

Migration von FDM zu FMC über FMT mit der Datei "Configuration.zip"

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Überlegungen](#)

[Konfiguration](#)

[API-Anfragen - Post](#)

[Firewall Migration-Tool](#)

[FMC-Verifizierung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie die Konfigurationsdatei .zip eines Secure Firewall Device Manager (FDM) generiert wird, der mithilfe von FMT zu einem FMC migriert werden soll.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Firewall Threat Defense (FTD)
- Cisco Firewall Management Center (FMC)
- Firewall Migration-Tool (FMT)
- Postman-API-Plattform

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen.

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postbote 11.50.0

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

- FDM kann jetzt auf verschiedene Weise zu FMC migriert werden. In diesem Dokument wird das Szenario untersucht, in dem die ZIP-Konfigurationsdatei mithilfe von API-Anforderungen generiert und später an FMT hochgeladen wird, um die Konfiguration zu FMC zu migrieren.
- Die in diesem Dokument beschriebenen Schritte beginnen direkt mit Postman. Es wird daher empfohlen, Postman bereits installiert zu haben. Der PC oder Laptop, den Sie verwenden werden, müssen Zugriff auf FDM und FMC haben, auch FMT muss installiert sein und ausgeführt werden.

Überlegungen

- In diesem Dokument wird die ZIP-Konfigurationsdatei stärker als bei der FMT-Verwendung behandelt.
- Die FDM-Migration mit der ZIP-Konfigurationsdatei ist für nicht aktive Migrationen vorgesehen und erfordert nicht sofort eine FTD-Zieladresse.

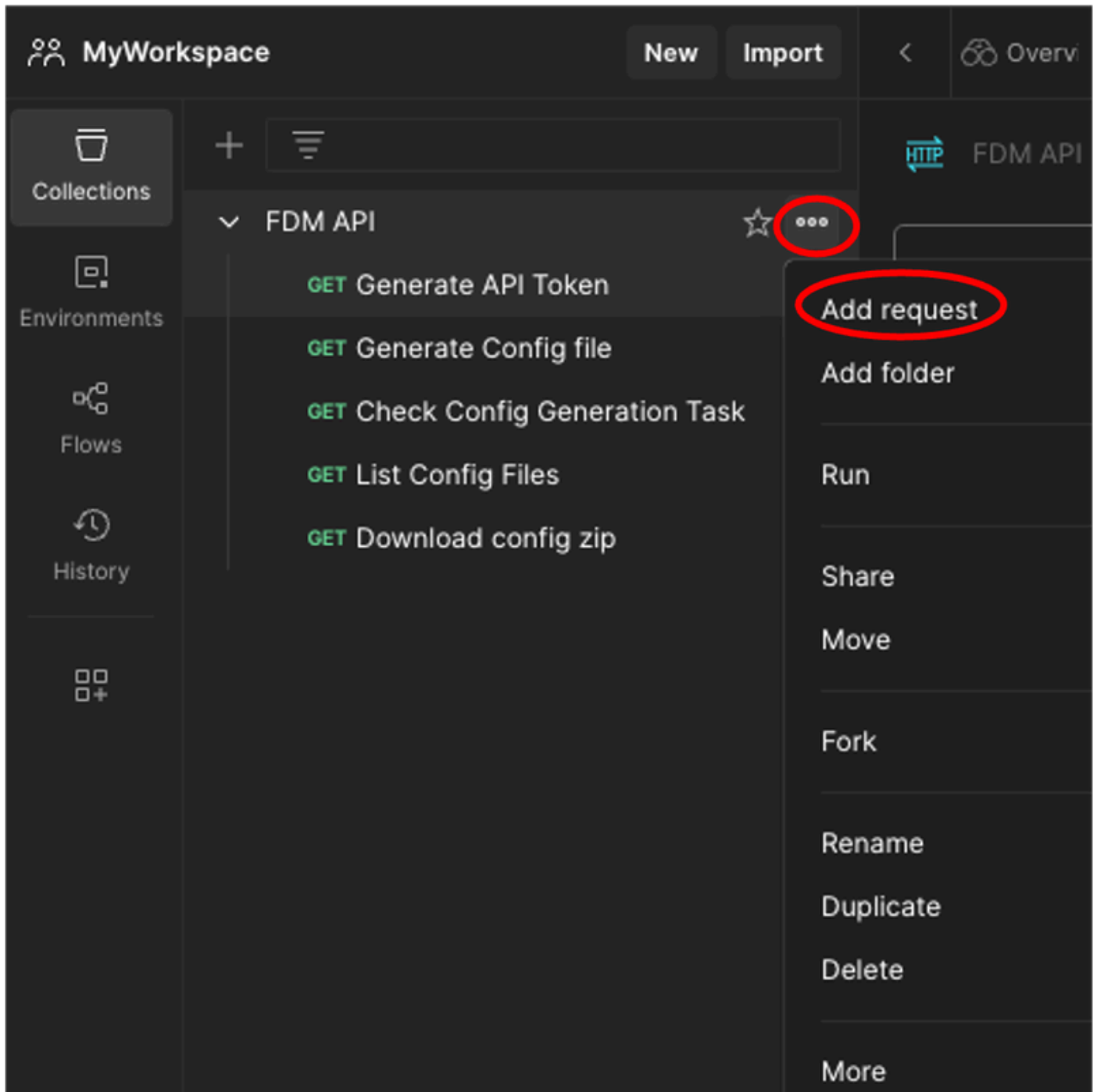


Warnung: Bei Auswahl dieses Modus können nur Zugriffskontrollrichtlinien (ACP), Network Address Translation Policy (NAT) und Objekte migriert werden. In Bezug auf die Objekte müssen diese in einer zu migrierenden ACP-Regel oder NAT verwendet werden, andernfalls werden sie ignoriert.

Konfiguration

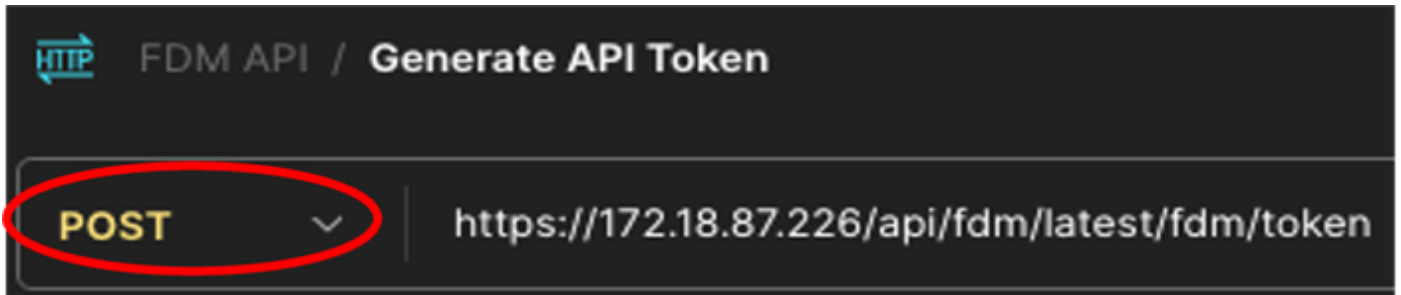
API-Anfragen - Post

1. Erstellen Sie in Postman eine neue Sammlung (in diesem Szenario wird FDM API verwendet).
2. Klicken Sie auf die drei Punkte und anschließend auf Add request (Anforderung hinzufügen).



Postman - Sammlung erstellen und Ergänzung beantragen

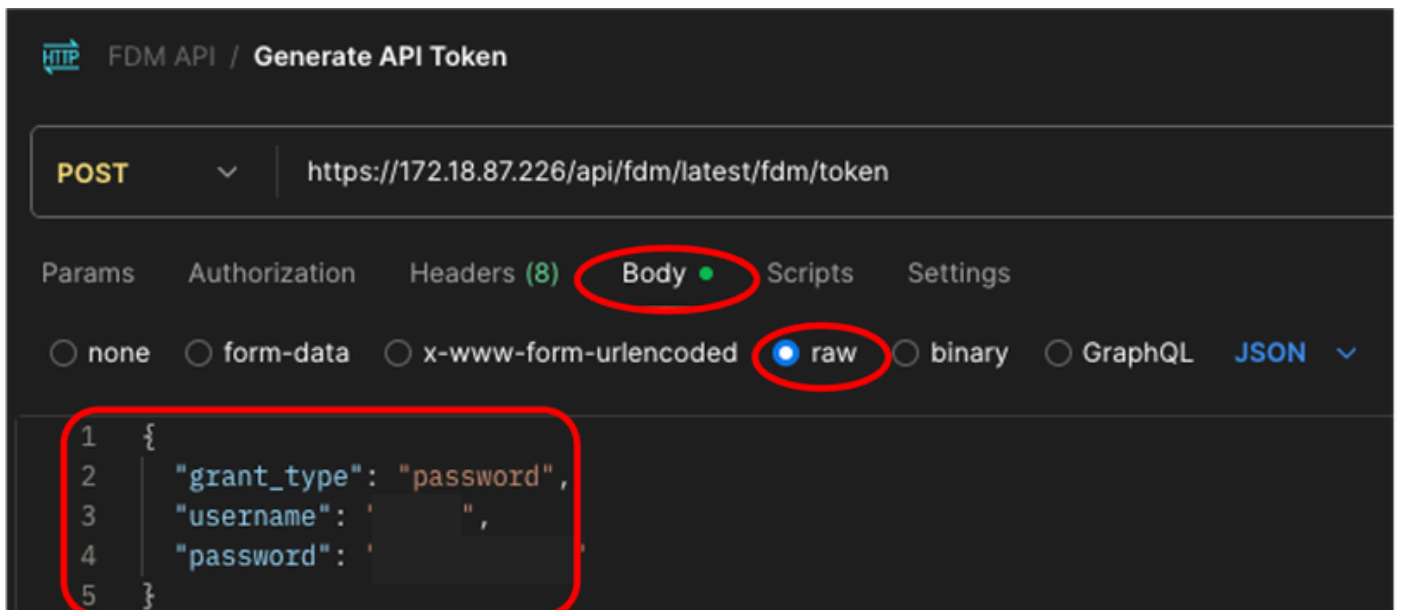
3. Neue Anforderung anrufen: API-Token generieren. Sie wird als GET-Anforderung erstellt. Zum Zeitpunkt der Ausführung muss jedoch POST aus dem Dropdown-Menü ausgewählt werden. Im Textfeld neben POST die nächste Zeile vorstellen: `https://<FDM IP ADD>/api/fdm/latest/fdm/token`



