## CDO 내에서 FMT를 사용하여 FDM을 cdFMC로 마이그레이션

#### 목차

<u>소개</u>		
<u>사전 요구 사항</u>		
<u>요구 사항</u>		
<u>사용되는 구성 요소</u>		
<u>배경 정보</u>		
<u>구성</u>		
<u>다음을 확인합니다.</u>		

### 소개

이 문서에서는 CDO의 FMT(Firepower 마이그레이션 도구)를 사용하여 FDM(Firepower 장치 관리 자)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 디바 이스는 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

#### 다.

## 구성

1.- FDM에서 Cisco Cloud Services 활성화

마이그레이션을 시작하려면 보류 중인 배포가 없는 FDM 장치를 가지고 Cloud Services에 등록해 야 합니다. Cloud Services(클라우드 서비스)에 등록하려면 System Settings(시스템 설정) > See More(자세히) > Cloud Services(클라우드 서비스)로 이동합니다.

Cloud Services(클라우드 서비스) 섹션에서 디바이스가 등록되지 않았으므로 Security/CDO Account(보안/CDO 어카운트) 유형으로 등록을 수행해야 합니다. 등록 키를 구성한 다음 등록을 수 행해야 합니다.

	Device					Administrator	CURE
Model Cisco Firepower Thr	eat Defense for Azure	Software VDB 7.4.1-172 376.0	Intrusion Rule 20231011-15	Update Cloud Services 536 Sconnected   SEC TA	High Availab AC Not Configu	configure	
O/1       Internet         Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         0/0       0/1       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①       Image: Cisco Firepower Threat Defense for Azure ①         Image: Cisco Firepower Threat Defense for Azure ①<							
Interfaces	Routing			Updates		System Settings	
Management: Unmerged () Enabled 2 of 2	1 static rou	ite		Geolocation, Rule, VDB, Syste Security Intelligence Feeds	em Upgrade,	Management Access Logging Settings	
View All Interfaces	View Confi	iguration	>	View Configuration	> se	DHCP Server / Relay SL Settings loud Services	
Smart License Registered Tic:: FTDy20 - 3 Gbps	Backup	and Restore		Troubleshoot No files created yet	H <sup>1</sup> R Cu	TTP Proxy Server eboot/Shutdownt Interin 20 entral Management RL Filtering Preferences	
View Configuration	View Confi	iguration	>	REQUEST FILE TO BE CREATE	ED	See more	
Site-to-Site VPN There are no connections yet	Remote Requires Se No connect	Access VPN ecure Client License tions   1 Group Policy		Advanced Configuration	on Li	Device Administration Audit Events, Deployment History, Download Configuration	
View Configuration	Configure		>	View Configuration	>	View Configuration	>

클라우드 서비스 등록

Over Cloud Services(클라우드 서비스 이상)에는 등록되지 않은 것으로 표시됩니다. CDO 계정 등 록 유형을 선택하고 CDO의 등록 키를 제공합니다.

Firewall Device Manager	版 砂 苹王 Monitoring Policies Objects Device	S (a) (b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
System Settings +- Management Access Logging Settings	Device Summary Cloud Services Not Registered	
DHCP DDNS Service DNS Server Management Interface	You can register the device with the Clisco cloud to use additional cloud-based services. If you want to use Clisco Defense Orchestrator (CDO) for management or want to remain in evaluation mode, then register with the cloud using your CDO or other searchy account registration itsy, you can alternatively auto-enroll with CDO or a Secure Firewall Management Clearer using the device serial number, if you want to secure service and the classical security account are ready to learness the device, then cooperate service learned in the classical security account security account are device to learness the device, then cooperate visit the cloud, you can enable or disable features an ededd.	
Hostname Time Services SSL Settings	Enrollment Type Security/CDO Account Smart Licensing Region	
HTTP Proxy	US Region 🗸 🖉	
Reboot/Shutdown Remote Management	Registration Key Enter Registration Key	
Cloud Services Central Management	Service Enrolment     Cisco Defense Orchestrator     Cisco Defense Orchestrator     Cisco Defense Orchestrator is a cloud-based management tool used for managing network	
Traffic Settings	devices. Select this option if you want to register the device in your Cisco Defense Orchestrator account.	
	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 our the Sample Data that will be sent to Cisco. See more > profile Enrol Cisco Success Network Need help?(5)	

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 활 성화해야 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.

cisco Defense Orchestrator	Inventory	Q Search	ଓ ୨୫- ୦୦- ଲଣ ଡ	· ·
Hide Menu	Devices Terministes     O Search hu Device Name 10 Address or Sarial Number	Displaying B of B results.		
A Dashboard				
C Multicloud Defense	AI ASA FTD			
inventory	Name \$	Configuration Status 🗘	Connectivity \$	

Onboard FDM, 추가 옵션

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



장치 또는 서비스 유형 선택

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

Follow the steps below				Cancel
FTD 0000	A Important: This method of onb delivered Firewall Management Sy	oarding allows for local co-managem rstem, click the FTD button instead. I	nent of the firewall via FDM. To man Learn more 🖸	age your device with cloud-
Management Mode: O FTD O O FDM () (Recommended)	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 onlv)	Use Credentials (Basic) Onboard a device using its IP address, or host name, and a username and password.	
	Χ.			

