

FDM naar FMC migreren via FMT met behulp van Configuration.zip File

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[overwegingen](#)

[Configuratie](#)

[API-aanvragen - Postman](#)

[Firewall Migration Tool](#)

[VCC-verificatie](#)

[Gerelateerde informatie](#)

Inleiding

In dit document wordt beschreven hoe u het configuratiebestand .zip van een Secure Firewall Device Manager (FDM) kunt genereren dat met behulp van FMT naar een FMC moet worden gemigreerd.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

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

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende softwareversies.

FTD 7.4.2

VCC 7.4.2

FMT 7.7.0.1

Postbode 11.50.0

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

- FDM kan nu op verschillende manieren naar FMC worden gemigreerd. In dit document is het scenario dat zal worden onderzocht het genereren van het configuratie .zip-bestand met behulp van API-verzoeken en het later uploaden van dat bestand naar FMT om de configuratie naar FMC te migreren.
- De stappen die in dit document worden weergegeven, beginnen direct met het gebruik van Postman, dus het wordt aanbevolen dat u Postman al hebt geïnstalleerd. De pc of laptop die u gaat gebruiken, moet toegang hebben tot FDM en FMC, ook FMT moet worden geïnstalleerd en uitgevoerd.

overwegingen

- Dit document is meer gericht op het genereren van .zip-bestanden voor de configuratie dan op het gebruik van FMT.
- FDM-migratie met behulp van configuratie .zip-bestand, is voor niet-live migraties en vereisen niet onmiddellijk een bestemming FTD.