Postman - Token-Anfrage

4. Wählen Sie auf der Registerkarte Body die Option raw aus, und stellen Sie die Anmeldeinformationen für den Zugriff auf das FTD-Gerät (FDM) in diesem Format vor.

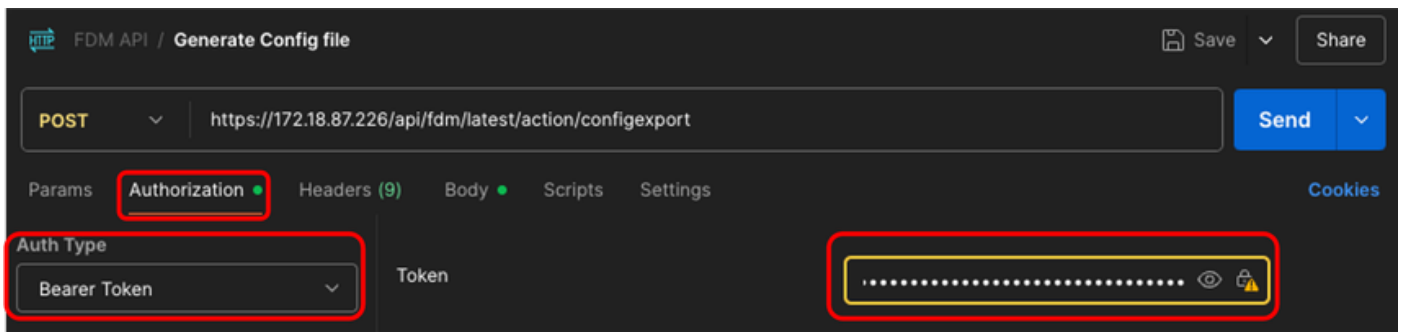
```
{  
  "Grande_type": "Kennwort",  
  "Benutzername": "Benutzername",  
  "Kennwort": "Kennwort"  
}
```



Postman - Token-Anforderungstext

5. Klicken Sie abschließend auf Senden, um Ihr Zugriffs-Token zu erhalten. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort. Erstellen Sie eine Kopie des gesamten Tokens (innerhalb der doppelten Anführungszeichen), da es in späteren Schritten verwendet wird.

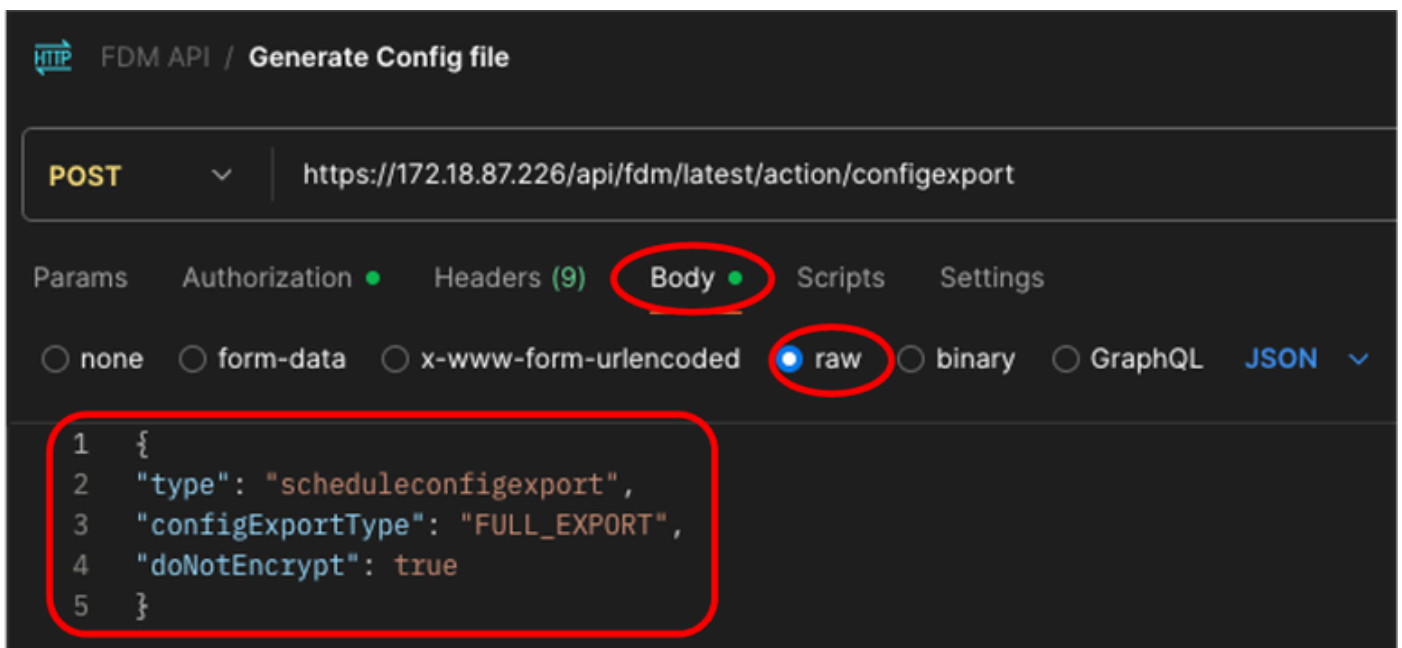
Token ein.



Postman - Generieren einer Konfigurationsdateianforderung - Autorisierung

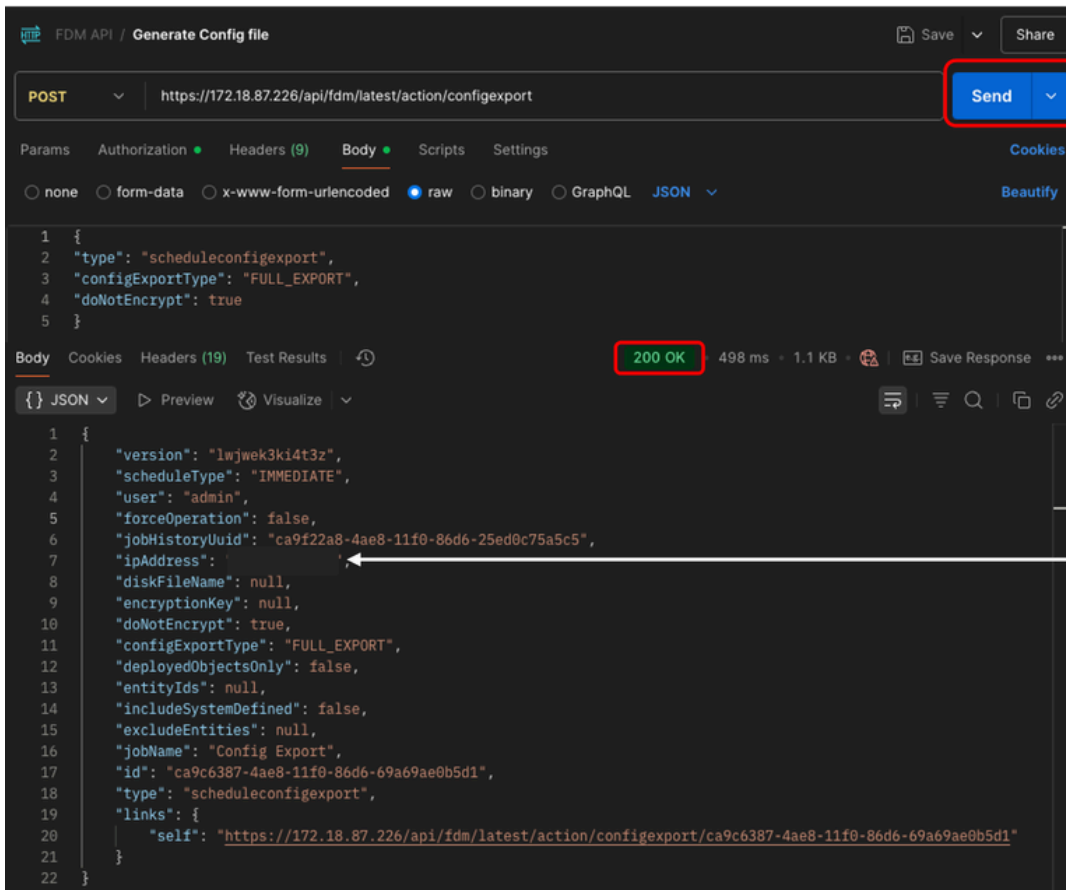
9. Wählen Sie auf der Registerkarte Haupttext die Option unformatiert, und stellen Sie diese Informationen vor.

```
{  
  Typ: "Scheduleconfigexport",  
  "configExportType": "VOLLSTÄNDIGER EXPORT",  
  "doNotEncrypt": wahr  
}
```