#### 여기에는 이전 단계에서 필요한 등록 키가 표시됩니다.

FTI Firev Mana (Rec	wall Threat Defense agement Mode: FTD • • FDM • ommended)	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 C      Use Registration Key Onboard a device using a registration key generated from CDO and applied on the device using from the output of for onboarding configured devices using their serial number. (FTD 6.7+, 1000, 2100 and 3100 series only)
		series onivi
1	Device Name	
2 [	Database Updates	Enabled
3 (	Create Registration Key	7a53c
4 5	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 O 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 라이센스를 건너뛰었습니다.

Monitoring	Policies	Objects	Device: joroa-fdm-tech
Device Summ Cloud Se	ary ervices gistered		
You can regist use Cisco Def register with t auto-enroll wi want to use S configure Sma register with t	er the device v ense Orchestra he cloud using th CDO or a Se ecure Firewall art Licensing, v he cloud, you o	with the Cisco clo ator (CDO) for ma your CDO or oth ecure Firewall Ma device manager f vhich automatical can enable or dis	bud to use additional cloud-based services. If you want to anagement or want to remain in evaluation mode, then er security account registration key. You can alternatively anagement Center using the device serial number. If you for management and are ready to license the device, then lly registers the device with the Cisco cloud. After you able features as needed.
Enrollment Ty	pe DO Account	Smart Licensing	
Region US Region Registration K 7a53c2t	ey		~ 1
Service E Cisco E Cisco De devices. account.	nrollment Defense Orc fense Orchestr Select this opt	chestrator	ased management tool used for managing network
Cisco S Cisco Su essential product a of the pro Check ou Enro	Die Cisco Defer Success Network for Cisco to pr and to make yo oduct in your n at the Sample ( Il Cisco Succes	ion if you want to nse Orchestrator twork enablement prov ovide technical s u aware of unuse etwork. Data that will be s ss Network	vides usage information and statistics to Cisco which are upport. This information also allows Cisco to improve the ad available features so that you can maximize the value sent to Cisco. See.more V

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 동 기화의 진행률과 흐름은 Workflows(워크플로) 섹션에서 검토할 수 있습니다.

#### 이 프로세스가 완료되면 동기화 및 온라인으로 표시됩니다.

situdia casco Defense Orchestrator	Inventory		Q Search 😗 🎝 -	¢•• ≜• ⊙•
Hide Menu Dashboard	Devices Templates     Q Search by Device Name, IP Address, or Serial Number		Displaying 9 of 9 results	Pom 22
Multicloud     Defense     Inventory     Configuration		Configuration Status +	Cennectivity ÷	Model Cisco Firepower Threat Defense for Azure Serial Version 7.4.1-172
Policies >			Serial Number Mismatch	Orbaading Registration Key Method Snort Version 3.153.100-56
$a_{\sigma}^{\bullet}$ VPN $\rightarrow$ Events & Monitoring $\sqrt{r}$ Analytics $\rightarrow$		Not Synced	Pending Setup     Pending Setup	CDD is communicating with your device. Please check back in a moment.
Change Log			Pending Setup	API Tool     Workflows     Manage Backups
资 Settings >	FTD FTD	Syncing	Online     Online	Management  Notes
	C FTD		Online	ⓒ Changelog 로 Executive Report 스 Conflict Detection ● Disabled •
		Not Synced	Lunreachable	Check every: Tenant default (24 hours) - Label Groups and Labels
				Add Labels 🛛

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.

% Tools & Services	Tools & Services	Migrations		
<ol> <li>Settings &gt;</li> </ol>	Dynamic Attributes Connector	Firewall Migration Tool		
	⇒ Secure Connectors	會 ASA to FDM Migration		
	🖨 Firewall Management Center	會 Migrate FTD to cdFMC		
	ASA Templates			

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

T G Search for a migration by name		Displaying 0 of 0 results			1 C 🔹
Name 2	Status	Created Date (p)	Deprecisioning Date (1)	Actions	/
		to migrations found. Begin migrating ASA, P	DM, Checkpoint, Fortinet, or Palo Alto Networks firewalts to FTD.		

