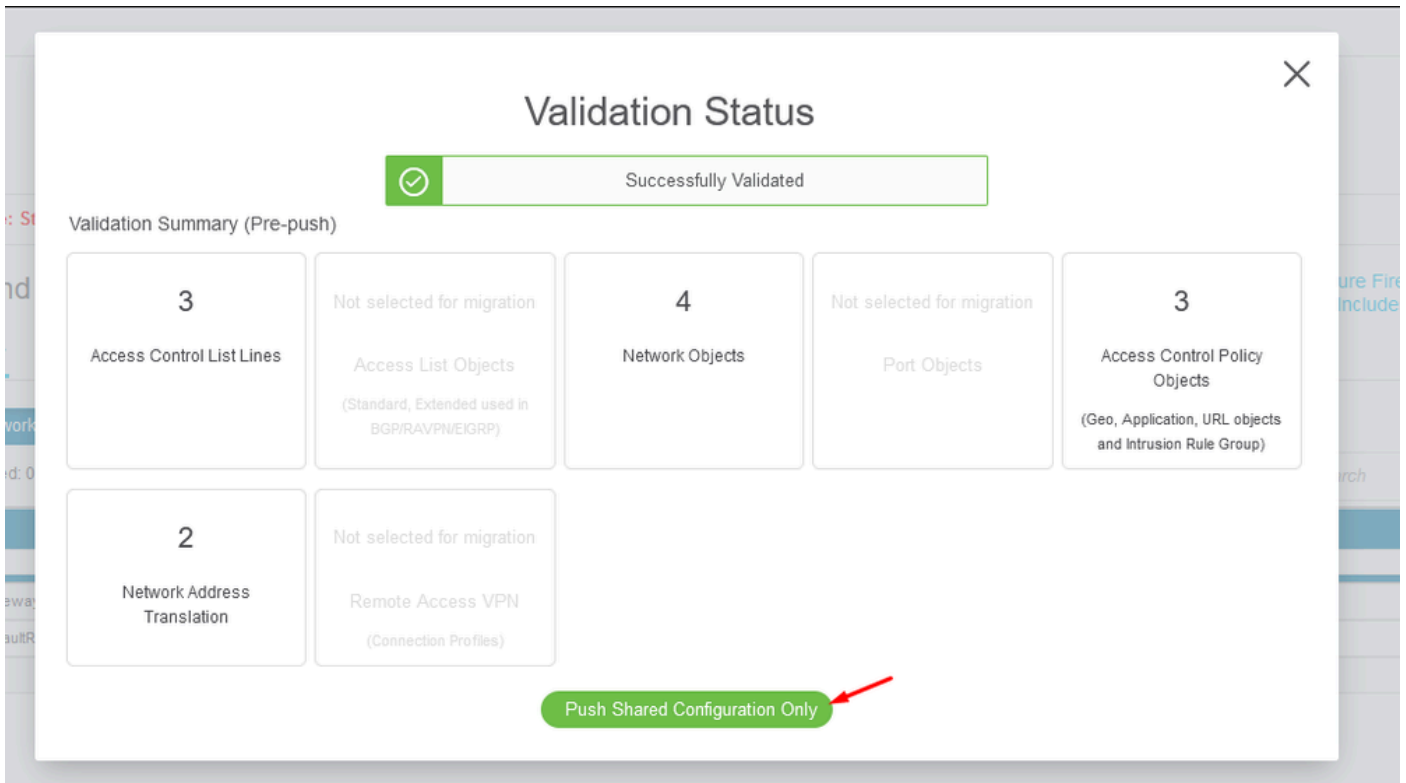
11 page 1 to 3 of 3 |< < Page 1 of 1 > >|

[Validate](#)



