

Migration von FDM zu cdFMC mit FMT innerhalb von CDO

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Überprüfung](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen FirePOWER Device Manager (FDM) mithilfe des FirePOWER Migration Tools (FMT) in CDO zu Cloud-gestütztem FMC (cdFMC) migrieren.

Voraussetzungen

Anforderungen

- FirePOWER Device Manager (FDM) 7.2+
- Cloud-bereitgestelltes Firewall Management Center (cdFMC)
- FirePOWER Migration Tool (FMT) im CDO enthalten

Verwendete Komponenten

Dieses Dokument wurde auf der Grundlage der oben genannten Anforderungen erstellt.

- Firepower Device Manager (FDM) auf Version 7.4.1
- Cloud-bereitgestelltes Firewall Management Center (cdFMC)
- Cloud Defense Orchestrator (CDO)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

CDO-Administrator-Benutzer können Migrationen ihrer Geräte auf cdFMC durchführen, wenn die

Geräte auf Version 7.2 oder höher sind. Bei der in diesem Dokument beschriebenen Migration ist cdFMC auf dem CDO Tenant bereits aktiviert.

Konfigurieren

1.- Unterstützung von Cisco Cloud Services auf FDM

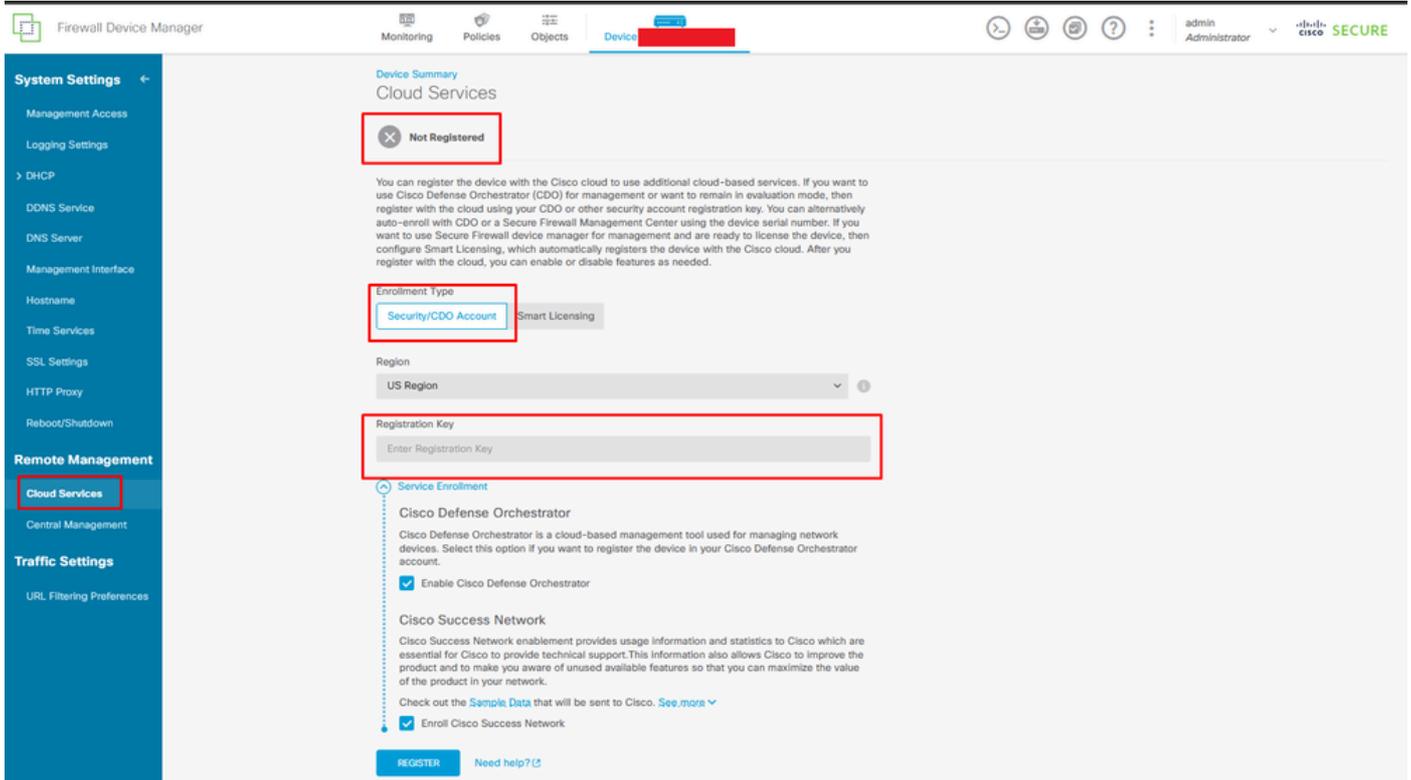
Um mit der Migration zu beginnen, muss das FDM-Gerät ohne ausstehende Bereitstellungen konfiguriert sein und sich für Cloud-Services registrieren. Um sich für Cloud-Services zu registrieren, navigieren Sie zu Systemeinstellungen > Weitere Informationen > Cloud-Services.

Im Bereich Cloud-Services ist das Gerät nicht registriert. Aus diesem Grund muss die Registrierung über den Typ Security/CDO-Konto erfolgen. Sie müssen einen Registrierungsschlüssel konfigurieren und anschließend registrieren.