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

Initialize Migration	>
To initialize the migration process, name this migration a notify you when the migration tool is ready for use. When migration and launch the tool.	nd click OK. CDO will n ready, select this named
Name *	
fdm_migration	
This is an auto-generated name. You can change it if you	wish.
	Cancel

마이그레이션 초기화

Launch(실행)를 클릭하여 마이그레이션 컨피그레이션을 시작합니다.

Firewall Migration Tool			Q Search	<mark>ଓ</mark> ⊳,-	¢7. ⇔1	<b>?</b> -	•
Q         Search for a migration by name		Displaying 1 of 1 results					i C +
Name 0	Status	Created Date 0	Deprovisioning Date ©		Actions		
fdm_migration	<ul> <li>Ready to Migrate</li> </ul>	Jun 12, 2024	Jun 19, 2024		C 🔒 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 활 성화됩니다.

# 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.

С	lick 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)	$\sim$
	<ul> <li>This option migrates both device and shared configuration. Same FTD is moved from FDM managed to FMC managed.</li> </ul>	
	<ul> <li>The migration process is to be done over a scheduled downtime or maintenance window. There is device downtime involved in this migration process.</li> </ul>	
	<ul> <li>Ensure connectivity between FDM device and FMC to move the device from FDM to FMC using FDM.</li> </ul>	
	<ul> <li>User should provide FDM credentials to fetch details.</li> </ul>	
	<ul> <li>FDM Devices enrolled with the cloud management will lose access upon registration with FMC</li> </ul>	
	<ul> <li>Ensure out-of-band access to FTD device is available, to access the device in case of accessibility issues during migration.</li> </ul>	
	• 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.	
	<ul> <li>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.</li> </ul>	
	<ul> <li>FDM with Universal PLR cannot be moved from FDM to FMC.</li> </ul>	
	• 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.	

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.									
<ul> <li>Only devices with online connectivity and synced status will be displayed in the dropdown.</li> </ul>									
Click on change device status button to update the FDM device status from In-Use to Available.     Select EDM Managed Device									
Select FDM Managed Device									
fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_fdm_									
Connect									

FDM 장치 선택



구성 추출 완료

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



마이그레이션 프로세스 단계

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

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

기존 구성에 대한 취소 옵션

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

	1	2	3	4	5	6	7	8	9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 shou	d be carried o	ut in a maintena	nce window.						
Select Target 🕕					^			Selec	ource: Cisco Secure cted Migration: Inclu	Firewall Device Manager (7.2+) Ides Device and Shared Config
Firewall Management - Cl	oud-delivered FMC									>
Select Features										~
Device Configuration		SI	ared Configura	ition				Optimization		
✓ Interfaces		~	Access Control					Migrate Only Re	eferenced Objects	
Routes			🖂 Migrate tunn	elled rules as Pref	lter		(	Object Group S	earch 🕕	
ECMP			NAT							
<ul> <li>✓ Static</li> </ul>		~	Network Objects							
BGP			] Port Objects(no	data)						
EIGRP			Access List Obje	ects(Standard, Ext	anded)					
Site-to-Site VPN Tunnel	s (no data)		Access Control I	Policy Objects (Ge	olocation, Applic	ation, URL objects a	nd Intrusion Rul	9		
Policy Based (Crypt	o Map)		Time based Obi	ects (no data)						
Route Based (VTI)			Remote Access	VPN						
Platform Settings			File and Malware	Policy						
- DHCP										
<ul> <li>Server</li> </ul>										
Relay										
DDNS										
Proceed										
Note:Platform settings and	file and malware policy migrat	ion is supporte	d in FMC 7.4 and I	ater versions.						

선택할 기능

#### 그런 다음 변환을 시작합니다.

Firewall Migration Tool (Version 6.0.1)

	1	2	3	4	5	6	7		9	
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
	Note: Steps 7,8 and 9 should	d be carried o	ut in a maintena	nce window.		_				
Select Target 🗿					<u> </u>			Sele	ource: Cisco Secure Fin cted Migration: Include	ewall Device Manager (7 s Device and Shared Co
Firewall Management -	Cloud-delivered FMC									
Select Features										
Rule Conversion/ Proce	ess Config									
Start Conversion										

변환을 시작합니다.

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



보고서 다운로드.

