# CDO内のFMTを使用したcdFMCへのFDMの移行

闪谷		
<u>はじめに</u>		
<u>前提条件</u>		
<u>要件</u>		
<u>使用するコンポーネント</u>		
<u>背景説明</u>		
<u>設定</u>		
<u>確認</u>		

## はじめに

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

## 前提条件

要件

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

### 使用するコンポーネント

このドキュメントは、前述の要件に基づいて作成されました。

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

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

### 背景説明

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

### 設定

1.-FDMでシスコクラウドサービスを有効にする

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

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



Registration Cloudサービス

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

Firewall Device Manager	國 砂 詳正 Monitoring Policies Objects Device	(b) (c) (c) (c) (c) (c) (c) (c) (c) (c) (c
Firowall Device Manager  System Settings  Management Access Logging Settings DHCP DDNS Service DNS Service Management Interface Hostname Time Services SSL Settings	Monitoring     Policies     Objects     Device <b>Device Summary Cloud Services</b> Diverse     Diverse   With Begistered       Not 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 user register with the Clisco Device Service Ser	Administrator
	US Region V	
HTTP Proxy		
Reboot/Shutdown	Registration Key Enter Registration Key	
Cloud Services	Service Enrollment	
Central Management	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.	
URL Filtering Preferences	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 bimprove 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 Semple Data that will be sent to Cisco. See more      Profit Cisco Success Network      Med help?(2)	

```
クラウドサービスへの登録
```

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

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

discle Defense Orchestrator	Inventory	Q Search	<mark>७ २</mark> न- <b>८०</b> - <b>±1</b> ७	•
Hide Menu	T Devices Templates Q Search by Device Name, IP Address, or Serial Number	Displaying 8 of 8 results		C (8) +
Dashboard     Multicloud     Defense	All ASA FTD			
inventory	Name ¢	Configuration Status 🗢	Connectivity \$	

オンボードFDM、オプションの追加

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



#### デバイスまたはサービスタイプの選択

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



### ここでは、前の手順で必要な登録キーが示されています。

FTD 0000 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. (FTD 6.7+, 1000, 2100 and 3100 series only)	
1 Device Name		
2 Database Updates	Enabled	
3 Create Registration Key	7a53c	
4 Smart License	(Skipped)	
5 Done	Your device is now onboarding. This may take a long time to finish. You can check the status of the device on the Devices and Services page. Add Labels Add label groups and labels Go to Inventory	

登録プロセス

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

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

Monitoring	Policies	Objects	Device: joroa-fdm-tech
Device Summary Cloud Serv	/ices		
You can register to use Cisco Defense register with the of auto-enroll with C want to use Secur configure Smart L register with the o	ne device w e Orchestra cloud using CDO or a Se re Firewall o .icensing, w cloud, you c	vith the Cisco clo ator (CDO) for m your CDO or oth cure Firewall Ma device manager which automatica can enable or dis	anagement or want to remain in evaluation mode, then her 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 Type	_		
Security/CDO A	Account	Smart Licensing	3
Region US Region			~ 🕚
Registration Key 7a53c2			
Service Enrol	Iment		
Cisco Def	ense Orc	hestrator	
Cisco Defens devices. Sele account.	se Orchestra act this option	ator is a cloud-b on if you want to	pased management tool used for managing network o register the device in your Cisco Defense Orchestrator
🔽 Enable C	Cisco Defen	se Orchestrator	
Cisco Suc	cess Net	work	
Cisco Succes essential for product and of the produc	ss Network Cisco to pro to make you ct in your ne	enablement pro ovide technical s u aware of unuso atwork.	vides usage information and statistics to Cisco which are support. This information also allows Cisco to improve the ed available features so that you can maximize the value
Check out the	e Sample D	ata that will be s	sent to Cisco. See more 💙
🚦 🔽 Enroll Ci	sco Succes	s Network	

FDM登録

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

Monitoring Policies Objects Device:	() (in the second secon
Device Summary         Cloud Services         Connected         Registered         Enrollment Type: Security/CDO Account         Tenancy:         Region: US Region	¢ ~
Cisco Defense Orchestrator DISABLE	Cisco Success Network Cisco Success Network enablement provides usage information and statistics to Cisco which
Clock Place with the transformed equation of the device and re-on-board using the registration key method with the "Security/CDO account" option.  Cisco Defense Orchestrator (2 allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.	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 <u>Sample Data</u> that will be sent to Cisco.
Send Events to the Cisco Cloud ENABLE	
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 (2, to analyze the events and to evaluate threats that the device might have encountered. When you enable this service, this device will send high priority intrusion, file, malware events and all connection events to the Cisco cloud.	