Postman - Generieren einer Konfigurationsdateianfrage - Text

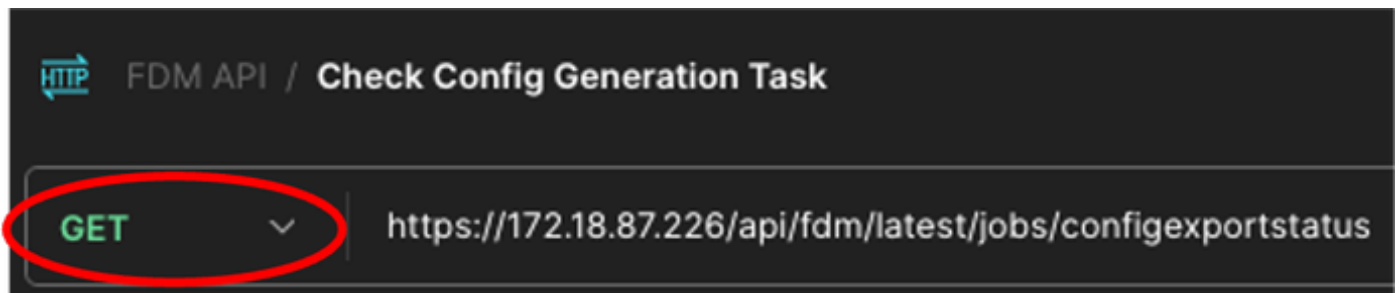
10. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort.



Postman - Generieren einer Konfigurationsdateianforderung - Ausgabe

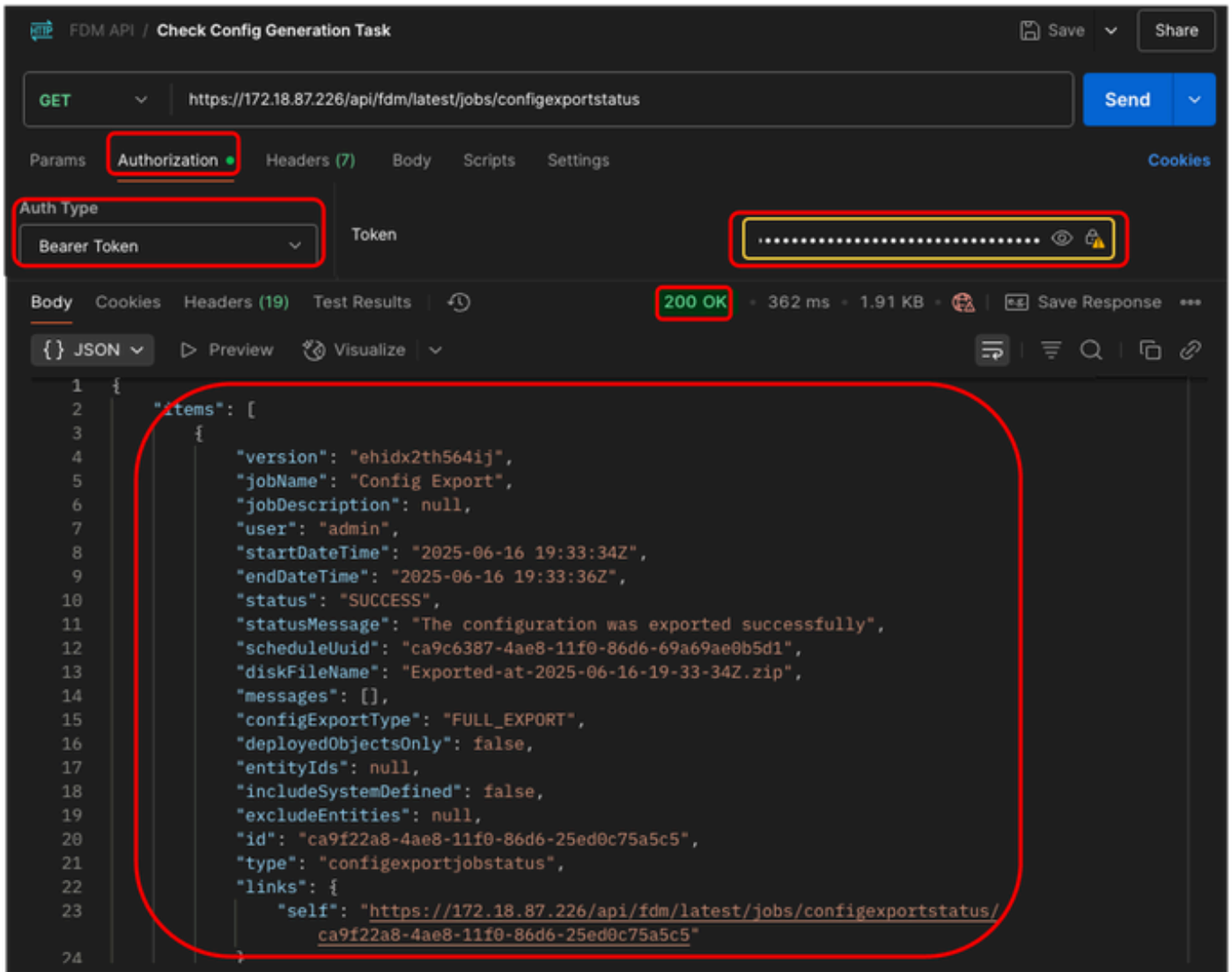
11. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen. Dieses Mal wird GET verwendet.

12. Wählen Sie diese neue Anforderung: Aufgabe zur Konfigurationsgenerierung überprüfen. Sie wird als GET-Anforderung erstellt. Außerdem muss die Option GET aus dem Dropdown-Menü ausgewählt werden, wenn Sie diesen Befehl ausführen. Führen Sie im Textfeld neben GET die nächste Zeile `https://<FDM IP ADD>/api/fdm/latest/jobs/configureExportStatus` ein.



Postman: Anfrage für Konfigurationsexport prüfen

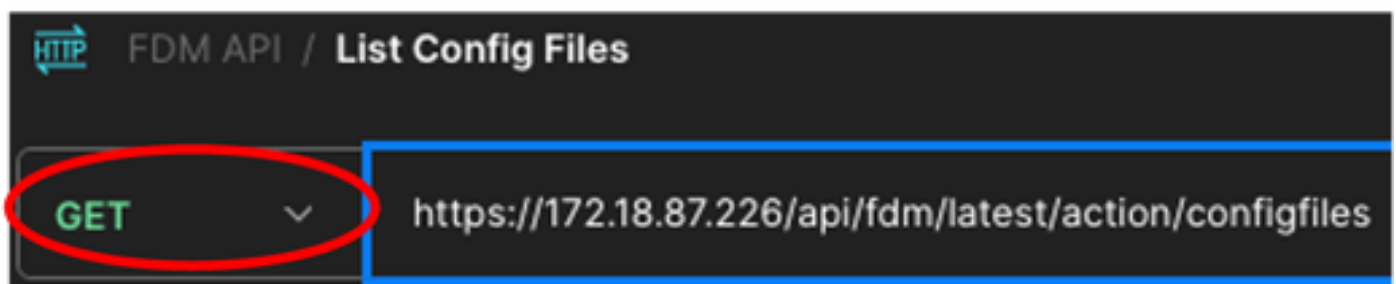
13. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token als Authentifizierungstyp und im Textfeld neben Token fügen Sie das in Schritt 5 kopierte Token ein. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK Antwort und im JSON Feld können Sie den Aufgabenstatus und andere Details sehen.



Postman - Anfrage für Konfigurationsexport-Status - Autorisierung und Ausgabe

14. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen, GET wird dieses Mal verwendet werden.