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

	-	-	-									
	1			4	5	6	7	8	9			
	Extract FDM Information	Select Target	Map FTD Interface	Map Security Zones &	Review & Validate	Push Shared Config To	Move Manager	Review & Validate	Complete Migration			
				Interface Groups	(Shared Config)	FMC		(Device Config)				
	lote: Steps 7,8 and 9 shoul	d be carried	out in a maintenar	nce window.								
					^							
ap FTD Interface (	D						So	elected Option:	ure Firewall Device Ma Includes Device and Si	nager (7.2+) hared Config		
					0	Refresh						
FDM Interface Name			FTD Interface Nam	e								
igabitEthernet0/0		Gi	gabitEthernet0/0									
igabitEthernet0/1		Gi	gabitEthernet0/1									
0 v perupagel 2   4 4	Page 1 of 1 > >										$\odot$	Success
										$\sim$		Successfully gather
										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.

irewall Migration	n Tool (Version 6.0.1)						
		2 Extract FDM Information Select Target	3 Map FTD Interface Map Security Zor Interface Grou	5 6 es & Review & Validate Push Shared Config ps (Shared Config) FMC	g To Move Manager Review & Validate (Device Config)	9 Complete Mgration	
	Note:	Steps 7,8 and 9 should be carried	d out in a maintenance window.				
	Map Security Zones an	d Interface Groups 0			Idd SZ & IG	Source: Cisco Secure Firewall D Selected Option: Includes Devic	evice Manager (7.2+) e 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 v		
	inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	Select Interface Groups v		
	Note:Click on Auto-Create button to	p auto map the FDM nameif as the n	ame of the FMC interface objects an	d security zones. Click on next butto	n to proceed ahead.		

보안 영역 및 인터페이스 그룹

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



#### 그런 다음 다음을 선택합니다.

Firewall Migration Tool (Version 6.	0.1)						
	Extract FDM Information Se	2 3 lect Target Map FTD Interface Map Int	5 Security Zones & Review & Validate Push Share terface Groups (Shared Config) Fi	6 7 ed Config To Move Manager MC	8 Review & Validate (Device Config)	9 Complete Migration	
	Note: Steps 7,8 and 9 should be	carried out in a maintenance v	vindow.				
Map Security Zon	es and Interface Groups	0				Source: Cisco Secure Firewall Selected Option: Includes De	Device Manager (7.2+) vice and Shared Config
				Add SZ & IG	Auto-Create		
FDM Logical Interface	N FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface C	iroups		
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 a	is the name of the FMC interface o	bjects and security zones. Click on next	t button to proceed ahead.			
<b>₽₽1,0₽₽9</b> ₹2   4	✓ Page 1 of 1 ▶ ▶]						$\overline{\mathbf{x}}$
							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 구 성에 문제가 없음을 확인합니다.

Firewall Migration	n Tool	(Versio	on 6.0.1)			
			1     2 Extract FDM Information Select Target	3 4 6 Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Bhared Config)	6 7 8 Push Drawd Config To Move Manager Review & Wildone FMC (Device Config)	B Complete Migration
			Note: Steps 7,8 and 9 should be carried or	t in a maintenance window.		
	Opti	mize, F	Review and Validate Shared Conf	iguration Only 🕠	Sc Selec	urce: Cisco Secure Firewall Device Manager (7.2+) sted Migration: Includes Device and Shared Config
	Access	Control	Objects NAT Interfaces Routes Site-to-Si	e VPN Tunnels 👩 Remote Access VPN SNI		
	Acc	ess List Obj	jects Network Objects Port Objects Access Cor	trol Policy Objects VPN Objects Dynamic-Route	Objects	
	Se	lect all 3 ent	tries Selected: 0/3 Actions - Save	,		Q Search 4
			Name	Validation State	Туре	Value
			Q	۹	Q	Q
	0	1	OutsideIPv4Gateway	Validation pending	Network Object	172.18.1.1
		2	OutsidelPv4DefaultRoute	Validation pending	Network Object	0.0.0.0/0
		3	Banned	Validation pending	Network Object	103.104.73.155
ierpage 1 to3 of3 [4 ∢	Page	1 of 1	▶ FI			

Validate

#### 그런 다음 공유 컨피그레이션만 푸시

	$\oslash$	Successfully Validat	ed	
idation Summary (Pre-pu	Not selected for migration	4		3
Access Control List Lines		Network Objects		Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2	Not selected for migration			
Translation				

공유 컨피그레이션만 푸시

#### 완료율과 작업 중인 특정 작업을 관찰할 수 있습니다.

Firewall Migrati	on Tool (Version 6.0.1)				
	Push Shared Config to I	FMC		DISHING	Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Migration Status			24% Complete	
	Network Objects 🥏		Push to Cloud-delivered FMC is In progress. Please wait for entire push process to complete the migration.		
	Network Address Translation				
	Access Control Policies	0			
	Policy Assignment				
	Please download the Post-Push migration	n report for a detailed sum	mary. Download		