The screenshot shows the Cisco Firepower Threat Defense (FTD) configuration interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device'. The main content area displays a network diagram with 'Inside Network', 'Cisco Firepower Threat Defense for Azure', and 'ISP/WAN/Gateway' components. Below the diagram is a grid of configuration tiles: 'Interfaces' (Management: Unmerged, Enabled 2 of 2), 'Smart License' (Registered, Tier: FTDv20 - 3 Gbps), 'Site-to-Site VPN' (There are no connections yet), 'Routing' (1 static route), 'Backup and Restore', 'Remote Access VPN' (Requires Secure Client License, No connections | 1 Group Policy), 'Updates' (Geolocation, Rule, VDB, System Upgrade, Security Intelligence Feeds), 'Troubleshoot' (No files created yet), 'Advanced Configuration' (Includes: FlexConfig, Smart CLI), 'System Settings' (Management Access, Logging Settings, SSL Settings, Cloud Services, HTTP Proxy, Reboot/Shutdown, Central Management, URL Filtering Preferences), and 'Device Administration' (Audit Events, Deployment History, Download Configuration). A dropdown menu is open over the 'System Settings' tile, highlighting 'Cloud Services'.

Registrierung Cloud-Services

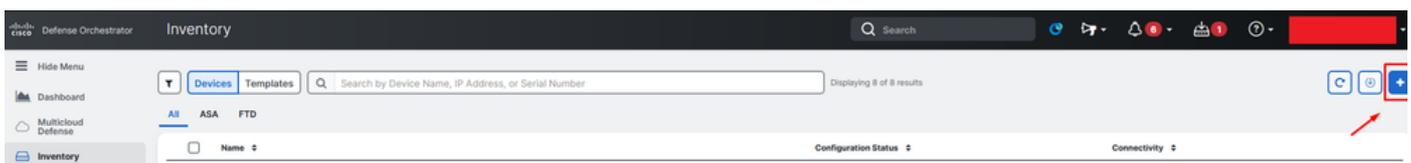
Über Cloud-Services wird angezeigt, dass nicht registriert ist. Wählen Sie den CDO-Kontoregistrierungstyp aus, und geben Sie den Registrierungsschlüssel von CDO an.



Registrierung für Cloud-Services

Der Registrierungsschlüssel befindet sich im CDO. Navigieren Sie zu CDO, und gehen Sie zu Bestand > Symbol hinzufügen.

Ein Menü wird angezeigt, in dem Sie den Gerätetyp auswählen können. Wählen Sie die FTD-Option aus. Sie müssen die FDM-Option aktivieren. Andernfalls kann die entsprechende Migration nicht durchgeführt werden. Bei der Art der Registrierung wird der Registrierungsschlüssel verwendet. Bei dieser Option wird der Registrierungsschlüssel in Schritt 3 angezeigt, den Sie kopieren und in den FDM einfügen müssen.



Integriertes FDM, Option hinzufügen

Es wird ein Menü angezeigt, in dem Sie ein Gerät oder einen Servicetyp auswählen können.

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

Gerät oder Servicetyp auswählen

Für dieses Dokument wurde Registrierungsschlüssel auswählen ausgewählt.

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.

Registrierungstyp

Hier wird der im vorherigen Schritt erforderliche Registrierungsschlüssel angezeigt.

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

Registrierungsprozess

Wenn Sie den Registrierungsschlüssel erhalten haben, kopieren Sie ihn, fügen Sie ihn in den FDM ein, und klicken Sie auf Registrieren. Nach der Registrierung des FDM bei Cloud Services wird er wie im Bild gezeigt als Aktiviert angezeigt.

Die Smart License wurde übersprungen, da das Gerät registriert wird, sobald es betriebsbereit ist.

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-Registrierung

Bei der FDM-Registrierung werden Tenancy, verbundene und registrierte Cloud-Services angezeigt.

Monitoring Policies Objects Device: [REDACTED]

admin Administrator

Device Summary
Cloud Services

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

Cisco Defense Orchestrator
 Enabled
 Note: If the device is registered to cloud services using Smart Licensing, the device will not work with CDO. Please [register](#) the device and re-on-board using the registration key method with the "Security/CDO account" option.
 Cisco Defense Orchestrator allows you to configure multiple devices of different types from a cloud-based configuration portal, allowing deployment across your network.

Cisco Success Network
 Enabled
 Cisco Success Network enablement provides usage information and statistics to Cisco which are essential for Cisco to provide technical support. This information also allows Cisco to improve the product and to make you aware of unused available features so that you can maximize the value of the product in your network. Check out the [Sample Data](#) that will be sent to Cisco.

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

FDM-Registrierung abgeschlossen

In CDO befindet sich der FDM im Menü "Inventory" (Bestand) und wird nun integriert und synchronisiert. Fortschritt und Ablauf dieser Synchronisation können im Abschnitt Workflows überprüft werden.

Sobald dieser Prozess abgeschlossen ist, wird er als Synchronisiert und Online angezeigt.

Defense Orchestrator Inventory

Hide Menu
 Dashboard
 Multicloud Defense
 Inventory
 Configuration
 Policies
 Objects
 VPN
 Events & Monitoring
 Analytics
 Change Log
 Jobs
 Tools & Services
 Settings

Devices Templates
 Search by Device Name, IP Address, or Serial Number
 Displaying 9 of 9 results

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

Device Details
 Model: Cisco Firepower Threat Defense for Azure
 Serial: [REDACTED]
 Version: 7.4.1-172
 Onboarding Method: Registration Key
 Smart Version: 3.15.3.100-56

Syncing
 CDO is communicating with your device. Please check back in a moment.

Device Actions
 API Tool
 Workflows
 Manage Backups
 Remove

Management
 Notes
 Changelog
 Executive Report

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

Label Groups and Labels
 Add Labels

CDO-Bestand - FDM-integriert

Wenn die Geräte synchronisiert wurden, wird dies als "Online" und "Synchronisiert" angezeigt.