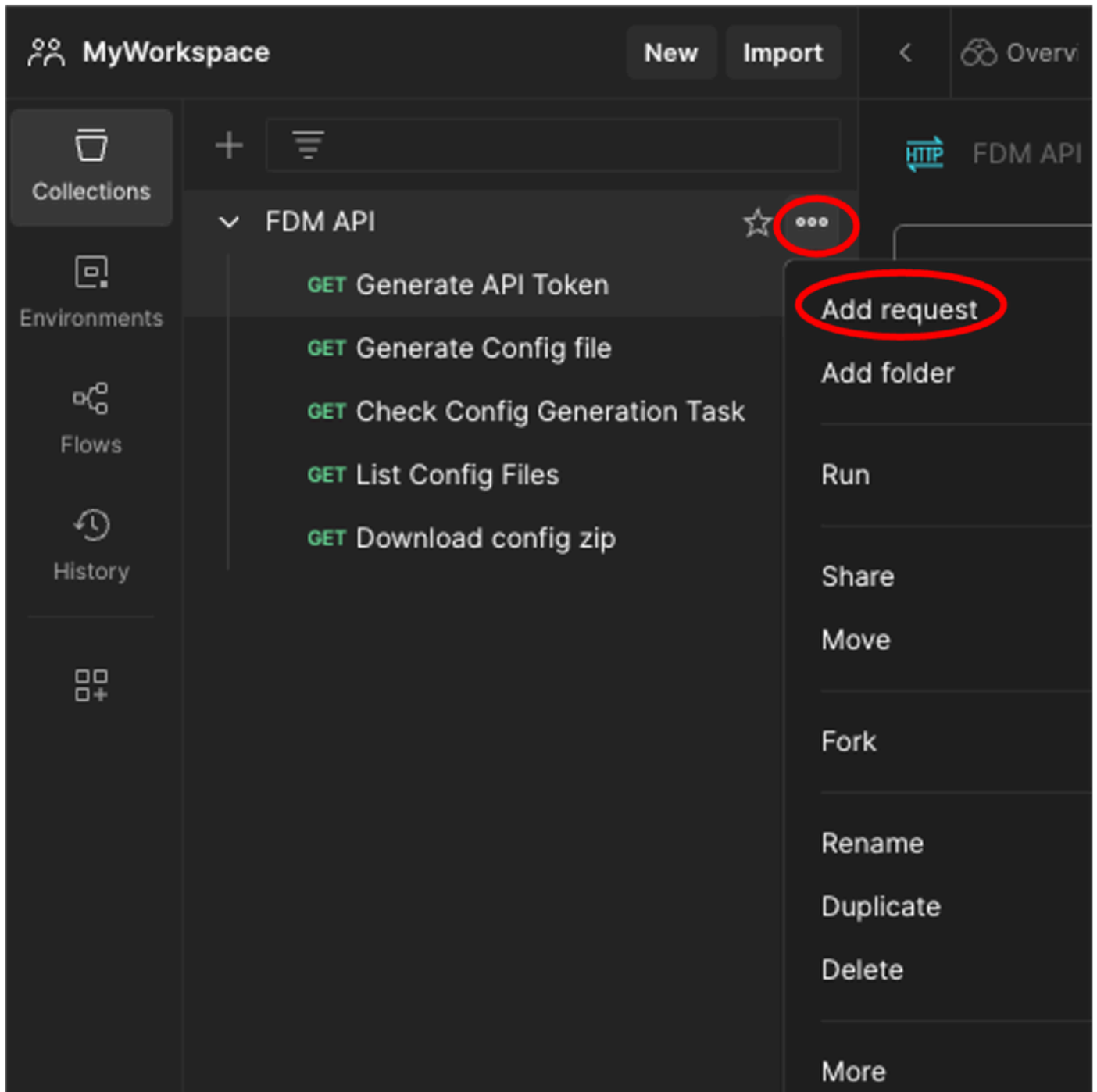


Waarschuwing: als u deze modus kiest, kunt u alleen Access Control Policy (ACP), Network Address Translation Policy (NAT) en Objecten migreren. Met betrekking tot de objecten die moeten worden gebruikt in een ACS-regel of NAT, te migreren, anders worden die genegeerd.

Configuratie

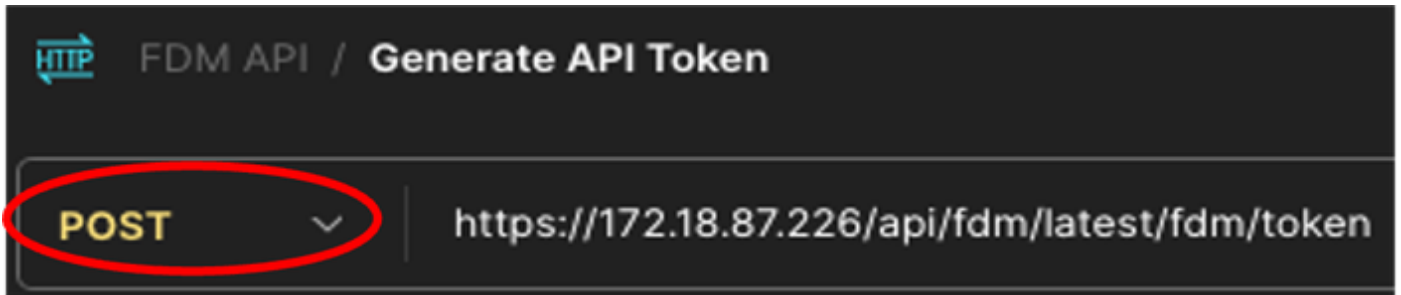
API-aanvragen - Postman

1. Maak in Postman een nieuwe collectie (in dit scenario wordt FDM API gebruikt).
2. Klik op de 3 punten en klik op Aanvraag toevoegen.