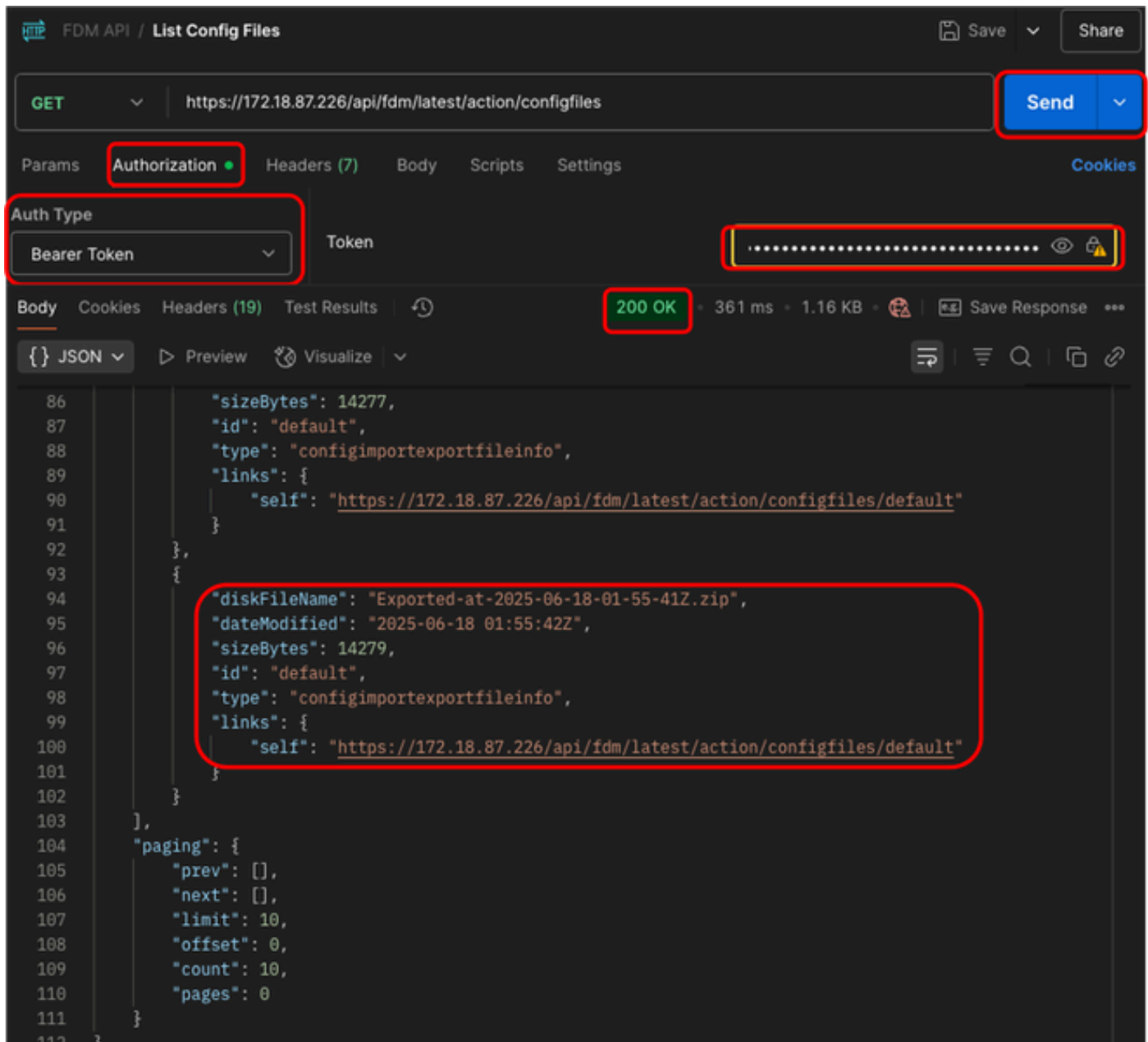
15. Neue Anforderung anrufen: Listen Sie die Konfigurationsdateien auf. Sie wird als GET-Anforderung erstellt. Auch wenn Sie diese Anforderung ausführen, muss GET aus dem Dropdown-Menü ausgewählt werden. Im Textfeld neben GET führen Sie die nächste Zeile ein: `https://<FDM IP ADD>/api/fdm/latest/action/configfiles`



Postman - Anfrage für exportierte Konfigurationsdateien anzeigen

16. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token

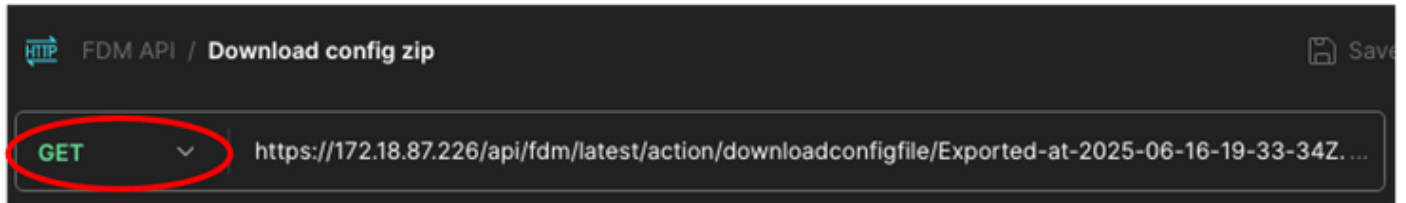
als Authentifizierungstyp und im Textfeld neben Token fügen Sie das in Schritt 5 kopierte Token ein. Klicken Sie abschließend auf Senden. Wenn alles in Ordnung ist, erhalten Sie eine 200 OK-Antwort. Im JSON-Feld wird die Liste der exportierten Dateien angezeigt. Die aktuellere ist unten aufgelistet. Kopieren Sie den aktuellen Dateinamen (aktuelleres Datum im Dateinamen), da er im letzten Schritt verwendet wird.



Postman - Anfrage für exportierte Konfigurationsdateien auflisten - Autorisierung und Ausgabe

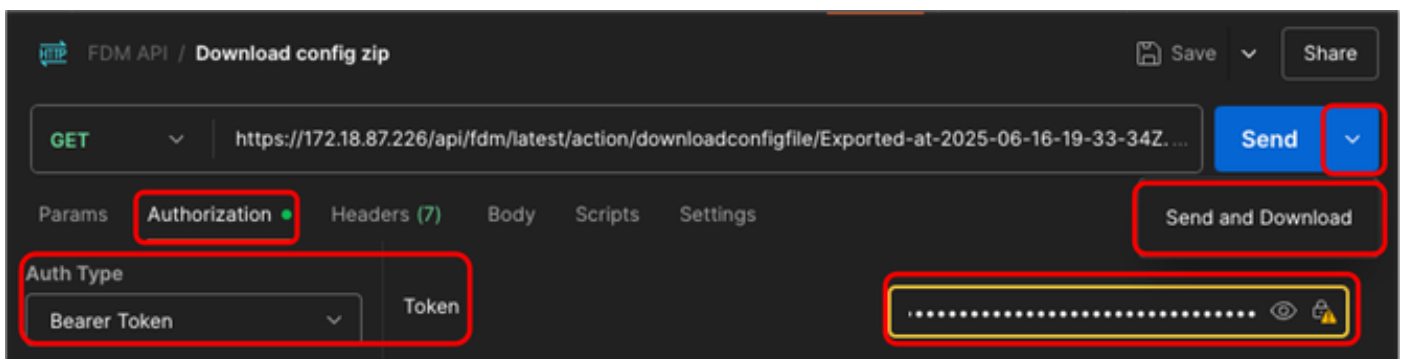
17. Wiederholen Sie Schritt 2, um eine neue Anforderung zu erstellen, GET wird dieses Mal verwendet.

18. Neue Anforderung anrufen: Konfigurationszip herunterladen Sie wird als GET-Anforderung erstellt. Auch wenn Sie diese Anforderung ausführen, muss GET aus dem Dropdown-Menü ausgewählt werden. Führen Sie im Textfeld neben GET die nächste Zeile ein, und fügen Sie am Ende den Dateinamen ein, den Sie in Schritt 16 kopiert haben. `https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >`



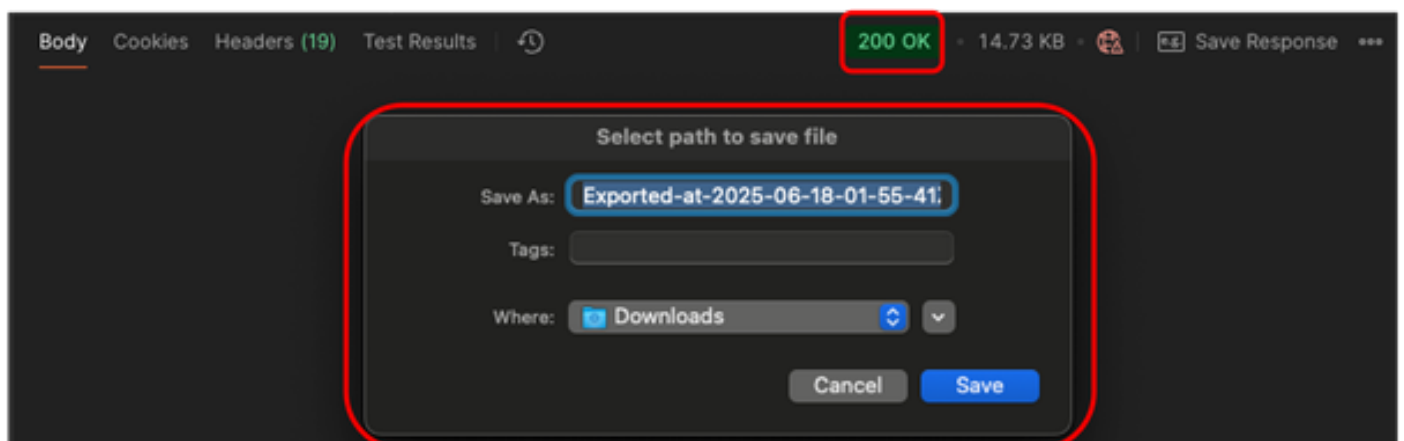
Postman - Config.zip-Dateianforderung herunterladen

19. Wählen Sie auf der Registerkarte Autorisierung im Dropdown-Menü die Option Träger-Token als Authentifizierungstyp, und fügen Sie das in Schritt 5 kopierte Token in das Textfeld neben Token ein. Klicken Sie abschließend auf den Abwärtspfeil neben Senden, und wählen Sie Senden und Herunterladen aus.