Integrierte FDM

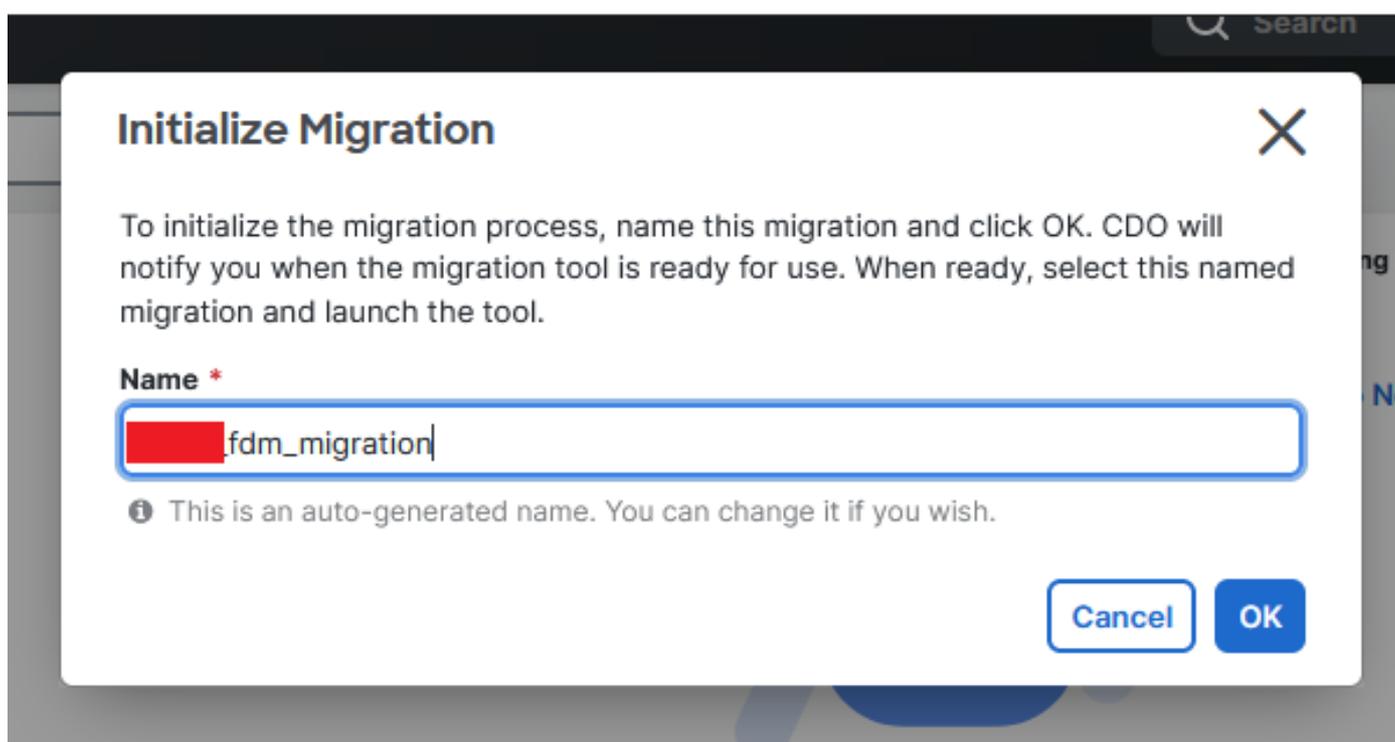
Wenn der FDM erfolgreich in CDO integriert wurde, müssen wir uns vom FDM abmelden. Navigieren Sie nach dem Abmelden vom FDM in CDO zu Tools & Services > Migration > Firewall Migration Tool.



Klicken Sie auf das Symbol Hinzufügen, um einen zufälligen Namen anzuzeigen, der angibt, dass der Name umbenannt werden muss, um den Migrationsprozess zu starten.

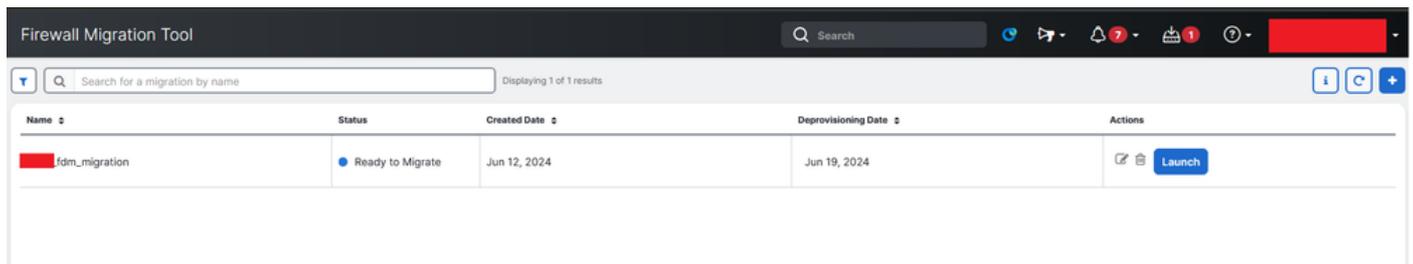


Nach der Umbenennung klicken Sie auf Starten, um die Migration zu starten.



Migration initialisieren

Klicken Sie auf Starten, um die Migrationskonfiguration zu starten.