Postman - Collectie creatie en verzoek toevoeging

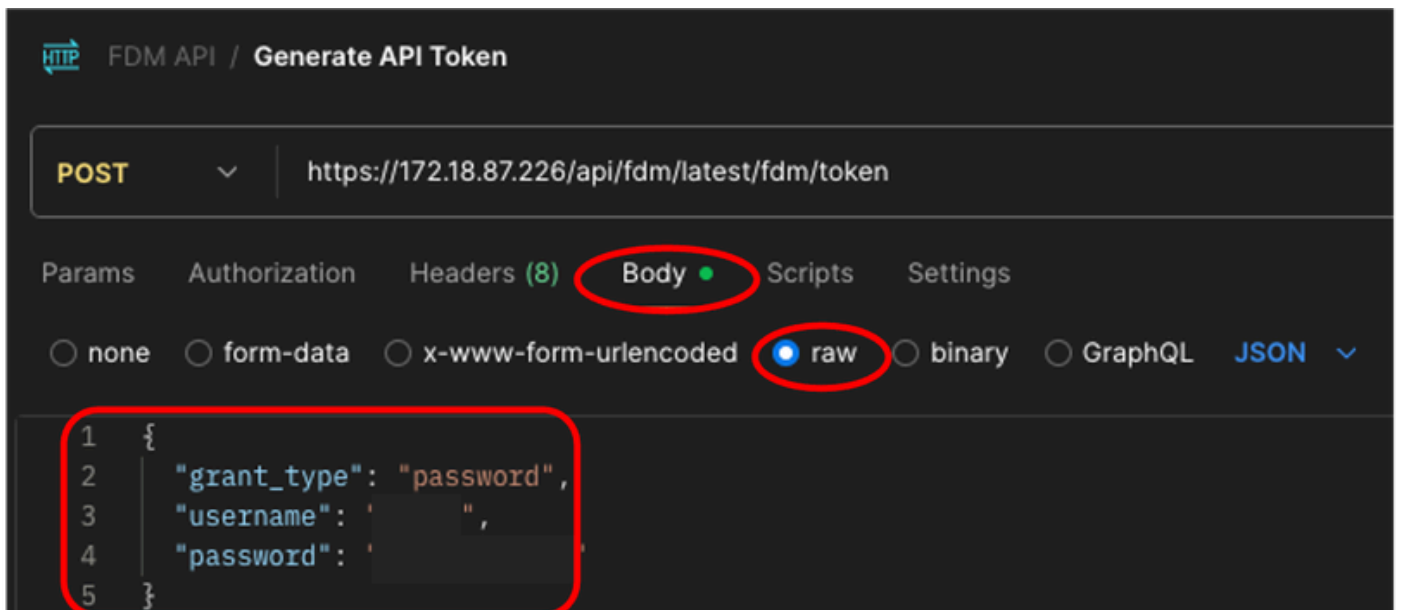
3. Noem dit nieuwe verzoek: Genereer API Token. Het wordt gemaakt als een GET-verzoek, maar op het moment dat u deze uitvoert, moet POST worden geselecteerd in het vervolgkeuzemenu. In het tekstvak naast POST, introduceert u de volgende regel `https://<FDM IP ADD>/api/fdm/latest/fdm/token`



Postbode - Token Request

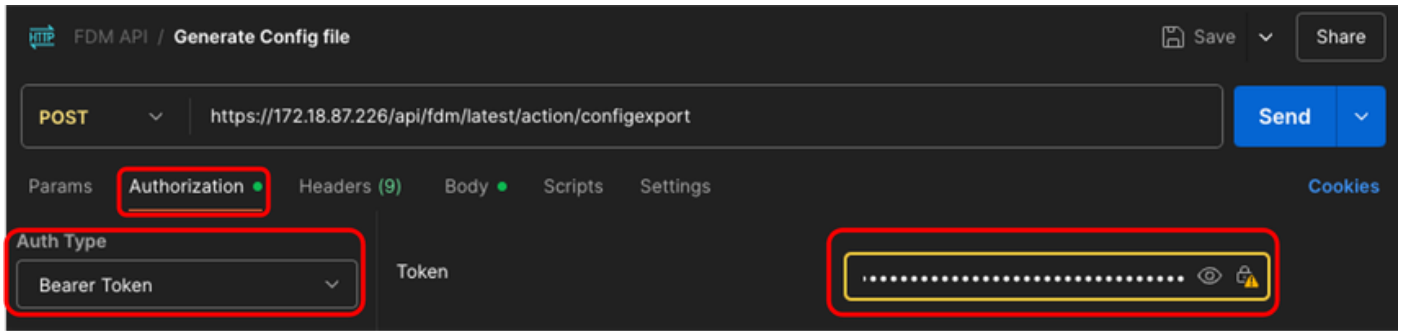
4. Selecteer op het tabblad Body de optie raw en introduceer de referenties om met dit formaat toegang te krijgen tot het FTD-apparaat (FDM).

```
{  
  "grant_type": "password",  
  "gebruikersnaam": "gebruikersnaam",  
  "Password": "Password"  
}
```