FDM登録の完了

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

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

"dudi: cisco Defense Orchestrator	Inventory	у				Q Search	<mark>ଓ</mark> ⊳7•	۰ 🗅 ¢	⇔1	۰.
Hide Menu	T Device	Templates Q Search by D	Device Name, IP Address, or Serial	Number		Displaying 9 of 9 results	C 🖲 🕇	> Fom		2
Multicloud	All ASA	FTD						Device	Details	
Defense	• •	iame 0		Co	nfiguration Status 🌣	Connectivity \$		Mod	el	Cisco Firepower Threat Defense for Azure
Configuration	0	LSA				A Unreachable		Vers	ion sarding sod	7.4.1-172 Registration Key
Objects	0	DM				Serial Number Mismatch		Sno	t Version	3.1.53.100-56
son VPN	0	TD		Ø	Not Synced	Pending Setup		Syn coo in ar	cing is communicat noment.	ing with your device. Please check back
√r Analytics →	0	TD				Pending Setup		Device	Actions	
(Change Log	0	TD				Pending Setup		φ 	PI Tool /orkflows lanage Back	ups
Tools & Services	•	fdm <mark>.</mark> DM		3	Syncing	Online		B R	emove	
tig setungs	0	TD				Online			otes	
	0	TD				Online		11 E	xecutive Rep	port
	0	TD		ø	Not Synced	A Unreachable		止 Cor Che	flict Detecti ck every:	on Disabled • Tenant default (24 hours) •
								Label	Groups and L	abels
								Add L	abels O	

CDOインベントリFDMオンボーディング

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



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

% Tools & Services		Tools & Services	Migrations
{ŷ} Settings	>	Ø Dynamic Attributes Connector	Firewall Migration Tool
		⇒ Secure Connectors	會 ASA to FDM Migration
		🖨 Firewall Management Center	备 Migrate FTD to cdFMC
		ASA Templates	

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

•	Q Search for a migration by name		Displaying 0 of 0 results			10
Name	1 Data	. 0	reated Date (p	Deprovisioning Data 8	Actions	/
		No migration	a found. Begin migrating ASA, FDM, Checkpoint, Fortinet	, or Palo Alto Networks firewalls to FTD.		

名前を変更したら、Launchをクリックして移行を開始します。

	U Sei
Initialize Migration	×
To initialize the migration process, name this migration and click OK. notify you when the migration tool is ready for use. When ready, sele migration and launch the tool.	CDO will ct this named
Name *	
.fdm_migration	
This is an auto-generated name. You can change it if you wish.	
Ca	ancel OK

移行の初期化

Launchをクリックして、移行の設定を開始します。

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

移行の開始プロセス

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

# Firewall Migration Tool (Version 6.0.1)

# Select Source Configuration ()

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

FMTソース設定の選択

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

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

) C	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>	
	User should provide FDM credentials to fetch details.	
	<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.	

移行オプション

移行方法を選択したら、表示されたリストからデバイスを選択します。

Live Connect to FDM									
Select any FDM device onboarded on CDO from the below dropdown.									
<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デバイスの選択



構成の抽出が完了しました

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



移行プロセスの手順

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

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

既存の構成のキャンセルオプション

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

	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 🕕					^			Selec	ource: Cisco Secure Fin cted Migration: Include	rewall Device Manager (7.2 es Device and Shared Con
Firewall Management - C	Cloud-delivered FMC									)
Select Features										~
Device Configuration		SI	ared Configura	ation				Optimization		
✓ Interfaces		~	Access Control				1	🗸 Migrate Only Re	eferenced Objects	
Routes			✓ Migrate tunn	elled rules as Prefi	lter		(	Object Group S	earch 🕕	
ECMP			NAT							
Static		~	Network Objects							
BGP			Port Objects(no	data)						
EIGRP			Access List Obje	ects(Standard, Exte	inded)					
Site-to-Site VPN Tunne	als (no data)	~	Access Control I	Policy Objects (Geo	olocation, Applic	ation, URL objects a	nd Intrusion Rul	9		
Policy Based (Cry	pto Map)		Time based Obje	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	d file and malware policy migrat	ion is supporte	f in FMC 7.4 and I	ater versions.						

選択するフィーチャ

### 次に、変換を開始します。

Firewall Migration Tool (Version 6.0	.1)					
	Educat FDM Information Select Tar	3 4 get Map FTD Interface Map Security Zone Interface Group	5 6 s.8. Review & Validate Push Shared Config s (Shared Config) FMC	7 8 To Move Manager Review & V (Device C	9 alidate Complete Migration onfig)	
	Note: Steps 7,8 and 9 should be carr	ied out in a maintenance window.				
Select Target 📀					Source: Cisco Secure Firewa Selected Migration: Includes D	all Device Manager (7.2+) Device and Shared Config
Firewall Management - C	Cloud-delivered FMC					>
Select Features						>
Rule Conversion/ Proces	ss Config					~
Start Conversion						

変換を開始します。

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



レポートのダウンロード

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

1	2 3 4 ation Select Target Map FTD Interface Map Security Zones Interface Groups	5 6 4 Review & Validate Push Shared Config To (Shared Config) FMC	7 8 Move Manager Review & Validate (Device Confg)	9 Complete Migration		
Note: Steps 7,8 and 9 s	hould be carried out in a maintenance window.					
Map FTD Interface 0			Source: Cisco Seco	re Firewall Device Manager (7	.2+)	
		Refresh	Selected Option:	includes Device and Shared Co	xing	
FDM Interface Name	FTD Interface Name					
GigabitEthernet0/0	GigabitEthernet0/0					
GigabitEthernet0/1	GigabitEthernet0/1					
20 v percpage 2 (4 4 Page 1 of 1 >	۶I					Success Successfully gathered details!
				(	Back Next	