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

Startprozess der Migration

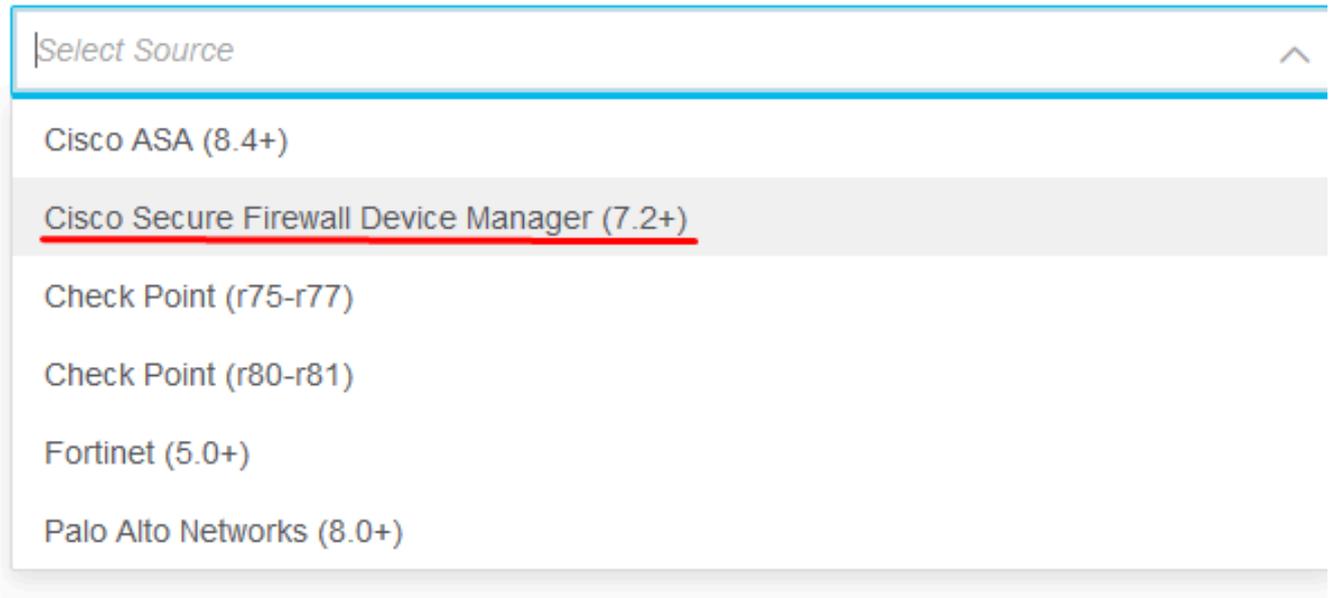
Wenn Sie auf Starten klicken, öffnet sich ein Fenster für den Migrationsprozess, in dem die Option Cisco Secure Firewall Device Manager (7.2+) ausgewählt ist. Wie bereits erwähnt, ist diese Option ab Version 7.2 aktiviert.



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 Quellkonfiguration auswählen

Nach der Auswahl werden drei verschiedene Migrationsoptionen angezeigt: Nur gemeinsam genutzte Konfiguration, Einschließlich Geräte- und gemeinsam genutzter Konfigurationen und Einschließlich Geräte- und gemeinsam genutzter Konfigurationen für neue FTD-Hardware.

Für diese Instanz wird die zweite Option "Migrate FirePOWER Device Manager (Includes Device & Shared Configuration)" ausgeführt.

How would you like to migrate from Firepower Device Manager :



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

Migrate Firepower Device Manager (Shared Configurations Only) >

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

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

Migrationsoptionen

Fahren Sie nach Auswahl der Migrationsmethode mit der Auswahl des Geräts aus der Liste fort.

Live Connect to FDM

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

Select FDM Managed Device

fdm - Available

Connect

Auswahl von FDM-Geräten

FDM device config extraction successful



100% Complete

Konfigurationsextraktion abgeschlossen

Es wird empfohlen, die Registerkarte oben zu öffnen, um zu überprüfen und zu verstehen, in welchem Schritt das Gerät ausgewählt wurde.

1 Extract FDM Information 2 Select Target 3 Map FTD Interface 4 Map Security Zones & Interface Groups 5 Review & Validate (Shared Config) 6 Push Shared Config To FMC 7 Move Manager 8 Review & Validate (Device Config) 9 Complete Migration

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

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 v

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPN/IGRP)	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

Schritte für den Migrationsprozess

Wählen Sie als neue Migration Abbrechen, wenn Sie mit der Option "Möchten Sie eine vorhandene Zugriffskontrollrichtlinie, NAT oder RAVPN-Richtlinie auf FMC verwenden?" aufgefordert werden.

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

Yes No

Save Cancel

Abbrechen-Option für vorhandene Konfiguration

Anschließend stehen Optionen zur Auswahl der zu migrierenden Funktionen zur Verfügung, wie im Bild dargestellt. Klicken Sie auf Fortfahren.



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.

Zu wählende Funktionen

Anschließend Konvertierung starten.

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

Konvertierung starten.

Nach Abschluss des Analyseprozesses können Sie zwei Optionen nutzen: Laden Sie das Dokument herunter und setzen Sie die Migration fort, indem Sie auf Weiter klicken.

Select Target

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

Firewall Management - Cloud-delivered FMC

Select Features

Rule Conversion/ Process Config

Start Conversion

No parsing error found. Refer to the pre-migration report for more details.

Please download the Pre-Migration report for a detailed summary of the parsed configuration.