푸시 비율

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

Image: control light ligh		.1)									
Image: Bissent FDB internation Wage FDD internation Bissent FDB internation   Internation Groups Bissent FDB internation   Internation Groups Bissent FDB internation		()—	2				-0-	- 7	8		
Note: Steps 7.8 and 9 should be carried out in a maintenance window.         Push Shared Config to FMC         Migration Status         Image: Control List Lines         Access Control List Lines         Access Control List Lines		Extract FDM Informat	on Select Target	Map FTD Interface	Map Security Zones & Interface Groups	Review & Validate (Shared Config)	Push Shared Config To FMC	Move Manager	Review & Validate (Device Config)	Complete Migration	
Push Shared Config to FMC       Surce: Clicco Secure Freewall Device Analyser (1 Selected Migration: includes Device and Shared Critical Secure		Note: Steps 7,8 and 9 sh	ould be carried out	t in a maintena	nce window.						
Migration Status         Image: Status         Image: Status         Image: Status         Live Connect:         Status         Image: Status         Ima	Push Shared Co	nfig to FMC				^	,		Sele	Source: Cisco Secure Firev ected Migration: Includes	vall Device Manager (7 Device and Shared Co
Mgration of Shared Config is complete, policy is pushed to FMC.         Wext Step - Login to FMC to deploy the policy to FTD.    Live Connect:  Selected Context: Single Context Mode  Access Control List Lines          Access Control List Lines              Martine Control List Lines              Access Control List Lines              Met selected for migration             Access Control List Lines             Met selected for migration             Access Control List Lines	Migration Status										
3         Not selected for migration         4         Not selected for migration         3           Access Control List Lines         Access List. Objects         Network Objects         Port Objects         Access Control Policy Objects (Geo, Application, URL objects and URL objects and URL objects)	Migration of Share Next Step - Login t	Config is complete, policy i FMC to deploy the policy t	s pushed to FMC. o FTD.								
	Live Connect: Selected Context: Single Migration Summary (Post	Context Mode Push)									
	Live Connect: Selected Context: Single Migration Summary (Post	eontext Mode Push) Is Net Cland			4 Network (	Dbjects				3 Access Control Policy O (Geo, Application, URL obje Intrusion Rule Group)	bjects cts and )
Not selected for migration 2 Not selected for migration Not selected for migration	Live Connect: Selected Context: Single Migration Summary (Post 3 Access Control List Lin Not selected for migra	Push) es Not citized	selected for migration ccess List Objects Intr. Extended used is 800 RAVPIECORP.		4 Network 0	Dejects or migration				3 Access Control Policy O (Geo, Application, URL obje- intrusion Rule Group) Not selected for migra	bjects cts and )

FMC에 공유 구성 밀어넣기 완료

#### 이 옵션은 확인 메시지를 트리거하여 관리자 마이그레이션을 계속할지 묻습니다.

## **Confirm Move Manager**

#### Requires maintainence window to be scheduled FDM manager will be moved to be managed in FMC.





관리자 이동 확인

관리자 마이그레이션을 진행하려면 Management Center ID 및 NAT ID가 있어야 하며, 이는 필수적 입니다. 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 창 이 시작됩니다.

1     2     3     4     5     6     7     8     9       Extract FDM Information     Select Target     Map FTD Interface     Map Security Zones & Review & Validate     Push Shared Config To     Nove Manager     Review & Validate     Complete Migration       Interface Groups     (Dhared Config)     FMC     (Device Config)     Complete Migration	
Extract FDM Information Select Target Map FTD Interface Map Beautry Zones & Review & Validate Push Shared Config To Move Manager Review & Validate Complex Migration Interface Groups (Shared Config) FMC (Device Config)	
Note: Steps 7,8 and 9 should be carried out in a maintenance window.	
Move Manager Selected Migration: includes Device and Shared C	(7.2+) 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 mana	ge it.
Management Cent Management Cente 💿 NAT ID 💿 Threat Defense Hostn DNS Server Group Management Center/ Data Interface	
cisco cdo j Lcioudapp.n CiscoUmbretaDNSServerGroup v 💽 Data Management Select Data Interface	¥.

#### Move Manager

#### 관리자 센터 ID 및 NAT ID

Firewall Migration Tool (Version 6	5.0.1)			X			
	1 Extract FDM Information Set	2 Upd	ate Device Name for F	Registration	B B Review & Validate (Device Config)		
	Note: Steps 7,8 and 9 should be	-fdm-					
Move Manage	r		Cancel Save		Source: Cisco Secure Selected Migration: Inclu		
Update D This step is mandatory	etails and should be performed during a d	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/ D	lata Interface	
cisco-mex-ngfw-tac.app.us.	.odo		joroa-fdm-tech.zone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup ~	Data Management Sek	ect Data Interface	

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.