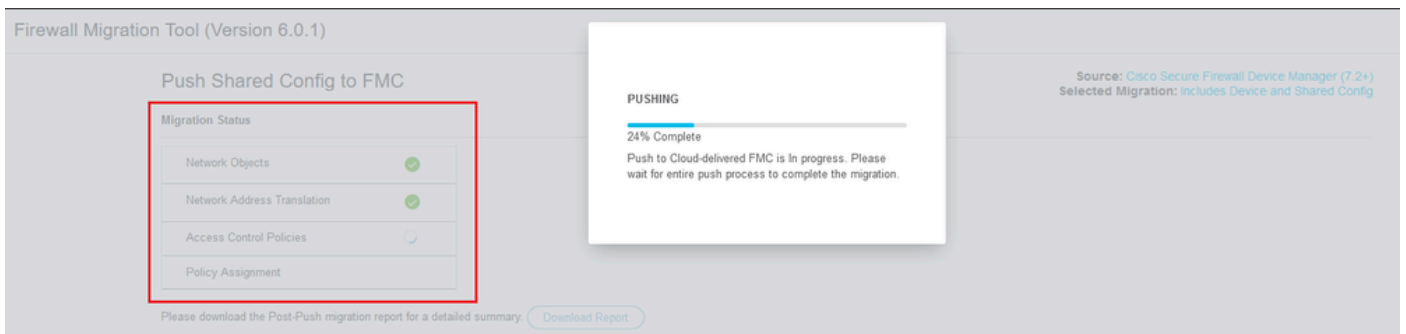
액세스 제어, 객체 및 NAT 컨피그레이션

그런 다음 공유 컨피그레이션만 푸시



공유 컨피그레이션만 푸시

완료율과 작업 중인 특정 작업을 관찰할 수 있습니다.



푸시 비율

5단계를 완료한 후 상단 표시줄에 표시된 대로 6단계로 진행합니다. 여기서 FMC로 공유 구성 밀어 넣기가 수행됩니다. 이때 다음 단추를 선택하여 진행합니다.



### Push Shared Config to FMC

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

#### Migration Status

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

#### Live Connect:

Selected Context: Single Context Mode

#### Migration Summary (Post Push)

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

Next

FMC에 공유 구성 밀어넣기 완료

이 옵션은 확인 메시지를 트리거하여 관리자 마이그레이션을 계속할지 묻습니다.

---

# 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.

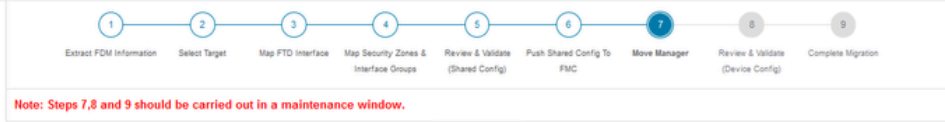
I acknowledge all the steps mentioned above have been completed.

Proceed

Cancel

관리자 이동 확인

관리자 마이그레이션을 진행하려면 Management Center ID 및 NAT ID가 있어야 하며, 이는 필수적입니다. 이러한 ID는 Update Details(업데이트 세부사항)를 선택하여 검색할 수 있습니다. 이 작업을 수행하면 cdFMC 내의 FDM 표현에 대해 원하는 이름을 입력한 다음 변경 사항을 저장하는 팝업 창이 시작됩니다.