Download Report

3 Access Control List Lines	0 Access List Objects (Standard, Extended used in BGP/ RAVPN/EGRP)	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, DNS)
0 Site-to-Site VPN Tunnels	0 Remote Access VPN (Connection Profiles)			

Back

Next

Bericht herunterladen

Die Geräteschnittstellen sind so eingestellt, dass sie angezeigt werden. Es wird empfohlen, auf Aktualisieren zu klicken, um die Schnittstellen zu aktualisieren. Klicken Sie nach der Validierung auf Weiter.



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

Map FTD Interface

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

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

Angezeigte Schnittstellen

Navigieren Sie zum Abschnitt Sicherheitszonen und Schnittstellengruppen, wo Sie SZ und IG

manuell hinzufügen müssen. Für dieses Beispiel wurde Auto-Create ausgewählt. Auf diese Weise können die Schnittstellen innerhalb des FMC, zu denen Sie migrieren, automatisch generiert werden. Klicken Sie anschließend auf die Schaltfläche Weiter.

Firewall Migration Tool (Version 6.0.1)

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

Map Security Zones and Interface Groups

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

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

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

Sicherheitszonen und Schnittstellengruppen

Bei der Option "Auto-Create" (Automatisch erstellen) werden FDM-Schnittstellen vorhandenen FTD-Sicherheitszonen und Schnittstellengruppen im FMC zugeordnet, die denselben Namen haben.

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

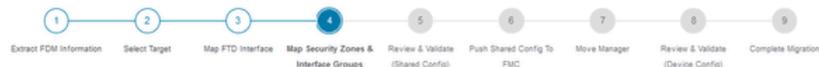
Cancel

Auto-Create

Option zum automatischen Erstellen.

Wählen Sie dann Weiter aus.

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_jg (A) <input type="button" value="v"/>
inside	inside_zone	GigabitEthernet0/1	inside_zone (A)	inside_jg (A) <input type="button" value="v"/>

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 PDF PAGE 2 Page 1 of 1

Back Next

Nach der automatischen Erstellung.

Nehmen Sie sich in Schritt 5, wie in der oberen Leiste gezeigt, die Zeit, die Zugriffskontrollrichtlinien (ACP), Objekte und NAT-Regeln zu überprüfen. Überprüfen Sie die einzelnen Elemente sorgfältig, und klicken Sie dann auf Validieren, um sicherzustellen, dass keine Probleme mit Namen oder Konfigurationen vorliegen.

Firewall Migration Tool (Version 6.0.1)

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

Optimize, Review and Validate Shared Configuration Only

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

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 Done Search

#	Name	Validation State	Type	Value
1	OutsidePv4Gateway	Validation pending	Network Object	172.18.1.1
2	OutsidePv4DefauRoute	Validation pending	Network Object	0.0.0.0/0
3	Banned	Validation pending	Network Object	103.104.73.155

Page 1 to 3 of 3 | Page 1 of 1

Validate

Zugriffskontrolle, Objekte und NAT-Konfigurationen

Push nur für freigegebene Konfiguration

Validation Status

Successfully Validated

Validation Summary (Pre-push)

3 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EGRP)	4 Network Objects	Not selected for migration Port Objects	3 Access Control Policy Objects (Geo, Application, URL objects and Intrusion Rule Group)
2 Network Address Translation	Not selected for migration Remote Access VPN (Connection Profiles)			

Push Shared Configuration Only

Nur gemeinsam genutzte Konfiguration Push

Der Prozentsatz des Abschlusses und die spezifische Aufgabe, die bearbeitet wird, können beobachtet werden.

Firewall Migration Tool (Version 6.0.1)

Push Shared Config to FMC

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

PUSHING
24% Complete
Push to Cloud-delivered FMC is in progress. Please wait for entire push process to complete the migration.

Migration Status	
Network Objects	✓
Network Address Translation	✓
Access Control Policies	✓
Policy Assignment	✓

Please download the Post-Push migration report for a detailed summary. [Download Report](#)

Push-Prozentsatz

Fahren Sie nach Abschluss von Schritt 5 mit Schritt 6 fort, wie in der oberen Leiste dargestellt, wo der Push Shared Configuration to FMC stattfindet. Klicken Sie nun auf die Schaltfläche Weiter, um fortzufahren.

Firewall Migration Tool (Version 6.0.1)

1 Extract FDM Information 2 Select Target 3 Map FTD Interface 4 Map Security Zones & Interface Groups 5 Review & Validate (Shared Config) 6 **Push Shared Config to FMC** 7 Move Manager 8 Review & Validate (Device Config) 9 Complete Migration

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

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

Push Shared Config to FMC

Migration Status

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

Live Connect:
Selected Context: Single Context Mode

Migration Summary (Post Push)

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

[Next](#)

Push der freigegebenen Konfiguration an FMC abgeschlossen

Diese Option löst eine Bestätigungsmeldung aus und fordert Sie auf, die Migration des Managers fortzusetzen.

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

Verschieben-Manager bestätigen

Um die Manager-Migration fortzusetzen, ist es erforderlich, über die Management Center-ID und die NAT-ID zu verfügen. Dies ist äußerst wichtig. Diese IDs können durch Auswahl von Update Details (Details aktualisieren) abgerufen werden. Durch diese Aktion wird ein Popup-Fenster mit dem gewünschten Namen für die FDM-Darstellung im cdFMC geöffnet, in dem die Änderungen gespeichert werden.



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

Manager Center-ID und NAT-ID

Gerätename für Registrierung aktualisieren.

Nach diesem Vorgang werden die IDs für die oben genannten Felder angezeigt.



Warnung: Nehmen Sie keine Änderungen an der Management Center-Schnittstelle vor. Standardmäßig ist die Option "Management" ausgewählt. Lassen Sie diese Option als Standardeinstellung unverändert.