Postman - Config.zip-Dateianforderung herunterladen - Autorisierung

20. Wenn alles in Ordnung ist, erhalten Sie eine Antwort von 200 OK und ein Popup-Fenster wird angezeigt, in dem Sie nach dem Zielordner gefragt werden, in dem die Datei configuration.zip gespeichert werden soll. Diese ZIP-Datei kann jetzt in das Firewall Migration Tool hochgeladen werden.



Postman - Config.zip-Dateianforderung herunterladen - Speichern

Firewall Migration-Tool

21. Öffnen Sie das Firewall Migration Tool, wählen Sie im Dropdown-Menü Select Source Configuration die Option Cisco Secure Firewall Device Manager (7.2+) aus, und klicken Sie auf Migration starten.

Select Source Configuration

Source Firewall Vendor
Cisco Secure Firewall Device Manager (7.2+)

Start Migration Demo Mode

Cisco Secure Firewall Device Manager (7.2+) Pre-Migration Instructions

This migration may take a while. Do not make any changes to the Firewall Management Center (FMC) and Firewall Device Manager (FDM) when migration is in progress. FDM to FMC manager movement process should be done over a downtime/maintenance window. FDM Devices enrolled with the cloud management will lose access upon registration with FMC.

Session Telemetry:
Cisco collects the firewall telemetry set forth below in connection with this migration. By completing the migration, you consent to Cisco's collection and use of this telemetry data for purposes of tracking and following up on firewall device migrations and performing related migration analytics.

Acronyms used:
FMT: Firewall Migration Tool
FTD: Firewall Threat Defense
FMC: Firewall Management Center
FDM: Firewall Device Manager

Before you begin your Firewall Device Manager (FDM) to Firewall Threat Defense migration, you must have the following items:

- **Stable IP Connection:**
Ensure that the connection is stable between FMT, FDM and FMC. The host-pc from which the Firewall Migration tool is being run, should have connectivity to the FDM and the FMC.
- **FMC and FDM Version:** Ensure that the FMC version is 7.3 or later and FDM version is 7.2 or later. FDM version should be always equal or less than the FMC version. For optimal migration time, improved software quality and stability, use the suggested release for your **FTD** and **FMC**. Refer to the gold star on CCO for the suggested release.
- **FMC Requirements:**
Create a dedicated user account with administrative privileges for the FMT and use the credentials during migration. RestAPI is enabled on FMC by default. It is highly recommended that this is checked before migration. FMC should be registered with smart licensing server, and the licenses enabled on FDM must be enabled on FMC for smooth onboarding.
- **FDM Migration Options :**
Migration from FDM is supported in following ways.
 1. **Migrate Firewall Device Manager (Shared Configurations Only)**
 - This option migrates shared configuration to FMC.
 - This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
 - User can either upload a configuration bundle or provide FDM credentials to fetch details.
 - Automated fetching of configuration is a preferred method.
 2. **Migrate Firewall 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.
 - Ensure FDM Configuration has AD Realm with encryption set to NONE. [Click here](#) for more info.
 - User should provide FDM IP and credentials to fetch details. Uploading configuration bundle is not supported.
 - 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

FMT - FDM-Auswahl

22. Aktivieren Sie das erste Optionsfeld, Firewall-Gerätemanager migrieren (nur freigegebene Konfigurationen) und klicken Sie auf Weiter.

How would you like to migrate from Firewall Device Manager :



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

☒ Migrate Firewall Device Manager (Shared Configurations Only) 

- This option migrates shared configuration to FMC.
- This approach should be used to stage shared configuration to FMC. Maintenance window is not required.
- User can either upload a configuration bundle or provide FDM credentials to fetch details.
- Automated fetching of configuration is a preferred method.

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations) 

☐ Migrate Firewall Device Manager (Includes Device & Shared Configurations) to FTD Device (New Hardware) 

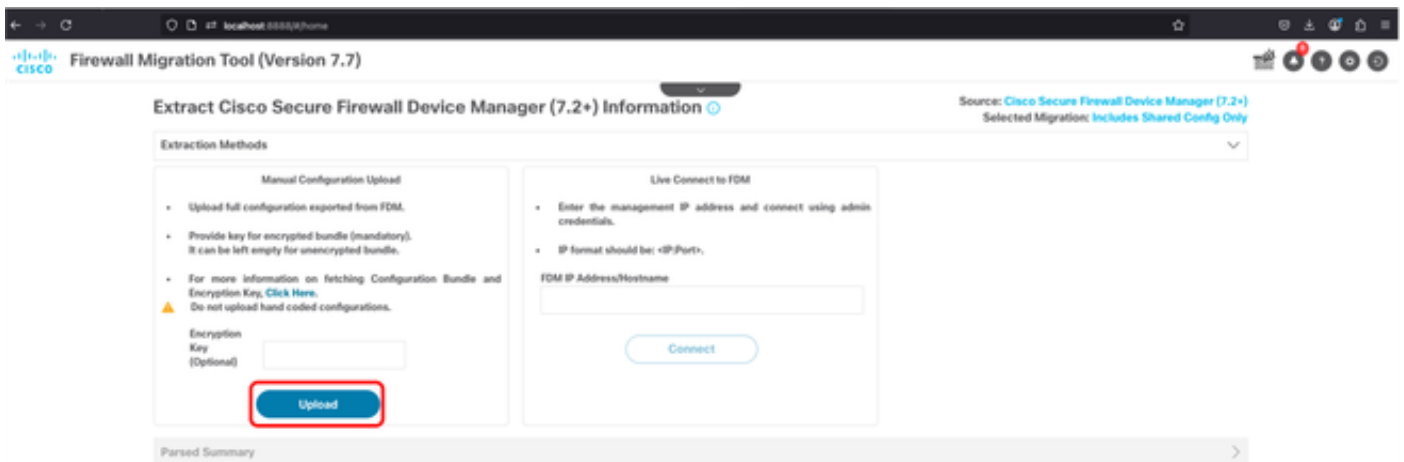
Note :

- Device configuration includes Interfaces, Routes and Site to Site VPN based features.
- Shared configuration includes Access control Policy, Remote Access VPN, NAT and Objects based features.

Continue

FMT = FDM Migration Shared Configurations Only

23. Klicken Sie im linken Bereich (Manuelles Hochladen der Konfiguration) auf Hochladen.



Firewall Migration Tool (Version 7.7)

Extract Cisco Secure Firewall Device Manager (7.2+) Information

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

Extraction Methods

Manual Configuration Upload

- Upload full configuration exported from FDM.
- Provide key for encrypted bundle (mandatory). It can be left empty for unencrypted bundle.
- For more information on fetching Configuration Bundle and Encryption Key, [Click Here](#). Do not upload hand coded configurations.

Encryption Key (Optional)

Upload

Live Connect to FDM

- Enter the management IP address and connect using admin credentials.
- IP format should be: <IP>:<Port>.