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

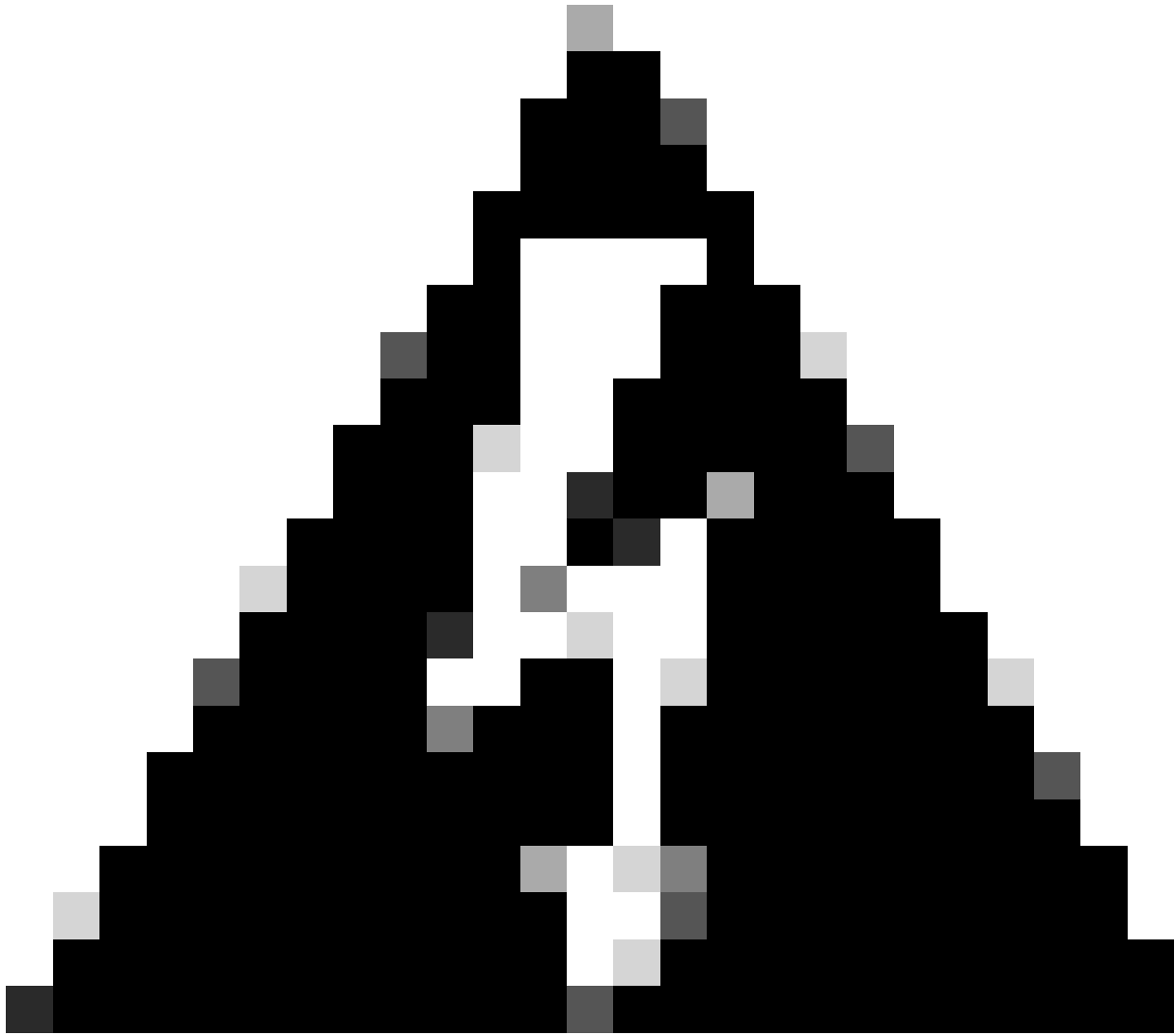
Save

Move Manager

관리자 센터 ID 및 NAT ID

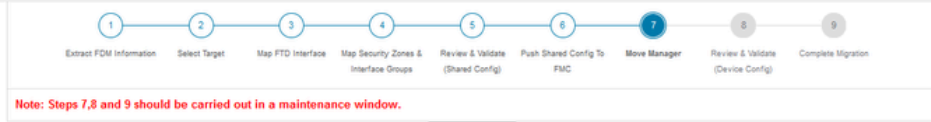
등록을 위해 디바이스 이름을 업데이트합니다.

이 작업 후에는 앞서 설명한 필드의 ID가 표시됩니다.



경고: Management Center 인터페이스를 변경하지 마십시오. 기본적으로 Management(관리) 옵션이 선택되어 있으며 이 옵션을 기본 설정으로 유지합니다.

---



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

Move Manager

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

**Update Details**

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

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco	us.cdo... ego	#56GW/ 104v 2aPMT	fdm-Azure	CiscoUmbrellaDNSServerGroup	<input checked="" type="radio"/> Data <input type="radio"/> Management	Select Data interface

Save

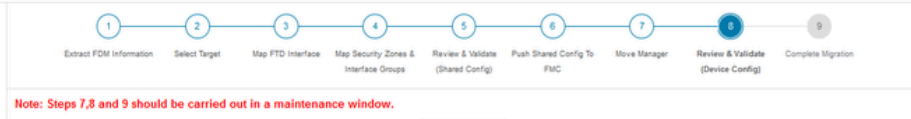
Move Manager

관리 센터 ID 및 NAT ID

Update Details 옵션을 선택한 후 동기화를 시작할 디바이스입니다.

FDM 장치 동기화

마이그레이션이 완료되면 다음 단계는 Validate(검증)를 선택하여 FDM에 구성된 인터페이스, 경로 및 DHCP 설정을 검토하는 것입니다.



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	15.1	Enabled

Page 1 to 2 of 2 Page 1 of 1



FDM 구성 설정 검증

검증 후 구성 밀어넣기를 선택하여 구성 밀어넣기 프로세스를 시작합니다. 이 작업은 마이그레이션이 완료될 때까지 계속됩니다. 추가로, 실행 중인 태스크들을 모니터링할 수 있다.