Firewall Migratio	n Tool (Version 6.0	.1)					
		Extract FDM Information Se	2 3 ect Target Map FTD Interface Map	4 5 p Security Zones & Review & Validate Pu Interface Groups (Shared Config)	6 7 sh Shared Confg To Move Manager FMC	8 9 Review & Valdate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should be	carried out in a maintenance	window.			
	Move Manager					Source: Cisco Sec Selected Migration: I	ure Firewall Device Manager (7.2+) ncludes Device and Shared Config
	Update Detai This step is mandatory and	ls d should be performed during a d	lowntime window. After you re	egister the device with the mana	gement center or Cloud-delivere	ed FMC, you can no longer use	the device manager to manage it.
	Management Cent	Management Cente 🕕	NAT ID 🕕	Threat Defense Hostn	DNS Server Group	Management Center/	Data Interface
	cisco us.cdo	ogu ¥66GW	104V 3sP	M fdm-Azure	CiscoUmbrellaDNSServerGroup ~	Data Management	Select Data Interface v
				_		$\overline{}$	/

Move Manager

관리 센터 ID 및 NAT ID

#### Update Details 옵션을 선택한 후 동기화를 시작할 디바이스입니다.

n Tool (Version 6.0	0.1)							
	1 Extract FDM Information Se	2 3 lect Target Map FTD Interface	4 Map Security Zones & Revi Interface Groups (Sha	5 6 ev & Validate Push Shared Config To red Config) FMC	7 Move Manager	8 9 Review & Validate Complete Migration (Device Config)		
	Note: Steps 7,8 and 9 should be	carried out in a mainten	ance window.					
Move Manager						Source: Cisco Selected Migration		
Update Deta	ails	downtime window.	SYNCING	he FDM Device	- ud-delive	red FMC, you can no longer us	e the device manager to	manage it.
Management Cent	Management Cente 🕕	NAT ID 🚯	9%	Complete		Management Center/	Data Interface	
cisco us.cd	o oguq I66GW	104	PMI fdm-Azure	CiscoUmbrellaD	NSServerGroup ~	Data Management	Select Data Interface	~

FDM 장치 동기화

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

rewall Migratior	n Tool (Versi	on 6.0.1)				
		1 2 Extract FDM Information Select T	yest Map FTD Interface Map Security Zones & Revi Interface Oroups (Sh	6 7 ev & Valdate Push Shared Config To Move Manager ared Config) FMC	9 Review & Validate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should be car	ried out in a maintenance window.			
	Optimize, F	Review and Validate Device C	Configuration Page 💿	^	Source: Cisco Secure F Selected Migration: Inclu	irewall Device Manager (7.2+) tes Device and Shared Confid
		Objects NAT Interfaces Routes Si	te-to-Site VPN Tunnels 🕥 Remote Access VPI	N SNMP DHCP		
	Static PPPo	ε)				
	Select all 2 er	tries Selected: 0 / 2			Q Search	+
	• *	Interface	Zone Q	IP Address	State	
	0 1	GigabitEthernet0/0	outside_zone		Enabled	
	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
	2	OgabEEternet01	inside_zone	45.1	Enabled	
1 to 2 of 2 🛛 4 🔺	Page 1 of 1	> >]				/
					Validate	

FDM 구성 설정 검증

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

	$\odot$	Successfully Validated		
alidation Summary (Pre-pu	ish)			
		2	1	1
		Logical Interfaces	Routes	DHCP
			(Static Routes, ECMP)	(Server, Relay, DDNS)
	0	0		
	Platform Settings	Malware & File Policy		
	(snmp,http)	manuale of her oney		

유효성 검사 상태 - 구성 밀어넣기

#### 푸시 컨피그레이션의 백분율이 표시된 팝업 창

Firewall Migration To	ool (Version 6.0	0.1)				
		Extract FDM Information 1	2 (3 Select Target Map FTD	PUSHING 10% Complete Push to Cloud-delivered FMC is in progress. Please wait for entire push process to complete the micration	7) danager	Berview & Voltane Complete Migration (Device Config)
Co	omplete Migrat	lion				Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Interfaces	0				
	Routes					
	Policy Assignment					
Ple	ase download the Post-F	ush migration report for a detailed	summary. Download R			