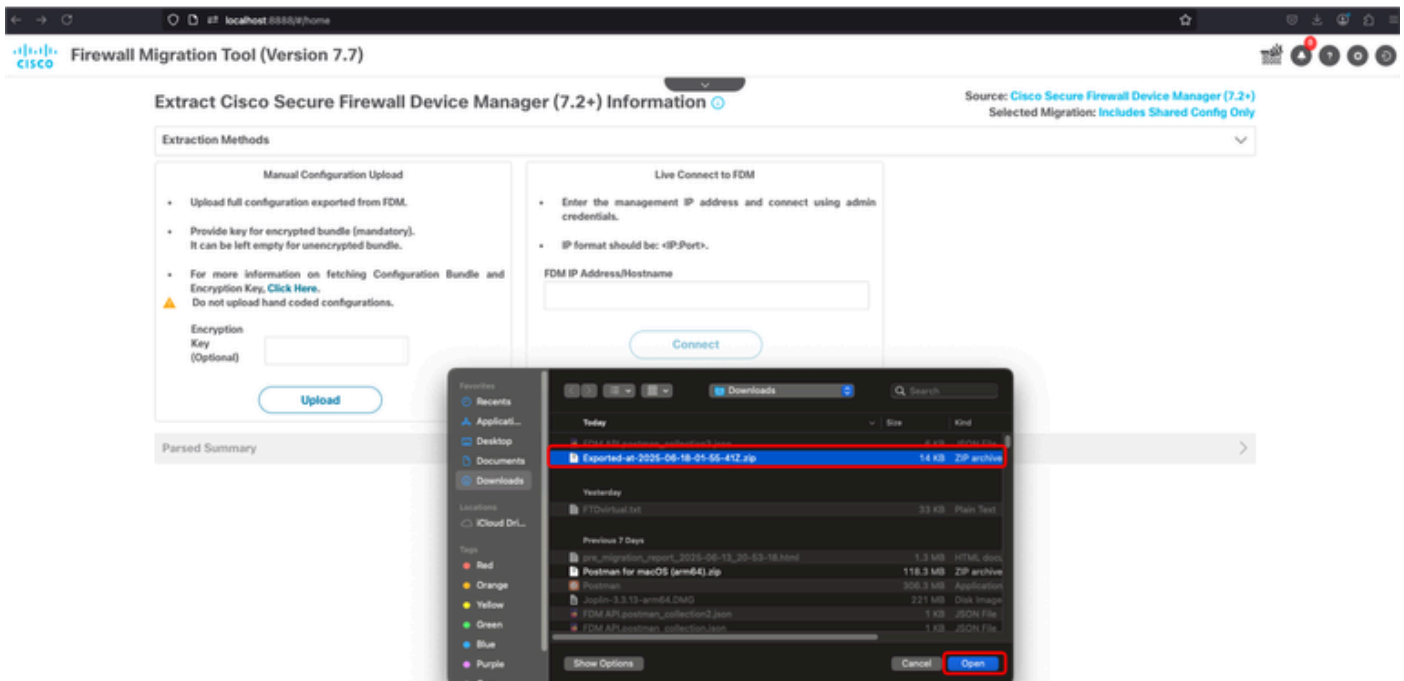
FDM IP Address/Hostname

Connect

Parsed Summary

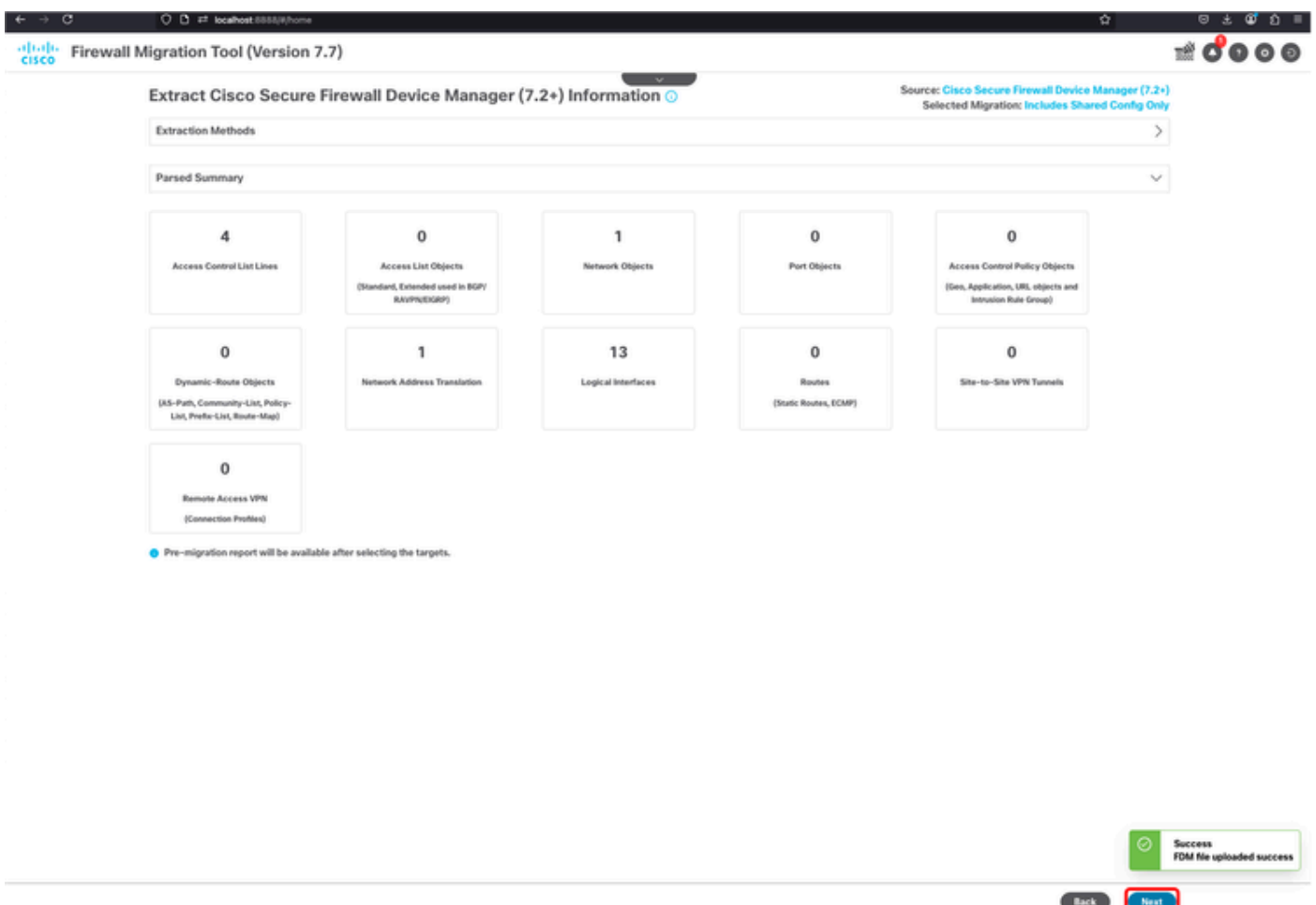
FMT - Config.zip-Datei hochladen

24. Wählen Sie die exportierte ZIP-Konfigurationsdatei im zuvor gespeicherten Ordner, und klicken Sie auf Öffnen.



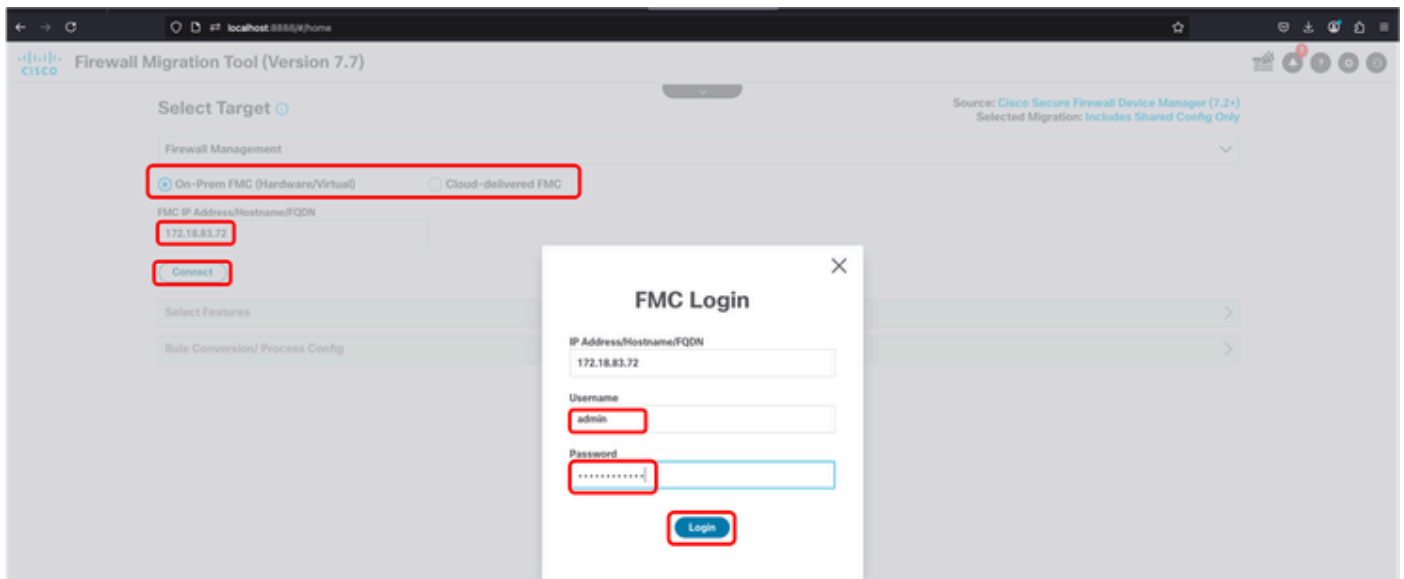
FMT - Config.zip-Dateiauswahl

25. Wenn alles wie erwartet verläuft, wird die analysierte Zusammenfassung angezeigt. In der rechten unteren Ecke wird ein Popup-Fenster mit der Meldung angezeigt, dass die FDM-Datei erfolgreich hochgeladen wurde. Klicken Sie auf Next (Weiter).