### Validation Status

✔ Successfully Validated

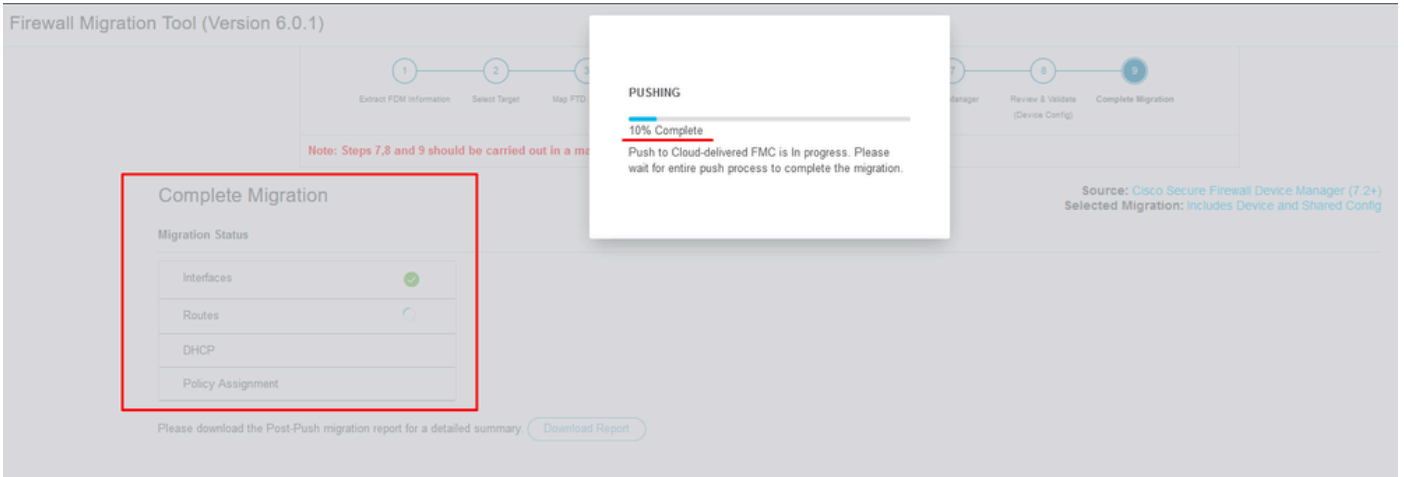
Validation Summary (Pre-push)