表示されるインターフェイス

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

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

Firewall Migration Tool (Version 6.0.1)

	Note: Stens 7.8 and 9 should be cr	urried out in a maintenance wir	ndow		
	note: Steps 1,0 and 5 anothe be ca	aneo out in a maintenance wi			
Map Security Zone	s and Interface Groups 🕕	)			Source: Cisco Secure Firewall Device Mana Selected Option: Includes Device and Sha
			(	Add SZ & IG Auto-Create	
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	

セキュリティゾーンとインターフェイスグループ

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

		Charon
FTD		Group
Gigabiti	Auto-Create	ups
Gigabiti	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.	ups
	Select the objects that you want to map to FDM interfaces	
	Cancel Auto-Create	

### 次にNextを選択します。

irewall Migration Tool (Version 6.0	0.1)						
	Extract FDM Information Select	3 Target Map FTD Interface Map 1 Interface Map 1	Security Zones & Review & Validate Push Sha erface Groups (Shared Config)	8 7 red Config To Move Manager FMC	8 Review & Validate (Device Config)	9 e Complete Migration	
	Note: Steps 7,8 and 9 should be ca	nried out in a maintenance w	vindow.				
Map Security Zon	es and Interface Groups (	)				Source: Cisco Secure Firewall I	evice Manager (7.2+
				Add SZ & IG	Auto-Create	selected option. Includes Dev	ce and shared comi
FDM Logical Interface	N FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface G	roups		
outside	outside_zone	GigabitEthernet0/0	outside_zone (A)	outside_ig (A)	v		
Note:Click on Auto-Create	button to auto map the FDM nameif as I	the name of the FMC interface o	bjects and security zones. Click on ne	t button to proceed ahead.			
10 v periopage 2 4	✓ Page 1 of 1 ▶ ▶						
							Back Next

After Auto-Creationオプション

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

Lever DOI kinner     Lever Config     Lever Config	Firewall Migration	n Tool	(Version	6.0.1)			
Interesting 2, 2, and 9 should be carried out in a maintenance window.         Optimize, Review and Validate Shared Configuration Only         Access Centrol       Objects       Nat       Bate Stebe Sde VPH Tunnels       Route Access VPH       DB/D       DB/D         Access Centrol       Objects       Nat       Bate Stebe Sde VPH Tunnels       Route Access VPH       DB/D       DB/D         Access Centrol       Objects       Nat       Bate Stebe Sde VPH Tunnels       Route Access VPH       DB/D       DB/D         Extended 0/13       Access Centrol       Objects       Objects </th <th></th> <th></th> <th></th> <th>1     2 Extract FDM Information Select Target</th> <th>3 4 5 Map FTD Interface Map Security Zones &amp; Review &amp; Validate Interface Groups (Bhared Config)</th> <th>6 7 8 Push Stared Config To Move Manager Review &amp; Validate FMC (Device Config)</th> <th>9 Complete Mgration</th>				1     2 Extract FDM Information Select Target	3 4 5 Map FTD Interface Map Security Zones & Review & Validate Interface Groups (Bhared Config)	6 7 8 Push Stared Config To Move Manager Review & Validate FMC (Device Config)	9 Complete Mgration
Optimize, Review and Validate Shared Configuration Only       Source: Cace Socure Fixewall Device Manager (7.2 Selected Migration: Includes Device and Shared Configuration: Includes Device And Includes Device and Shared Configuration: Include				Note: Steps 7,8 and 9 should be carried ou	t in a maintenance window.		
Access Control       Objects       NAT       Interfaces       Routes       Stete OStev VPN Trunnets       Remote Access VPN       SMMP       DICP         Access List Objects       Network Objects       Petr Objects       Access Control Policy Objects       VPN Objects       Dynamic-Route Objects         Select all 3 entries       Selected 0/3       Access Control Policy Objects       VPN Objects       Dynamic-Route Objects       Q       Search		Optin	nize, Re	eview and Validate Shared Conf	iguration Only 🕠	Si Sele	surce: Cisco Secure Firewall Device Manager (7.2+) cted Migration: Includes Device and Shared Config
Access List Objects       Network Objects       Port Objects       VPN Objects       VPN Objects       Dynamic-Route Objects       C       Search       C         Select all 3 entries       Selected. 0/3       Access Control Policy Objects       VPN Objects       Dynamic-Route Objects       Value       C		Access	Control O	bjects NAT Interfaces Routes Site-to-Sit	e VPN Tunnels 🕢 Remote Access VPN SNI		
Image: State Control         Validation State Control         Type Control         Value Control           Image: State Control         0		Acce	ss List Objec ect all 3 entrie	ts Network Objects Port Objects Access Con s Selected: 0/3 Actions - Save	trol Policy Objects VPN Objects Dynamic-Route	Objects	Q Search 🛓
Image: Construction of the state o		•		Name	Validation State	Туре	Value
1       OxdadeP+Gderway       Validation pending       Network Object       172.18.1.         2       OxdadeP+QDefwadRoute       Validation pending       Network Object       0.0.00         3       Banned       Validation pending       Network Object       103.104.73.155				Q	٩	Q	Q
2     Overage     Value     Value     Verwark Capet     0.0.00       3     Banned     Value     Value     Network Object     103.104.73.155		0	1	Dutside/Pv4Gateway	Validation pending	Network Object	172.18.1.1
			3 8	Sanoed	Valdation pending	Network Object	103 104 73 155