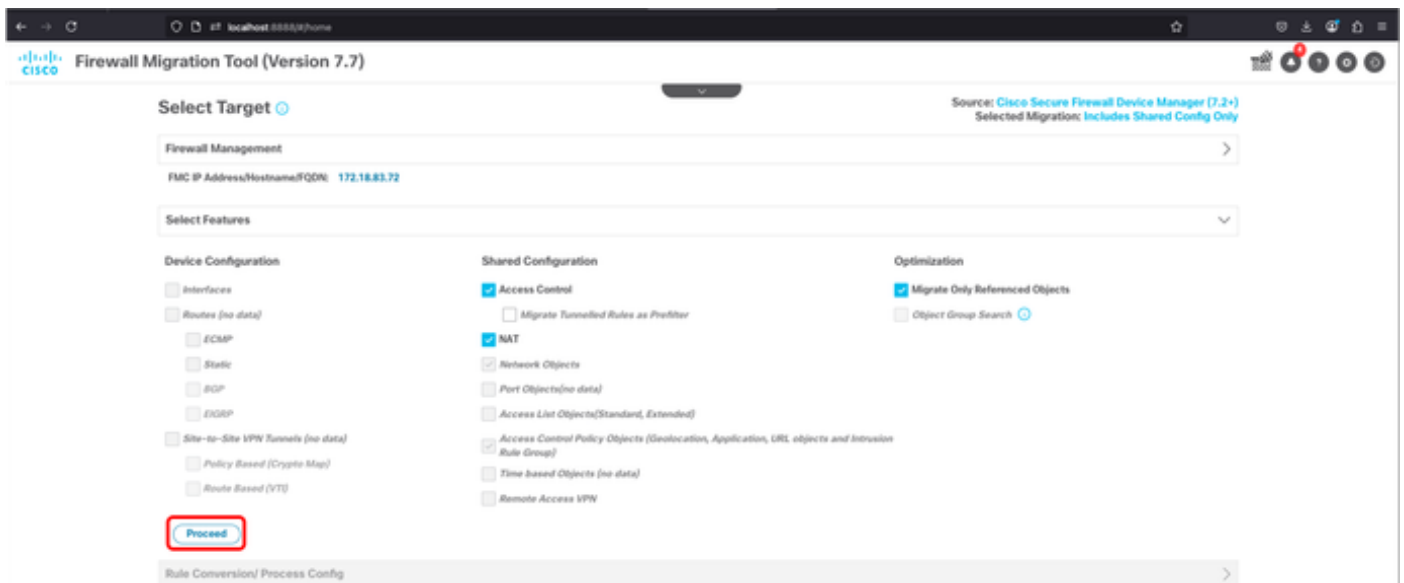
FMT - Zusammenfassung der Analyse

26. Aktivieren Sie die Option, die Ihrer Umgebung besser entspricht (Vor-Ort-FMC oder Cd-FMC). In diesem Szenario wird ein standortbasiertes FMC verwendet. Geben Sie die IP-Adresse des FMC ein, und klicken Sie auf Verbinden. Ein neues Popup-Fenster fordert FMC-Anmeldeinformationen an. Klicken Sie nach Eingabe dieser Informationen auf Anmelden.



FMT - FMC Zielanmeldung

27. Der nächste Bildschirm zeigt das Ziel-FMC und die Funktionen, die migriert werden sollen. Klicken Sie auf Fortfahren.