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...	ogp	166GW/ 104v	26PM/	fdm-Azure	CiscoUmbrellaDNSServerGroup
						<input checked="" type="radio"/> Data <input type="radio"/> Management
						Select Data interface

Save

Move Manager

Management Center-ID und NAT-ID

Nachdem Sie die Option Update Details (Details aktualisieren) ausgewählt haben, beginnt das Gerät mit der Synchronisierung.

on Tool (Version 6.0.1)

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

Move Manager

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.

SYNCING the FDM Device

9% Complete

Management Cent...	Management Cente...	NAT ID	Threat Defense Hostn...	DNS Server Group	Management Center/ ...	Data Interface
cisco	us.cdo...	ogp	166GW/ 104v	26PM/	fdm-Azure	CiscoUmbrellaDNSServerGroup
						<input checked="" type="radio"/> Data <input type="radio"/> Management
						Select Data interface

Save

FDM-Gerät wird synchronisiert

Nach Abschluss der Migration müssen im nächsten Schritt die im FDM konfigurierten Schnittstellen, Routen und DHCP-Einstellungen überprüft werden. Wählen Sie dazu Validieren.



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

#	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



Überprüfen der FDM-Konfigurationseinstellungen

Wählen Sie nach der Validierung Push Configuration aus, um den Push-Prozess für die Konfiguration zu initiieren. Dieser Vorgang wird fortgesetzt, bis die Migration abgeschlossen ist. Zusätzlich ist es möglich, die ausgeführten Tasks zu überwachen.

Validation Status

✔ Successfully Validated

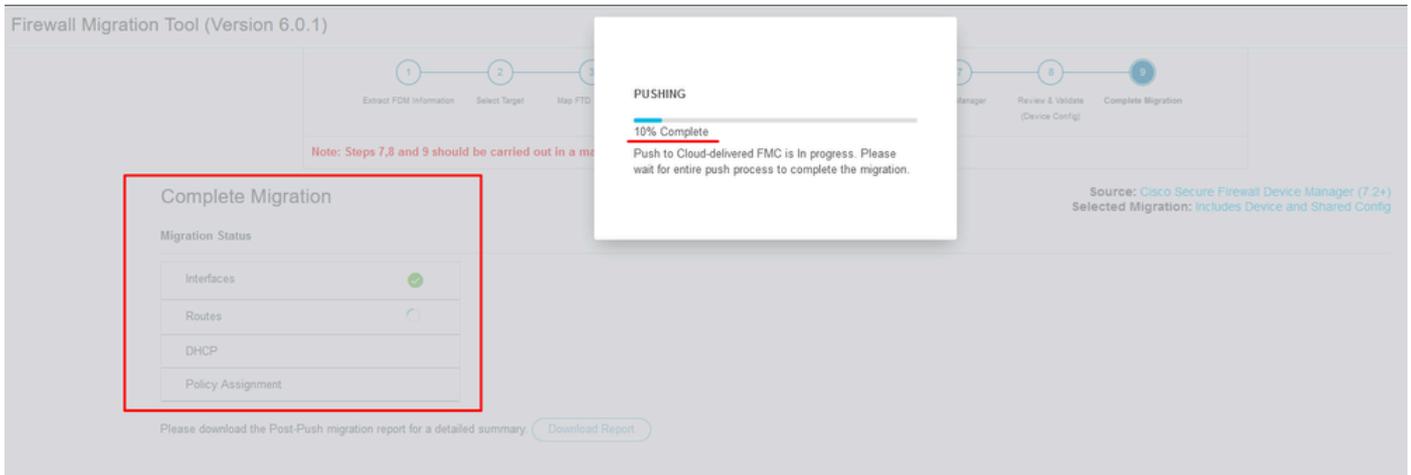
Validation Summary (Pre-push)

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

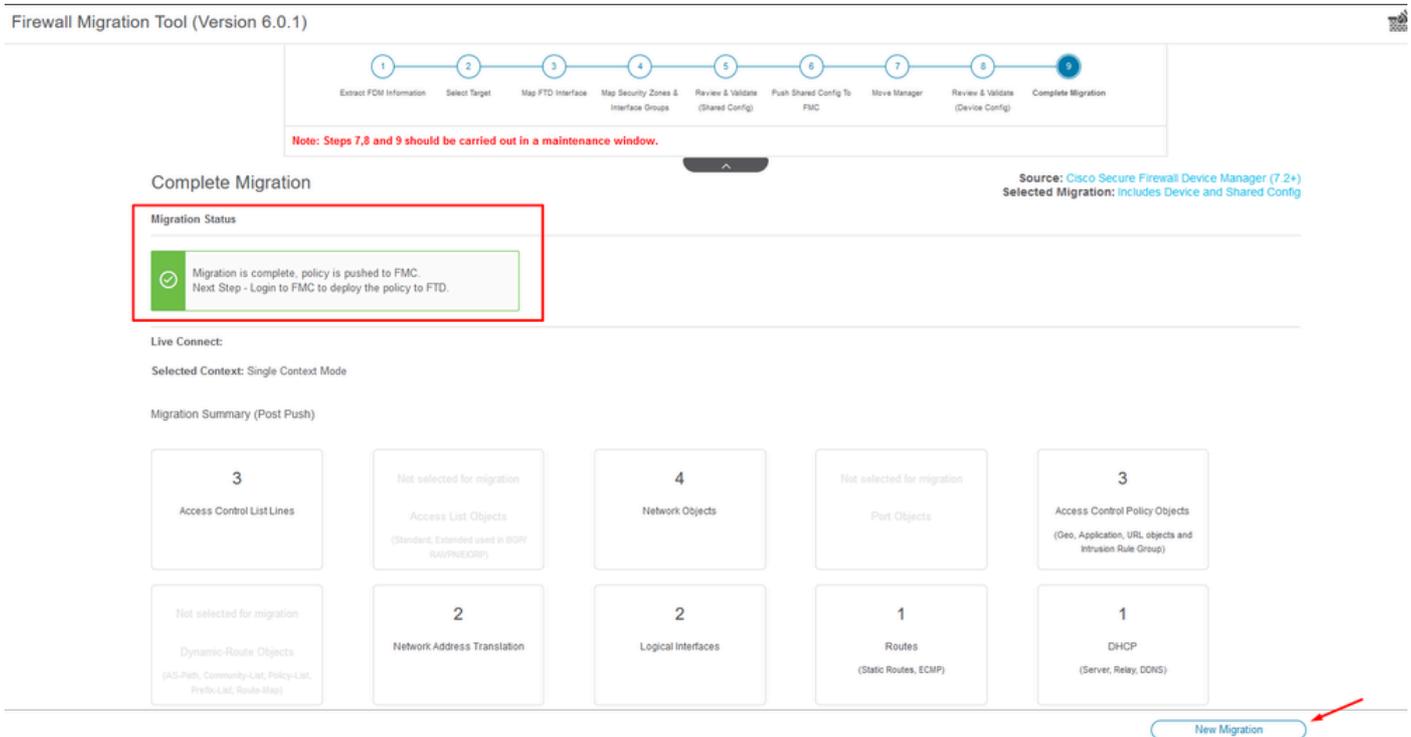
Validierungsstatus - Push-Konfiguration.