Validate

### 次に、共有設定のみをプッシュします

	$\odot$	Successfully Validat	ed	
dation Summary (Pre-pu	ush)			
3		4		3
ccess Control List Lines		Network Objects		Access Control Policy
				(Geo, Application, URL objects and Intrusion Rule Group)
2	Not selected for migration			
Network Address				
Tanolaton				

プッシュ共有構成のみ

### 完了の割合と作業している特定のタスクを確認できます。

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

プッシュ率

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

	Extract FDM Informatio	n Select Target M	ap FTD Interface	4 Map Security Zones & Revi Interface Groups (Shi	5 Push Sha red Config) To I	red Config FMC	8 Review & Validate (Device Confg)	9 Complete Migration	
	Note: Steps 7,8 and 9 sho	uld be carried out in	a maintenar	nce window.					
Push Shared Cor	fig to FMC				^		Sel	Source: Cisco Secure Firewa	II Device Manager (
Migration Status									
Live Connect: Selected Context: Single Co Migration Summary (Post F	ntext Mode Jsh)								
Live Connect: Selected Context: Single Co Migration Summary (Post P	ntext Mode Jsh)			4				3	
Live Connect: Selected Context: Single Co Migration Summary (Post F 3 Access Control List Line	ntext Mode ush)			4 Network Object				3 Access Control Policy Obji	ects
Live Connect: Selected Context: Single Co Migration Summary (Post F 3 Access Control List Line	ntext Mode ush) I Vet e Ac (Standa			4 Network Object				3 Access Control Policy Obj (Geo, Application, URL etjects intrusion Rule Group)	ects s and
Live Connect: Selected Context: Single Co Migration Summary (Post P 3 Access Control List Line Not selected for migratic	ntext Mode Isb) Net s Ac (Stands	elected for migration cess List Objects nt, Dranded used & BORY RAVPAREORY 2		4 Network: Object	ration			3 Access Control Policy Obj (Geo, Application, URL objects Intrusion Rule Group)	ects s and
Live Connect: Selected Context: Single Cr Migration Summary (Post P Access Control List Line Not selected for migratic Dynamic-Roote Object	ntext Mode ush) Not s Ac (Standa	elected for migration cess List Objects nt, Edmodel used to BOPF ntvriteComP 2 rk Address Translation		4 Network Object Not selected for mig Logical Interfact	ration			3 Access Control Policy Obje (Geo, Application, URL bejects intrusion Rule Group) Not selected for migratis DHCP	ects s and

共有構成のFMCへのプッシュが完了しました

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

# **Confirm Move Manager**

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



移動マネージャの確認

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

Firewall Migration Tool (Versior	n 6.0.1)											
		1			-0-			0	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		
	Not	e: Steps 7,8 and 9 should	be carried or	ut in a maintena	nce window.							
Move Manag	ger						·		So Selec	urce: Cisco Sec ted Migration:	cure Firewall Devi Includes Device a	ice Manager (7.2+) and Shared Config
Updat	e Details	•										
This step is mandat	ory and she	Suid be performed during	a downtime	window. After y	ou register the de	vice with the ma	anagement center	or Cloud-delive	Managemen	n no longer use	the device mana	iger to manage it.
management ce		management center.		Ĭ	The de De	nense nosun	Dit 5 Server	Group	managemen	a comen in	outa interiace	
cisco	cdo				i	Lelouda	pp.n CiscoUmbrellaDN	SServerGroup ~	💿 Data 🔵 Ma	nagement	Select Data Interface	0 V

#### Move Manager

#### マネージャセンターIDとNAT ID

Firewall Migration Tool (Version 6.	0.1) Extract FCM information See Note: Steps 7,8 and 9 should be	2 Updates Traper	ate Device Name for F	X	Revers & Voltares Clevios Config		
Move Manager Upstre Der This step is mandatory a	rais and should be performed during a d	lowntime	Cancel Save		Source: Cisco Sec Selected Migration: I d FMC, you can no longer use t	ure Firewall Device Man netudes Device and Sha the device manager to n	ager (7.2+) red Config nanage it.
Management Cent	Management Cente 💿	NAT ID 💿	Threat Defense Hostn	DNS Server Group	Management Center/	Data Interface	
cisco-mex-ngfw-tac.app.us.ci	do		joroa-fdm-techzone.internal.cloudapp.n	CiscoUmbrellaDNSServerGroup ~	💿 Data 🕥 Management	Select Data Interface	ų.