푸시 완료율

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

Aigration Tool (Version 6	.0.1)			
	Extract FDM Information Select Target	3 4 5 Map FTD Interface Map Security Zones & Raview & Val Interface Groups (Shared Con	6 7 Idans Push Shared Config To Move Manager Re rfg) PMC (0	eve & Valdara Complete Migration evec Config
	Note: Steps 7,8 and 9 should be carried ou	t in a maintenance window.		
Complete Migr	ation	<u>^</u>		Source: Cisco Secure Firewall Device Manager () Selected Migration: Includes Device and Shared C
Migration Status				
Migration is com Next Step - Logi	plete, policy is pushed to FMC. n to FMC to deploy the policy to FTD.			
Live Connect:				
Selected Context: Singl	e Context Mode			
Selected Context: Singl Migration Summary (Po	e Context Mode ist Push)			
Selected Context: Singl Migration Summary (Po	e Context Mode st Push)	× 4		3
Selected Context: Singl Migration Summary (Po 3 Access Control List	e Context Mode sst Push) Not selected for migratic	n 4 Network Objects		3 Access Control Policy Objects
Selected Context: Singl Migration Summary (Po 3 Access Control List	e Context Mode st Push) Not selected for migratio Access List Objects (Stendart, Extended used in B	n 4 Network Objects		3 Access Control Policy Objects (Geo, Application, URL objects and b) (Deo, Application, URL objects and
Selected Context: Singl Migration Summary (Po 3 Access Control List)	e Context Mode ist Push) Lines Access List Objects (Stendard, Edended used in B RevPrescopy)	on <b>4</b> Network Objects		3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
Selected Context: Singl Migration Summary (Po 3 Access Control List	e Context Mode st Push) Lines Lines Access List Objects (Stendart, Extended used in B RAVINECORP) pation 2	n 4 Network Objects	Nut selected for migration Post Objects 1	3 Access Control Policy Objects (Geo, Application, URL objects and htrusion Rule Group)
Selected Context: Singl Migration Summary (Po 3 Access Control List) Not selected for mig Dynamic-Roate Ob	e Context Mode st Push) Lines Reference of the selected for migration Access List Objects (Dandard, Extended used in B RAVPARCORP gation Jets	on 4 Network Objects Ion 2 Logical Interfaces	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and htrusion Rule Group)

마이그레이션 완료

## 다음을 확인합니다.

FDM이 cdFMC로 성공적으로 마이그레이션되었는지 확인합니다.

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

-1 1-1 1- CISCO	Defense Orchestrat	or	Ser	vices					Q Search		<b>0</b> 🕅	•	≙• د	1 0	-	-
≡	Hide Menu											>	Cloud-D	elivered	FMC	
in.	Dashboard		0	Search by Device Name ID Article	is or Serial N	imber							Version	20240514	4	
0	Multicloud Defense		FMC	Secure Connectors									Actions			
	Inventory		-										0.000	k Ear Change		
Con	Iguration		1	"Auto onboard On-Prem FMCs from S	ecureX tenant*	setting is not enabled. Click here to e	enable settin	g.					d Depl	oyment		
۲	Policies	>	2										Upda     Worl	ites flows		
٢	Objects	>		Name		Version	Devices	Туре	Status	Last Heartbeat			O APIE	xplorer		
-&-	VPN	>		Cloud-Delivered FMC		20240514	⊜3	Cloud-Delivered FMC	Active	06/12/2024, 12:42:21			Manageme	nt		
Ever	ts & Monitoring					7.2.7-build 500	⊜0	On-Prem FMC	A Unreachable				🖨 Devi	ces		
*	Analytics	>											Polic	ies cts		
0	Change Log												< NAT			
	Jobs												-> Site	ote Access V	(PN	
*	Tools & Services		Tools I	& Services	Migrations								Platf	orm Settings	1	
\$	Settings	>	© C	Dynamic Attributes Connector	Firewall	Migration Tool							System			
			# S	Frewall Management Center	ASA to F	DM Migration							O Conf	iguration		
			D A	SA Templates	El migrate	TO to control							Smarting     AMP	rt Licenses Managemen	nt	
													+ Devi	ce Health		
													O Cisc	o Cloud Even	ds	

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 찾 을 수 있습니다.

Defense Orchestrator Analysis Policies	Devices Objects Integration	to Re	eturn Home Deploy Q 🔿 🌮 🌣 🖉 📕	<ul> <li>SECURE</li> </ul>
-fdm-Azure		Deployments	Upgrades Health OTasks	±   ● Show Notifications
Cisco Firepower Threat Defense for Azure		20+ total 0 v	waiting 0 running 0 retrying 6 success 20+ failures	Q. Filter
Device Interfaces Inline Sets Routing DHCP VTEP		Policy Deployment	nt	
		Policy Deploym	nent to	1m 54s 🗙
General / ± +	License			
Name: -fdm-Azure	Performance Tier : FT	Health Policy		
Transfer Packets: No	Essentials:	Apply Initial_He Health Policy app	ealth_Policy 2023-06-29 17:28:08 to -fdm-Azure lied successfully	1m 40s ×
Troubleshoot: Logs CLI Download	Export-Controlled Features:			
Mode: Routed	Malware Defense:	<ul> <li>Discovery</li> </ul>		
Compliance Mode: None	IPS:	fdm-Azure	<ul> <li>Discovery from the device is successful.</li> </ul>	2m 10s 🗙
Performance Profile: Default	Carrier:	SFTunnel		
TLS Crypto Acceleration: Disabled	URL:	-fdm-Azure	- SFTunnel connection established successfully.	- ×
	Secure Client Premier:			
Device Configuration: Export Export Download	Secure Client Advantage:	Register		
OnBoarding Method: Registration Key	Secure Client VPN Only:		Remove completed tasks	
Inspection Engine	Health		Management	/ 🔍
Inspection Engine: Snort 3	Status:	0	Remote Host Address:	NO-IP
Revent to Smort 2	Policy: Initial_Health_Policy 2023-0	06-29 17:28:08	Secondary Address:	
	Excluded:	None	Status:	0
			Manager Access Interface:	Management Interface
Inventory Details c	Applied Policies	1	Advanced Settings	1
X III 🖙 + 1				

cdFMC 등록 작업이 완료되었습니다.