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

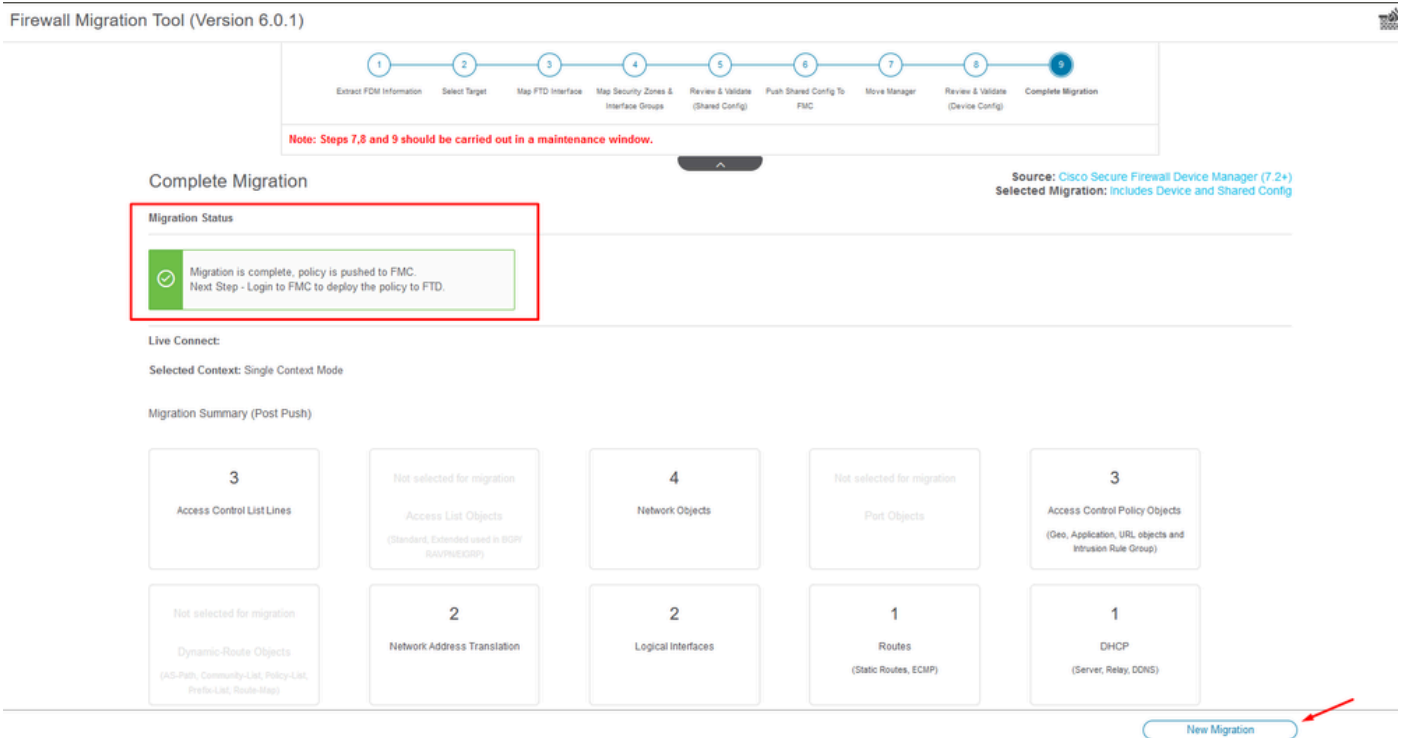
유효성 검사 상태 - 구성 밀어넣기

푸시 컨피그레이션의 백분율이 표시된 팝업 창



푸시 완료

완료되면 FDM에서 cdFMC로의 마이그레이션 프로세스의 종료를 표시하는 새 마이그레이션 시작 옵션이 표시됩니다.



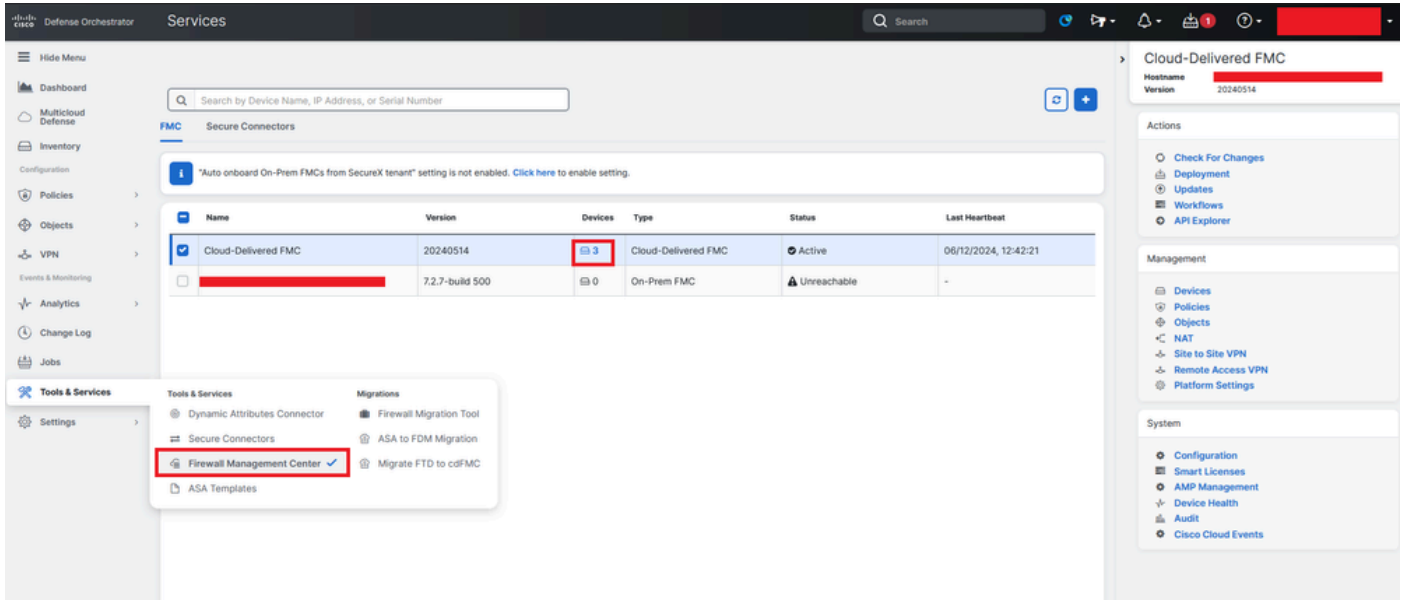
마이그레이션 완료

다음을 확인합니다.