登録するデバイス名を更新します。

### この操作の後、前述のフィールドのIDが表示されます。



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

Firewall Migration Tool (Version 6.0.	.1)						
	Extract FDM information Select	2 3 t Target Map FTD Interface Map St		6 7 Push Shared Config To Move Manager	8 9 Review & Validate Complete Migration		
	Note: Steps 7,8 and 9 should be c	arried out in a maintenance wi	indow.	PNG	(Davide Conrig)		
Move Manager					Source: Cisco Se Selected Migration:	cure Firewall Device Mana Includes Device and Share	ger (7.2+) ed Config
Update Detail This step is mandatory and Management Cent	s should be performed during a do Management Cente ①	wntime window. After you reg NAT ID 💿	ister the device with the ma Threat Defense Hostn	DNS Server Group	red FMC, you can no longer use Management Center/	o the device manager to ma Data Interface	anage it.
cierce us ofe	400 VEROW	1045 3486	tón à rura	Ciscol ImbrelleDNSServerOrous		Select Data Interface	
100.00 00.000.						/	

管理センターIDとNAT ID。

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

	1(						
	Extract FDM Information Select	2 3 ct Target Map FTD Interface	4 5 Map Security Zones & Review & Vi Interface Groups (Shared Co	6 7 Idate Push Shand Confg To Move Manager rfg) FMC	8 9 Review & Validate Complete Migration (Device Config)		
Not	te: Steps 7,8 and 9 should be o	carried out in a maintenar	nce window.				
Move Manager					Source: Cisco Se Selected Migration:		iger (7.2+) ed Config
Update Details	)		SYNCING the F	DM Device			
Management Cent	Management Cente 🕕	NAT ID ()	9% Com	la denve	Management Center/	Data Interface	anage it.
cisco us.cdo o	guq I66GW.	104	PMV fdm-Azure	CiscoUmbrellaDNSServerGroup ~	Data Management	Select Data Interface	~

FDMデバイスの同期

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

ewall Migration Tool (	(Versio	on 6.0.1)				
		1     2 Extract FDM Information Select Targ	et Map FTD Interface Map Security Zones & Review Interface Oroups (Dhared	6 7 5 Valdate Push Shared Config To Move Manager Config) FMC	9 Review & Validate Complete Migration (Device Config)	
		Note: Steps 7,8 and 9 should be carri	ed out in a maintenance window.			
Optim	nize, R	eview and Validate Device Co	onfiguration Page 💿		Source: Cisco S Selected Migratio	ecure Firewall Device Manager (7.2+ n: Includes Device and Shared Confid
		Objects NAT Interfaces Routes Site	-to-Site VPN Tunnels 👩 Remote Access VPN	SNMP DHCP		
Static	PPPoE					
Sele	ect all 2 entr	ries Selected: 0 / 2			Q :	Search
•	*	Interface Q	Zone Q	IP Address	State	
	1	GigabitEthernet0/0	outside_zone		Enabled	
0	2	GigabitEthernet0/1	inside_zone	45.1	Enabled	
1 to 2 of 2  4 4 Page 1	1_ of 1 ≯	+ H				

FDM構成設定の検証

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

lidation Summary (Pre-pu	(der	Successfully Validated		
Not selected for migration	Not selected for migration	2	1	1
		Logical Interfaces	Routes	DHCP
			(Static Routes, ECMP)	(Server, Relay, DDNS)
	0	0		
	Platform Settings	Malware & File Policy		

検証ステータス:プッシュ設定。

プッシュ率の構成を示すポップアップウィンドウ。

Firewall Migratio	on Tool (Version 6.0	0.1)				
		Extract FDM Information Note: Steps 7,8 and 9 should I	2 Select Target Map FTD	PUSHING 10% Complete Push to Cloud-delivered FMC is In progress. Please waif for antie rush process to complete the micration	7) danager	B     Complete Migration     (Device Confg)
	Complete Migra Migration Status	tion				Source: Cisco Secure Firewall Device Manager (7.2+) Selected Migration: Includes Device and Shared Config
	Interfaces	0				
	Routes					
	Policy Assignment					
	Please download the Post-	Push migration report for a detailed	summary. Download R			

プッシュ率の完了

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

igration root (version (	3.0.1)				
	Extract FDM Information	2 3 m Select Target Map FTD Interfac	4 5 or Map Security Zones & Review & Validane Pri Interface Groups (Shared Config)	6 7 8 ah Shared Config To Move Manager Review & Valic PMC (Device Conf	Complete Migration
	Note: Steps 7,8 and 9 sho	uld be carried out in a mainter	nance window.		
Complete Mig	ration		_ ^ _		Source: Cisco Secure Firewall Device Manager (7.2+ Selected Migration: Includes Device and Shared Config
Migration Status					
Migration is cor Next Step - Log	nplete, policy is pushed to FMC. in to FMC to deploy the policy to	> FTD.			
Live Connect:					
Selected Context: Sing	gle Context Mode				
Migration Summary (P	ost Push)				
3			4		3
Access Control List	Lines		Network Objects		Access Control Policy Objects
					(Geo, Application, URL objects and Intrusion Rule Group)
		ard, Extended used in BGPY RAV/PINEIGRP)	2	1	(Geo, Application, URL objects and Intrusion Rule Orcup)
	gration	rd, Extended used in BORY RAVPNECORPy 2 rk Address Translation	2 Logical Interfaces	1 Routes	(Geo, Application, URL objects and Intrusion Rule Group)