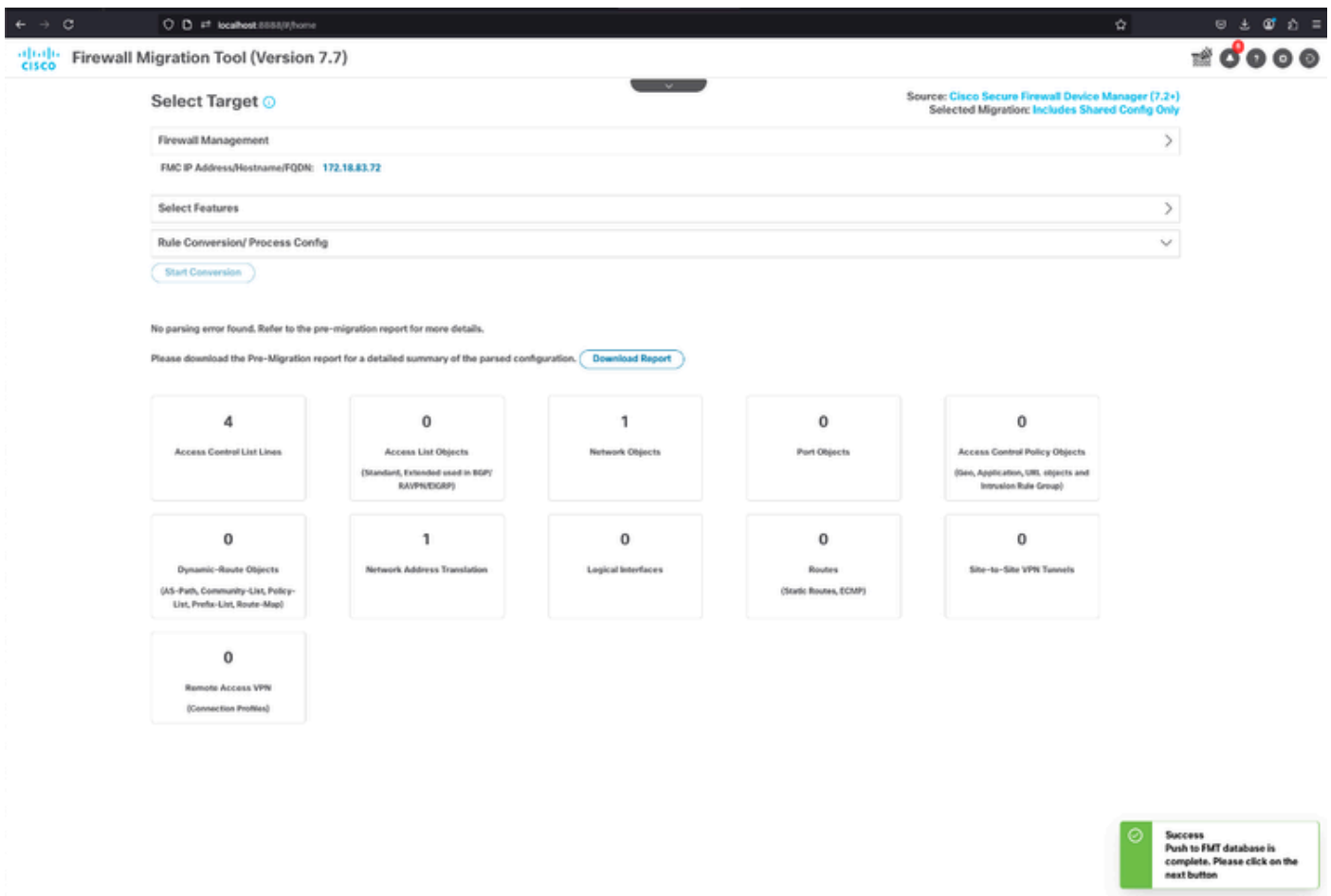
FMT - FMC-Ziel - Funktionsauswahl

28. Sobald FMC Target bestätigt ist, klicken Sie auf Start Conversion button.



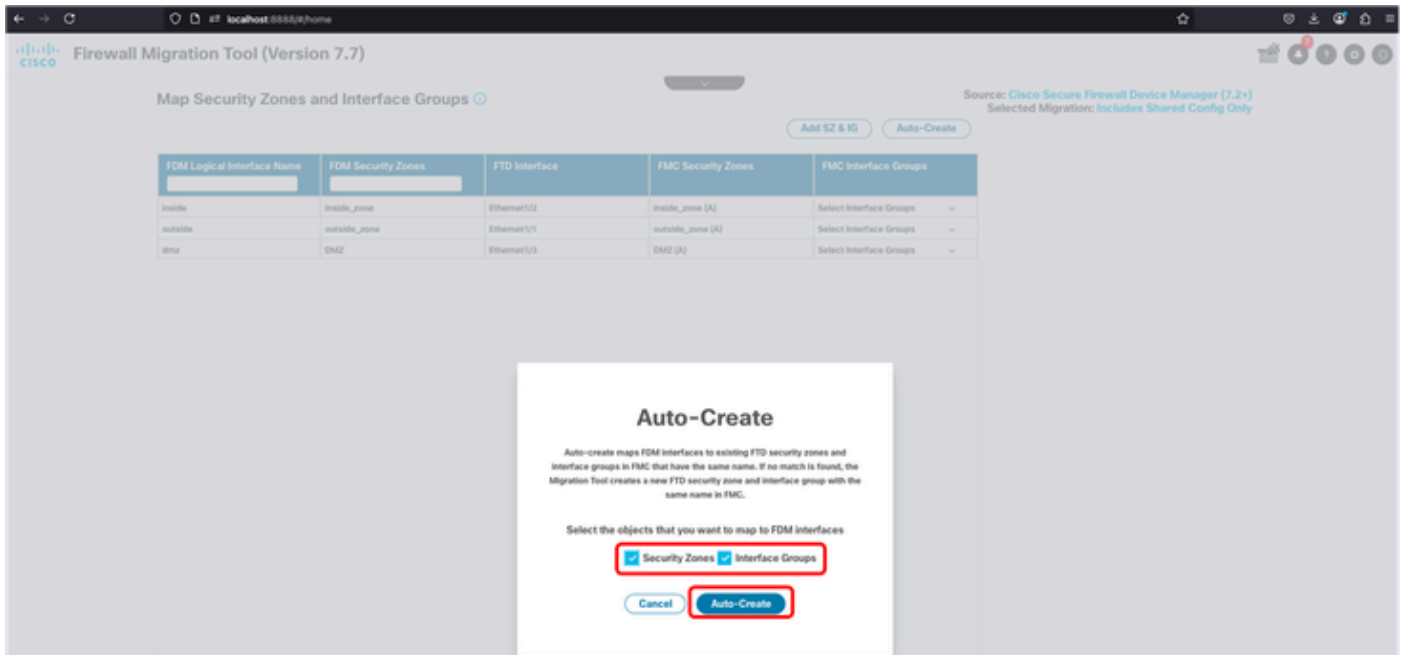
FMT - Konfig.-Konfiguration starten

29. Wenn alles wie erwartet läuft, wird ein Pop-Up in der rechten unteren Ecke angezeigt, das informiert, dass Push zur FMT-Datenbank abgeschlossen ist. Klicken Sie auf Next (Weiter).



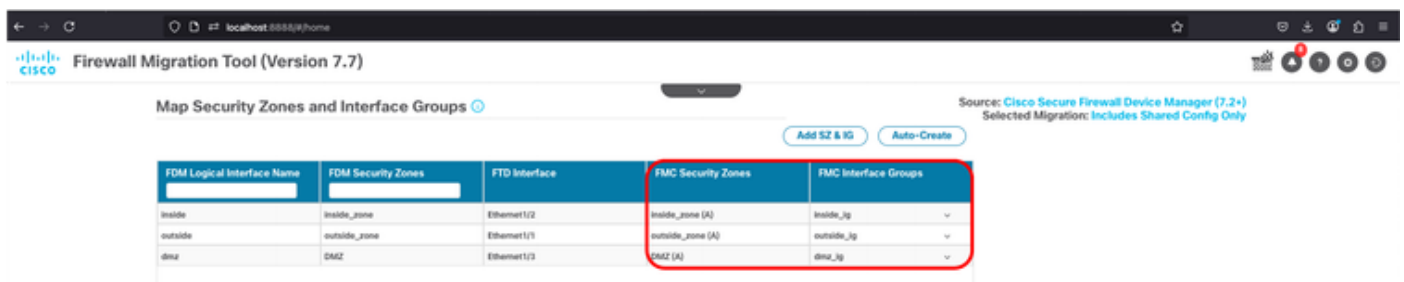
FMT - Datenbank-Push erfolgreich abgeschlossen

30. Auf dem nächsten Bildschirm müssen Sie die Sicherheitszonen und Schnittstellengruppen manuell erstellen oder die Option zum automatischen Erstellen auswählen. In diesem Szenario wird auto-create verwendet.



FMT - Auto Creating Security Zones and Interface Groups (Automatisches Erstellen von Sicherheitszonen und Schnittstellengruppen)

31. Nach Abschluss dieser Schritte werden in der 4. und 5. Spalte die Sicherheitszone bzw. die Schnittstellengruppe angezeigt.



FMT - Sicherheitszonen und Schnittstellengruppen erfolgreich erstellt

32. Im nächsten Bildschirm können Sie die Zugriffskontrollliste optimieren oder nur ACP, Objects und NAT validieren. Klicken Sie abschließend auf die Schaltfläche Validieren.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration Only

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

Access Control Objects NAT Interfaces Routers Site-to-Site VPN Remote Access VPN

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

50 per page 1 to 4 of 4 Page 1 of 1

Optimize ACL Validate

FMT = Optimization ACL = Validate Migration

33. Validierung dauert einige Minuten abgeschlossen werden.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared C

Validation in progress. It will take a while

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

Access Control Objects NAT Interfaces Routers Site-to-Site VPN Remote Access VPN

AGP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4

Search

#	Name	SOURCE			DESTINATION			ACCESS CONTROL POLICY ...		State	Action	ACE Count	TIME BASED
		Zone	Network	Port	Zone	Network	Port	Applications	URLs				
1	Inside_Outside_Rul...	inside_zone	ANY	ANY	outside_in...	ANY	ANY	ANY	ANY	✓	trust	1	None
2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
4	Outside_DMZ_R1	outside_in...	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

FMT - Validierung in Bearbeitung

34. Nach Abschluss des Vorgangs informiert FMT Sie, dass die Konfiguration erfolgreich validiert wurde, und als Nächstes klicken Sie auf die Schaltfläche "Push Configuration".

×

Validation Status

✓

Successfully Validated

Validation Summary (Pre-push)

4 Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	1 Network Objects	Not selected for migration Port Objects	0 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)	1 Network Address Translation	Not selected for migration Logical Interfaces	Not selected for migration Routes (Static Routes, ECMP)	Not selected for migration Site-to-Site VPN Tunnels
Not selected for migration Remote Access VPN (Connection Profiles)				

Push Configuration

FMT - Validierung erfolgreich - Push-Konfiguration an FMC

35. Schließlich, klicken Sie auf Fortfahren Schaltfläche.

The Step of final push to target FMC/FTD is subjected to zero, limited or many push errors that largely depend on the success or failure of API execution between migration tool and firewall management center.



Click on Proceed to continue.

Proceed

Recommendation: Please review the migration fallout report during the course of final push stage to understand firewall configurations that will not be migrated in addition to review the suggested actions to be taken on target FMC for "Abort Migration".

FMT - Mit Config Push fortfahren

36. Wenn alles wie erwartet verläuft, wird die Meldung Migration erfolgreich angezeigt. FMT fordert Sie auf, sich bei FMC anzumelden und die migrierte Richtlinie in FTD bereitzustellen.

Firewall Migration Tool (Version 7.7)

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

Complete Migration

Migration Status

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

[Click Here](#) to download troubleshooting bundle

Manual Upload: Exported-at-2025-06-18-01-55-41Z.zip

Migration Summary (Post Push)

Access Control List Lines	Access List Objects (Standard, Extended used in SGT, NATFWDGROUP)	Network Objects	Port Objects	Access Control Policy Objects (Dns, Application, URL, objects and Intrusion Rule Group)
4	Not selected for migration	1	Not selected for migration	0
Not selected for migration	Dynamic-Route Objects (IS-Path, Community-List, Policy-List, Profile List, Route-Map)	Network Address Translation	Not selected for migration	Not selected for migration
Not selected for migration	Logical Interfaces	Not selected for migration	Not selected for migration	Not selected for migration
Not selected for migration	Routers (Static Routes, EIGRP)	Not selected for migration	Not selected for migration	Not selected for migration
Not selected for migration	Site-to-Site VPN Tunnels	Not selected for migration	Not selected for migration	Not selected for migration
Not selected for migration	Remote Access VPN (Connection Profiles)	Not selected for migration	Not selected for migration	Not selected for migration

Please download the Post Migration Report for a detailed summary. [Download Report](#)

Success
The migration is complete, with no errors. Log in to the target FMC to review and deploy the configuration.

FMT - Benachrichtigung über erfolgreiche Migration

FMC-Verifizierung

37. Nach der Anmeldung bei FMC werden die ACP- und NAT-Richtlinien als FTD-Mig angezeigt. Jetzt können Sie mit der Bereitstellung für die neue FTD fortfahren.

Firewall Management Center			
Policies / Access Control / Access Control			
Overview Analysis Policies Devices Objects Integration			
Deploy Search Settings Admin Secure			
Object Management Intrusion Network Analysis Policy DNS Import/Export			
Type to search Total 3 policies Analyze Policies Delete Policies New Policy			
☐	Access Control Policy	Last Modified	Status
☐	ACP	2025-06-18 00:51:41 Modified by "Firepower System"	Targeting 1 device Out-of-date on all targeted devices
☐	FTD-Mig-ACP-1750297713	2025-06-18 21:48:35 Modified by "admin"	Targeting 0 devices
☐	SNMP	2025-06-18 00:51:41 Modified by "Firepower System"	Targeting 1 device Out-of-date on all targeted devices

FMC - ACP Migriert

Firewall Management Center			
Devices / NAT			
Overview Analysis Policies Devices Objects Integration			
Deploy Search Settings Admin Secure			
NAT Exemptions New Policy			
☐	NAT Policy	Device Type	Status
☐	FTD-Mig-1750297669	Threat Defense	Targeting 0 device(s)

FMC - NAT-Richtlinienmigration

Zugehörige Informationen

- [FMT - FDM Migration Guide to FMC](#)
- [FMT-Versionshinweise](#)

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.