Popup-Fenster mit der prozentualen Push-Konfiguration.



Verschiebeprozentsatz abgeschlossen

Nach Abschluss der Migration wird eine Option zur Initiierung einer neuen Migration vorgestellt, die das Ende des Migrationsprozesses von FDM zu cdFMC markiert.

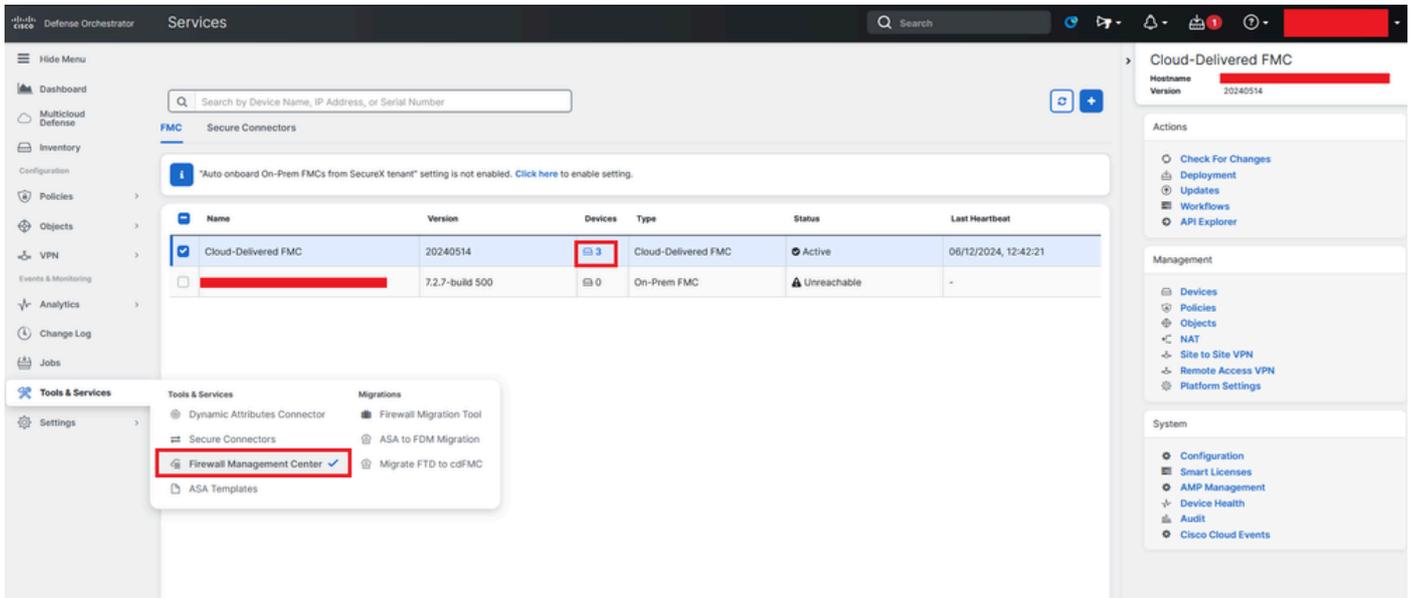


Vollständige Migration

Überprüfung

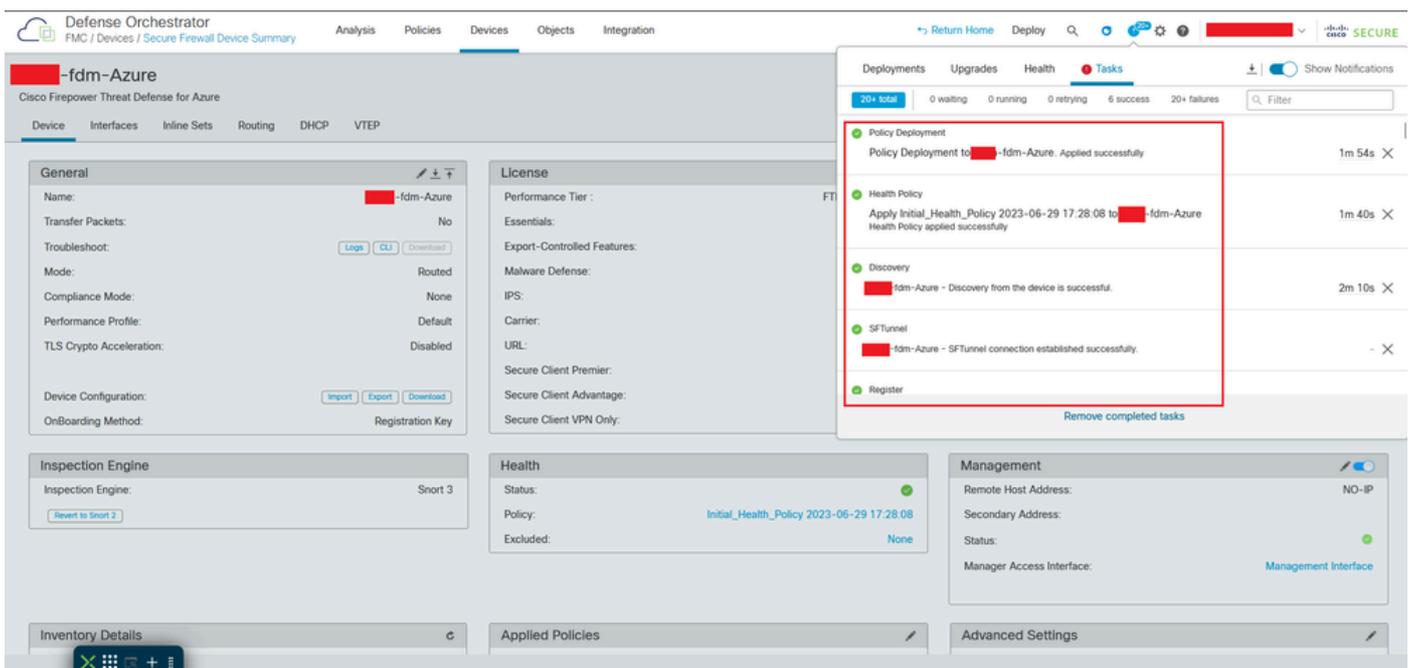
Überprüft, ob der FDM erfolgreich zum cdFMC migriert wurde.

Navigieren Sie zu CDO > Tools & Services > FirePOWER Management Center. Dort haben Sie festgestellt, dass die Anzahl der registrierten Geräte gestiegen ist.



Registrierte cdFMC-Geräte

Überprüfen Sie das Gerät unter Devices (Geräte) > Device Management (Gerätmanagement). Darüber hinaus können Sie in den Aufgaben des FMC feststellen, wann das Gerät erfolgreich registriert und die erste Bereitstellung erfolgreich abgeschlossen wurde.



Die cdFMC-Registrierungsaufgabe wurde abgeschlossen.

Gerät ist auf cdFMC > Gerät > Gerätmanagement.

Defense Orchestrator
FMC / Devices / Device Management

Analysis Policies Devices Objects Integration

Return Home Deploy Search Settings User Profile Cisco Secure

View By: Group

All (3) Error (0) Warning (0) Offline (0) Normal (3) Deployment Pending (3) Upgrade (0) Short 3 (3)

Search Device Add

Download Device List Report

Name	Model	Version	Chassis	Licenses	Access Control Policy	Auto Rollback
Ungrouped (3)						
fdm-Azure N/A - Routed	FTDv for Azure	7.4.1	N/A	Essentials	None	

Auf cdFMC registriertes Gerät

Die Zugriffskontrollrichtlinie wurde unter Richtlinien > Zugriffskontrolle migriert.