完全移行

## 確認

FDMがcdFMCに正常に移行されたことを確認します。

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

-11-11- CISCO	Defense Orchestrat	or	Serv	vices					Q Searc	h 🖁	⊳,	۵.	≜0 0-	•
≡	Hide Menu										>	Cloue	d-Delivered FM	c
<b>A</b>	Dashboard		Q	Search by Device Name, IP Addre	is, or Serial N	umber				D	•	Version	20240514	
0	Multicloud Defense		FMC	Secure Connectors							-	Action	5	
	Inventory		-										Chack For Changes	
Con	iguration			"Auto onboard On-Prem FMCs from S	ecureX tenant*	setting is not enabled. Click her	e to enable settin	g.				ă 1	Deployment	
۲	Policies	>	1									•	Updates Workflows	
•	Objects	>	•	Name		Version	Devices	Туре	Status	Last Heartbeat		0	API Explorer	
-&-	VPN	>		Cloud-Delivered FMC		20240514	⊜ 3	Cloud-Delivered FMC	O Active	06/12/2024, 12:42:21		Manag	ement	
Ever	ts & Monitoring					7.2.7-build 500	⊜0	On-Prem FMC	A Unreachable			-	Devices	
\$r	Analytics	>											Policies	
٢	Change Log											0	Objects NAT	
(1)	Jobs											**	Site to Site VPN	
*	Tools & Services		Tools 8	& Services	Migrations							ø	Platform Settings	
奋	Settings	>	6 0	Dynamic Attributes Connector	Firewall	Migration Tool						System	n	
			≓ S	ecure Connectors	ASA to F	DM Migration								
			l ⊆ F	irewall Management Center 🗸	Migrate	FTD to cdFMC							Configuration Smart Licenses	
				ISA Templates								•	AMP Management	
			_									1 A	Audit	
												•	Cisco Cloud Events	

cdFMCに登録されているデバイス

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

Defense Orchestrator FMC / Devices / Secure Firewall Device Summ	nary Analysis Policies De	tvices Objects Integration	•	Return Home Deploy Q O 🌮 🌣 🚱 📕	<ul> <li>diale secure</li> </ul>
-fdm-Azure			Deployments	Upgrades Health O Tasks	+ Show Notifications
Cisco Firepower Threat Defense for Azure			20+ total	0 waiting 0 running 0 retrying 6 success 20+ failures	Q, Filter
Device Interfaces Inline Sets Routing	DHCP VTEP		Policy Deploym	ent	
			Policy Deploy	ment to -fdm-Azure. Applied successfully	1m 54s 🗙
General	/±∓	License			
Name:	-fdm-Azure	Performance Tier :	FTI O Health Policy		
Transfer Packets:	No	Essentials:	Apply Initial_ Health Policy ap	pplied successfully	1m 40s X
Troubleshoot:	Logs CLI Download	Export-Controlled Features:			
Mode:	Routed	Malware Defense:	<ul> <li>Discovery</li> </ul>		
Compliance Mode:	None	IPS:	-fdm-Azu	e - Discovery from the device is successful.	2m 10s ×
Performance Profile:	Default	Carrier:	<ul> <li>SETurnel</li> </ul>		
TLS Crypto Acceleration:	Disabled	URL:	-1dm-Azu	e - SFTunnel connection established successfully.	- X
		Secure Client Premier:			
Device Configuration:	Import 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 Snort 2		Policy: Initial_Health_Policy 202	3-06-29 17:28:08	Secondary Address:	
		Excluded:	None	Status:	0
				Manager Access Interface:	Management Interface
Inventory Details	c	Applied Policies	/	Advanced Settings	1
× ⅲ ◻ + ।					

cdFMC登録タスクが完了しました。

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

Defense Orchestrator Ana FMC / Device / Device Management Ana	alysis Policies	Devices Objects Integratio	n		•> Return Home Deploy	Q O 🚱 🌣 🛛 📕	✓ the secure
View By: Group	(0) • Normal (2)	Deployment Deploy (2)	Inerrado (0)	<ul> <li>Seed 2 (2)</li> </ul>			Migrate   Deployment History
Collage All	(0) Normai (3)	<ul> <li>Deployment Pending (3)</li> </ul>	upgrade (u)	• SHORE 3 (3)			Download Device List Report
Name		Model	Version	Chassis	Licenses	Access Control Policy	Auto RollBack
Ungrouped (3)							
- fdm-Azure Snort 3 N/A - Routed		FTDv for Azure	7.4.1	N/A	Essentials	None	«» /:

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

٤	Defense Orchestrator FMC / Policies / Access Control / Access Control	Analysis	Policies	Devices	Objects	Integration		+> Return Home	Deploy	۹	•	<b>6</b> 24	0		~	ababa cisco	SECURE
								Object Ma	inagement	Intr	usion	Netw	ork Ana	lysis Policy	DNS	Import	t/Export
																Ne	w Policy
	Access Control Policy		St	atus			Last Modified		Lock !	Status							
	Default Access Control Policy Default Access Control Policy with default action block		Targ	geting 0 devices			2024-06-11 22:28:19 Modified by "Firepower System"									ъ 🛛	11
	FTD-Mig-ACP-1718216278		Targ Up-	peting 1 devices to-date on all targe	eted devices		2024-06-12 12:18:00 Modified by									% B	11