Postbode - Token Request Body

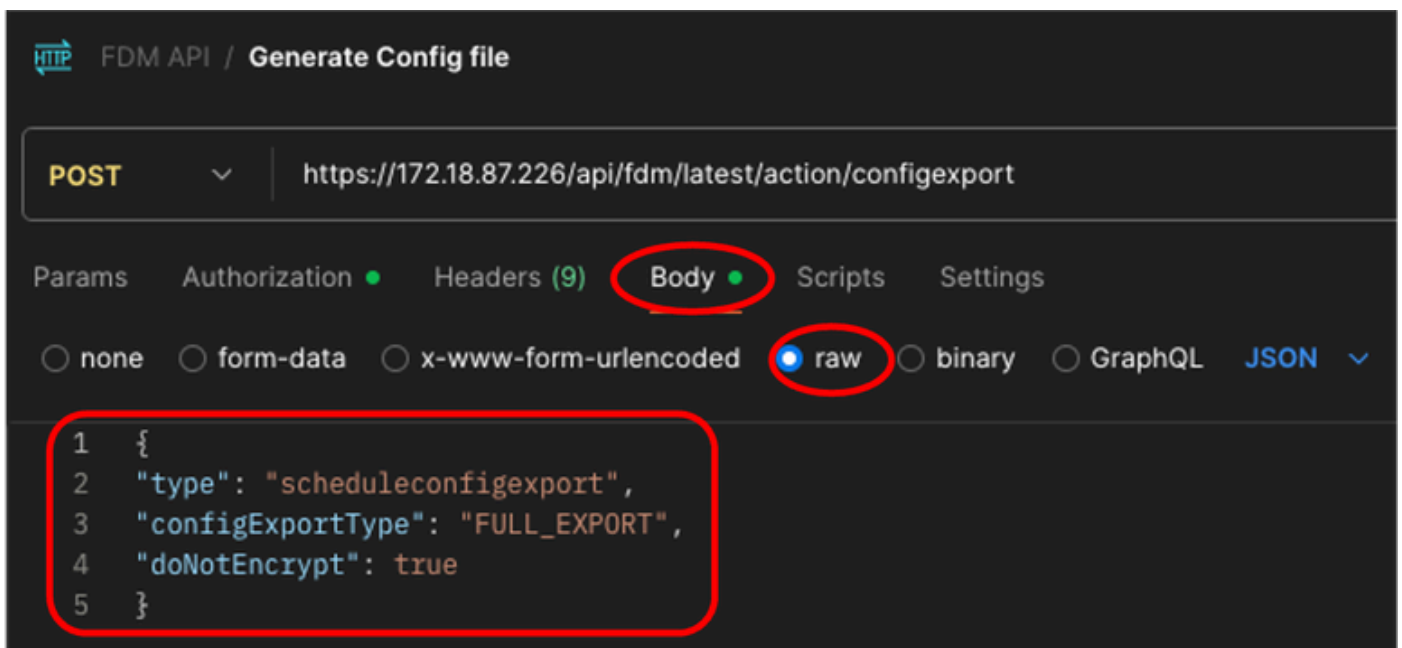
5. Klik ten slotte op Verzenden om uw toegangstoken te krijgen. Als alles goed is, krijg je een 200 OK reactie. Maak een kopie van het hele token (binnen de dubbele aanhalingstekens) omdat het in latere stappen zal worden gebruikt.