디바이스가 cdFMC > Device > Device Management에 있습니다.

Defense Orchestrator FMC / Devices / Device Management	Analysis	Policies	Devices C	bjects	Integratio	'n		*> Return Home	Deploy	Q	• 💞	° 0		×	cisco SECURE
View By: Group  All (3)  Error (0)  Warning (0)	Offline (0)	Normal (3)	<ul> <li>Deployment</li> </ul>	t Pending	(3) • L	Upgrade (0)	<ul> <li>Snort 3 (3)</li> </ul>						Migrat Q. Searc	e   Depk	oyment History
Collapse All														Download	Device List Report
Name			Model			Version	Chassis	Licenses		Acces	s Control P	olicy	Auto	RollBack	
Ungrouped (3)															
N/A - Routed Short 3			FTDv for Azu	•		7.4.1	N/A	Essentials		None			\$P		1

cdFMC에 등록된 디바이스

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

٢	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis	Policies	Devices	Objects	Integration			+> Return Home	Deploy	Q	•	<b>6</b> 24	0		~	cisco SECURE
									Object M	anagement	Int	rusion	Netw	ork Ana	lysis Policy	DNS	Import/Export
																	New Policy
	Access Control Policy			Status				Last Modified	Lock 5	Lock Status							
	Default Access Control Policy Default Access Control Policy with default action block		Targe	eting 0 devices				2024-06-11 22:28:19 Modified by "Firepower System"									% 0 ∕ ¥
	FTD-Mig-ACP-1718216278		Targe Up-tr	ating 1 devices ordate on all targ	eted devices			2024-06-12 12:18:00 Modified by 1									5 8 × ¥

마이그레이션 정책

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

			1.0										
Network		Add Network	▼ Q Fil	ter									
		Sh	now Unused Ob	jects									
- 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													
Name	Value		Туре	Override									
any	0.0.0.0/0 ::/0		Group		¶∎ Q ≣ M								
any-ipv4	0.0.0.0/0		Network		¶a q ≣ M								
any-ipv6	::/0		Host		¶a <b>q</b> ∦ #								
Banned	103.104.73.155		Host	0	有人资格								
Gw_test01	172.22.2.1		Host		哈/首め								
Inside_Network_IP	192.168.192.10		Host	0	┗/〒め								
IPv4-Benchmark-Tests	198.18.0.0/15		Network		¶a () ₩								
IPv4-Link-Local	169.254.0.0/16		Network		¶a q ⊕ M								
IPv4-Multicast	224.0.0.0/4		Network		¶∎ Q ≣ M								
IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶∎ ⊂ ≣ M								
IPv4-Private-172.16.0.0-12	172.16.0.0/12		Network		¶∎ Q ≣ M								
IPv4-Private-192.168.0.0-16	192.168.0.0/16		Network		唱く言め								
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		¶∎ Q ≣ #								
IPv6-IPv4-Mapped	::##:0.0.0.0/96		Network		¶∎ Q ≣ M								

FDM에서 cdFMC로 마이그레이션된 객체

#### 마이그레이션된 개체 관리 인터페이스입니다.

FMC / Objects / Object Mar	tor nagement	Analysis	Policies	Devices	Objects	Integration		*> Retur	n Home	Deploy	۹ 0	¢ 😜	0		× 1	diada: SECURI
AAA Server     Access List     Address Pools     Application Filters	Interface	CE	t your network	k to help you r	manage and c	lassify traffic flow. An i	nterface object simply groups inte	rfaces. These groups may span n	ultiple de	Add	an also con	figure multip	• C	, Filter	a single d	levice.
AS Path BFD Template Cipher Suite List	Name 🔺	•_ig					Type Interface Group		Routed	ce Type					,	¥∧
Community List     DHCP IPv6 Pool     Distinguished Name	> 🖷	-fdm-Azure					Security Zone		Routed						,	¥۸.
DNS Server Group External Attributes File List	> 🖷	-fdm-Azure de_ig					Interface Group		Routed						,	¥∧
FlexConfig     Geolocation     Interface     Kap Object	> =	-fdm-Azure de_zone					Security Zone		Routed						,	¥ 8
Key Chain Network > PKI	> =	-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 번 역 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.