移行ポリシー

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

Drow Unseed Orgects           Name         Yulue         Type         Override           any         0.00.00         Group         % Q < M           any-iprid         0.00.00         Network         % Q < M           any-iprid         103.104.73.155         Hest         % Q < M           findsa_Network_IP         112.22.2.1         Hest         % Z < M           invid-sectional         112.22.2.1         Hest         % Z < M           invid-sectional         192.168.192.10         Hest         % Z < M           invid-sectional         192.22.1         Hest         % Z < M           invid-sectional         192.168.192.10         Hest         % Z < M           invid-sectional         192.168.192.10         Hest         % Z < M           invid-sectional         192.48.0916         Network         % Q < M           invid-sectional         192.168.0916         Network         % Q < M     <	Network		Add Network	• Q, Fi	lter				
Name         Value         Type         Override           any         0.00.00         Group         Group         Group          Group	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, ar								
Name         Yatue         Type         Overside           any         0,000         Group         Gr									
any         요coup         Acoup         Acoup <th< td=""><td>Name</td><td>Value</td><td></td><td>Туре</td><td>Override</td><td></td></th<>	Name	Value		Туре	Override				
비가·iby4         0.0.0/0         Network         비 의 의 의 의           inv/·iby6         ::/0         Host         내 의 의 의 의           Banned         100.104.73.155         Host         내 기 의 의           Gw_stast01         172.22.1         Host         내 기 의           Inside_Network_IP         192.168.192.10         Host         내 기 의 의           IPv4-Benchmark-Tests         198.18.0.0/15         Network         내 의 의 의           IPv4-Link-Local         199.254.0.0/16         Network         내 의 의 교 의           IPv4-Private-100.0.0-8         100.0.0/8         Network         내 의 의 교 의           IPv4-Private-102.166.0-16         Network         내 의 의 교 의         내 의 의 교 의           IPv4-Private-102.166.0-16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0-16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0-16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0-16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0/16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0/16         Network         내 의 의 관         내 의 의 관           IPv4-Private-102.166.0.0/	any	0.0.0.0/0 ::/0		Group		唱く言め			
jay-ipy6         Hot         単々できき           Baned         103.104.73.155         Hot         ● マンマき           Gw_est01         172.22.2.1         Hot         ● マンマき           Inidde_Network_IP         192.168.192.10         Hot         ● マンマき           IPv4-Benchmark-Tests         198.180.0/15         Network         ● マンマき           IPv4-Muticast         198.180.0/16         Network         ● マンマき           IPv4-Muticast         100.0.0/8         Network         ● ママ き           IPv4-Phrate-100.0.0-8         100.0.0/8         Network         ● マ 章 き           IPv4-Phrate-122.168.0.0-12         172.168.0.0/12         Network         ● マ 章 き           IPv4-Phrate-192.168.0.0-16         192.168.0.0/16         Network         ● マ 章 き           IPv4-Phrate-All-RFC1918         100.0.0/96         Group         ● マ 章 き           IPv6-IPv4-Mapped         ::::::::::::::::::::::::::::::::::::	any-ipv4	0.0.0/0		Network		¶a (≣ #			
Banned         103.104.73.155         Hot         Image of the set of t	any-ipv6	::/0		Host		¶a,			
Gw_tes01         1722.2.1         Host         電子音音           Inside_Network_JP         192.168.192.10         Host         電子音音           IPv4-Benchmark-Tests         198.180.0/15         Network         電空音音           IPv4-Link-Local         169.254.0.0/16         Network         電空音音           IPv4-Multicat         169.254.0.0/16         Network         電空音音           IPv4-Private-102.06.0-8         10.0.0.0/8         Network         電空音音           IPv4-Private-102.168.0.0-12         Network         電空音音           IPv4-Private-192.168.0.0-16         122.168.0.0/16         Network         電空音音           IPv4-Private-AII-RFC1918         10.00.0/96         Scoop         電空音者           IPv4-Private-AII-RFC1918         10.00.0/96         Scoop         電空音者	Banned	103.104.73.155		Host	•	喧/膏丝			
Inside_Network_IP         192.188.192.10         Host         电子子格           IPV4-Benchmark-Tests         198.18.0.0/15         Network         唱 오 달 格           IPV4-Link-Local         199.284.0.0/16         Network         唱 오 달 格           IPV4-Link-Local         199.240.0/16         Network         唱 오 달 格           IPV4-Multicast         224.0.0/16         Network         唱 오 달 格           IPV4-Private-100.0.0-8         10.0.0/8         Network         唱 오 달 格           IPV4-Private-102.160.0-12         Network         唱 오 달 格           IPV4-Private-192.168.0.0-16         192.168.0/16         Network         唱 오 달 格           IPV4-Private-All-RFC1918         192.168.0/16         Network         唱 오 달 格           IPV4-Private-All-RFC1918         192.080.0/16         Network         唱 오 달 格           IPV6-IPV-Abapped         ::::::::::::::::::::::::::::::::::::	Gw_test01	172.22.2.1		Host		┗/〒め			
IPv4-Benchmark-Tests         198.8.0/15         Network         唱 오 급 용           IPv4-Link-Local         169.254.0/16         Network         唱 오 급 용           IPv4-Link-Local         169.254.0/16         Network         唱 오 급 용           IPv4-Multicoat         224.0.0/4         Network         唱 오 급 용           IPv4-Private-102.06-8         10.0.0/8         Network         唱 오 급 용           IPv4-Private-102.168.0.0-12         Network         唱 오 급 용           IPv4-Private-192.168.0.0-16         Network         唱 오 급 용           IPv4-Private-AII-RFC1918         100.00/8         Network         唱 오 급 용           IPv6-IPv4-AII-RFC1918         100.00/96         Group         唱 오 급 용           IPv6-IPv4-Mapped         ::tttt0.0.0/96         Network         唱 오 급 용	Inside_Network_IP	192.168.192.10		Host	0	唱/頁线			
IPv4-Lnk-Local         169 254.0.0/16         Network         Imp          Imp <t< td=""><td>IPv4-Benchmark-Tests</td><td>198.18.0.0/15</td><td></td><td>Network</td><td></td><td>¶a, ≣ #</td></t<>	IPv4-Benchmark-Tests	198.18.0.0/15		Network		¶a, ≣ #			
IPv4-Multicast         224 0.0/4         Network         Image 8           IPv4-Private-10.0.0.0-8         10.0.0/8         Network         Image 8           IPv4-Private-102.06.0-12         12.16.0.0/12         Network         Image 8           IPv4-Private-192.168.0.0-16         192.168.0.0/16         Network         Image 8           IPv4-Private-192.168.0.0-16         192.168.0.0/16         Network         Image 8           IPv4-Private-All-RFC1918         100.00/8         Network         Image 8           IPv6-IPv4-Mapped         ::::::::::::::::::::::::::::::::::::	IPv4-Link-Local	169.254.0.0/16		Network		¶∎ Q ⊕ M			
IPv4-Private-102.06.0-13         Network         唱 오 급 용           IPv4-Private-172.16.0.0-12         172.16.0.0/12         Network         唱 오 급 용           IPv4-Private-192.168.0.0-16         192.168.0.0/16         Network         唱 오 급 용           IPv4-Private-AII-RFC1918         190.00/8         Recupit         매 오 급 용           IPv6-IPv4-AII-RFC1918         100.00/8         Group         唱 오 급 용           IPv6-IPv4-Mapped         ::ttt0.0.0/96         Network         唱 오 급 용	IPv4-Multicast	224.0.0.0/4		Network		¶a Q ⊕ M			
IPv4-Private-122.160.0-12         Network         吸 管路           IPv4-Private-192.168.0.0-16         192.168.0.0/16         Network         吸 管路           IPv4-Private-AII-RFC1918         192.168.0.0/16         Group         吸 管路           IPv4-Private-AII-RFC1918         172.160.0/12         Group         吸 管路           IPv6-IPv4-Mapped         ::mt10.0.0/96         Network         吸 管路	IPv4-Private-10.0.0.0-8	10.0.0/8		Network		¶∎ Q 🗑 M			
IPv4-Private-192.168.0.0-16         192.168.0.0/16         Network         吸 只 前           IPv4-Private-192.168.0.0-16         10.0.0.0/8 172.160.0/12 192.188.0/16         Group         吸 可 動           IPv6-IPv4-Mapped         :fff:0.0.0/96         Network         吸 只 前	IPv4-Private-172.16.0.0-12	172.16.0.0/12		Network		¶a q ≣ M			
IPv4-Private-All-RFC1918         10.0.0.0/8 172,168.0.0/16         Group         팀 Q 을 용           IPv6-IPv4-Mapped         :::mft:0.0.0/96         Network         팀 Q 을 용	IPv4-Private-192.168.0.0-16	192.168.0.0/16		Network		¶∎ Q ≣ M			
IPv6-IPv4-Mapped ∷fff:0.0.0.0/96 Network 🖬 🤉 🗑 🚸	IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16		Group		¶∎ Q ≣ #8			
	IPv6-IPv4-Mapped	::fff:0.0.0.0/96		Network		¶∎ Q ≣ M			