Defense Orchestrator
FMC / Policies / Access Control / Access Control

Analysis Policies Devices Objects Integration

Return Home Deploy Search Settings User Profile Cisco Secure

Object Management | Intrusion | Network Analysis Policy | DNS | Import/Export

New Policy

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

Migrationsrichtlinie

Ebenso können Sie die im FDM erstellten Objekte überprüfen, die korrekt zum cdFMC migriert wurden.

Network

Add Network Filter

Show Unused Objects

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

Name	Value	Type	Override
any	0.0.0.0/0 :::0	Group	
any-ipv4	0.0.0.0/0	Network	
any-ipv6	:::0	Host	
Banned	103.104.73.155	Host	✔
Gw_test01	172.22.2.1	Host	
Inside_Network_IP	192.168.192.10	Host	✔
IPv4-Benchmark-Tests	198.18.0.0/15	Network	
IPv4-Link-Local	169.254.0.0/16	Network	
IPv4-Multicast	224.0.0.0/4	Network	
IPv4-Private-10.0.0.0-8	10.0.0.0/8	Network	
IPv4-Private-172.16.0.0-12	172.16.0.0/12	Network	
IPv4-Private-192.168.0.0-16	192.168.0.0/16	Network	
IPv4-Private-All-RFC1918	10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	Group	
IPv6-IPv4-Mapped	:::ffff:0.0.0.0/96	Network	

Objekte von FDM auf cdFMC migriert

Objektverwaltungsschnittstellen migriert.

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_jg	Interface Group	Routed	
> fdm-Azure			
inside_zone	Security Zone	Routed	
> fdm-Azure			
outside_jg	Interface Group	Routed	
> fdm-Azure			
outside_zone	Security Zone	Routed	
> fdm-Azure			

Objektverwaltungsschnittstellen migriert.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.