FDM이 cdFMC로 성공적으로 마이그레이션되었는지 확인합니다.

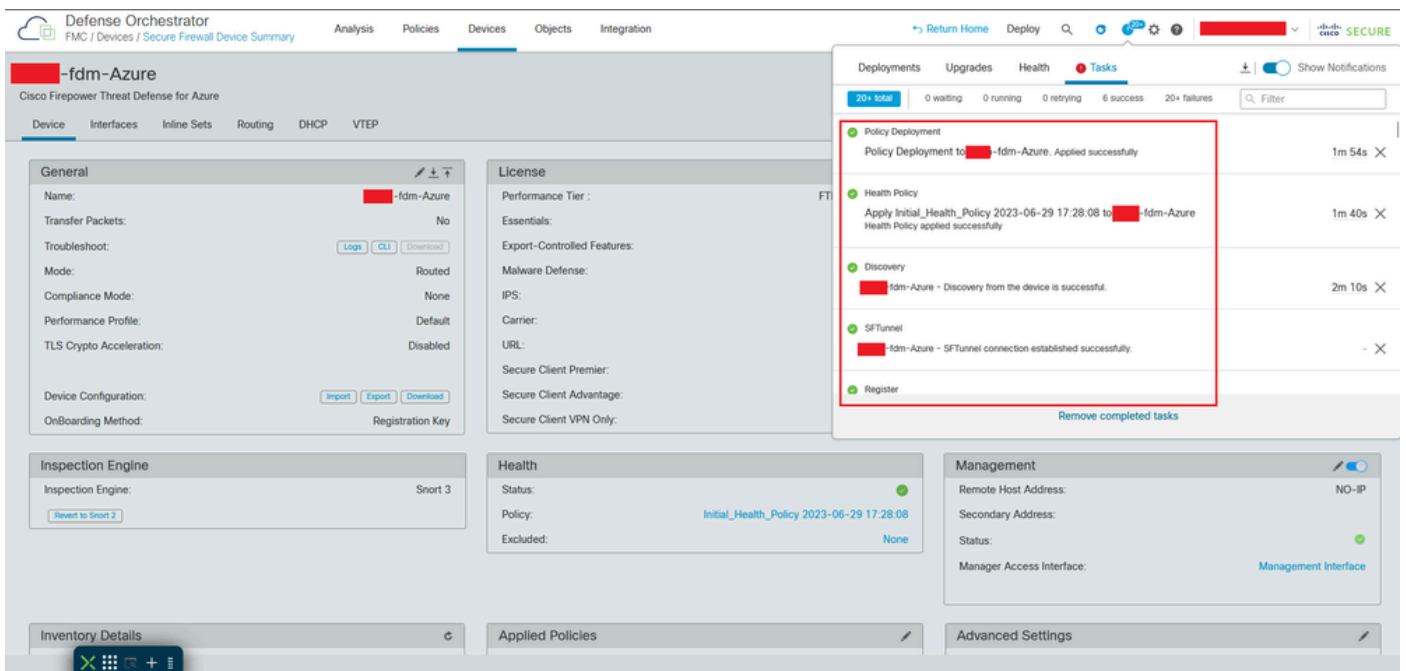
firepower CDO > Tools & Services > Monitoring Management Center로 이동합니다. 여기에서 등록된 디바이스 수가 증가했음을 확인할 수 있습니다.





cdFMC 등록된 디바이스

Devices(디바이스) > Device Management(디바이스 관리) 내에서 디바이스를 확인합니다. 또한 FMC의 작업 내에서 디바이스가 성공적으로 등록되고 첫 번째 구축이 성공적으로 완료된 시점을 찾을 수 있습니다.



cdFMC 등록 작업이 완료되었습니다.

디바이스가 cdFMC > Device > Device Management에 있습니다.

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

cdFMC에 등록된 디바이스

액세스 제어 정책은 Policies(정책) > Access Control(액세스 제어)에서 마이그레이션됩니다.

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

마이그레이션 정책

마찬가지로 FDM에서 생성된 객체를 검토하여 cdFMC로 올바르게 마이그레이션한 객체를 검토할 수 있습니다.

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

FDM에서 cdFMC로 마이그레이션된 객체

마이그레이션된 개체 관리 인터페이스입니다.

Defense Orchestrator  
FMC / Objects / Object Management

Analysis Policies Devices **Objects** Integration

Return Home Deploy Q Filter

SECURE

Interface

Add Filter

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

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

개체 관리 인터페이스가 마이그레이션되었습니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.