FDMからcdFMCに移行されたオブジェクト

### オブジェクト管理インターフェイスが移行されました。

FMC / Objects / Object Mar	Of Analysis Policies Devices Objects Integration	*> Retur	n Home Deploy Q 💿 🌮 🌣 🔞 🗾	✓ dode SECUR
> AAA Server	Interface		Add • C. Filter	
Access List     Address Pools	Interface objects segment your network to help you manage and classify traffic flow. An i	nterface object simply groups interfaces. These groups may span m	ultiple devices; you can also configure multiple interface obje	cts on a single device.
Application Filters				
AS Path BFD Template	Name A	Туре	Interface Type	15.0
Cipher Suite List	v 424 inside_lg	Interface Group	Routed	/ • *
DHCP IPv6 Pool	> aster - fdm - Azure		a const	
<ul> <li>Distinguished Name</li> <li>DNS Server Group</li> </ul>	<ul> <li>inside_zone</li> </ul>	Security Zone	Routed	/ .
> External Attributes	>		Provide Sector S	/ = H
> FlexConfig		inwriada Group	Rocera	× • • • •
Geolocation Interface		Casulty Zona	Deviled	/ E #
Key Chain		oavany zona	NAMES .	× • 00
> PKI	A sector formation a			

オブジェクト管理インターフェイスが移行されました。

翻訳について

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