Postman - Config File Request genereren - Autorisatie

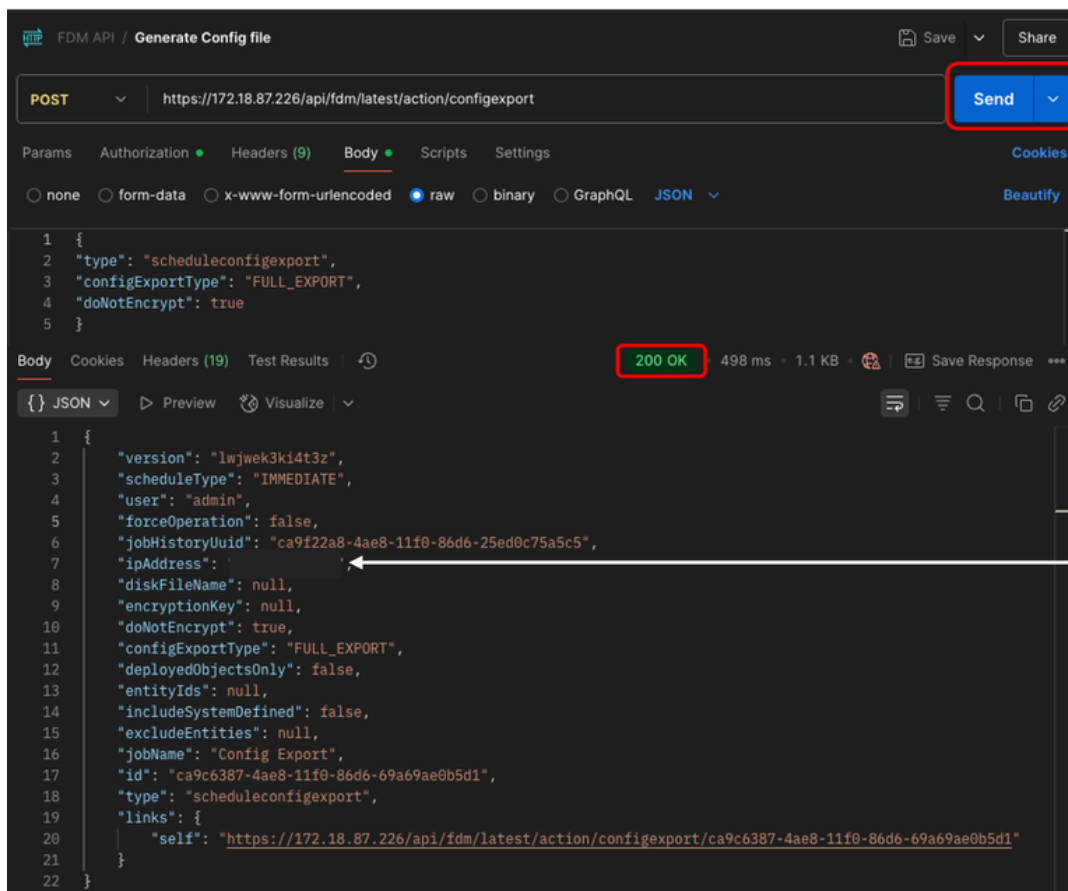
9. Selecteer op het tabblad Lichaam de onbewerkte optie en voer deze informatie in.

```
{  
  "type": "ScheduleConfigExport",  
  "configExportType": "FULL_EXPORT",  
  "doNotEncrypt": true  
}
```



Postman - Aanvraag voor configuratiebestand genereren - Body

10. Klik ten slotte op Verzenden. Als alles goed is, krijg je een 200 OK reactie.

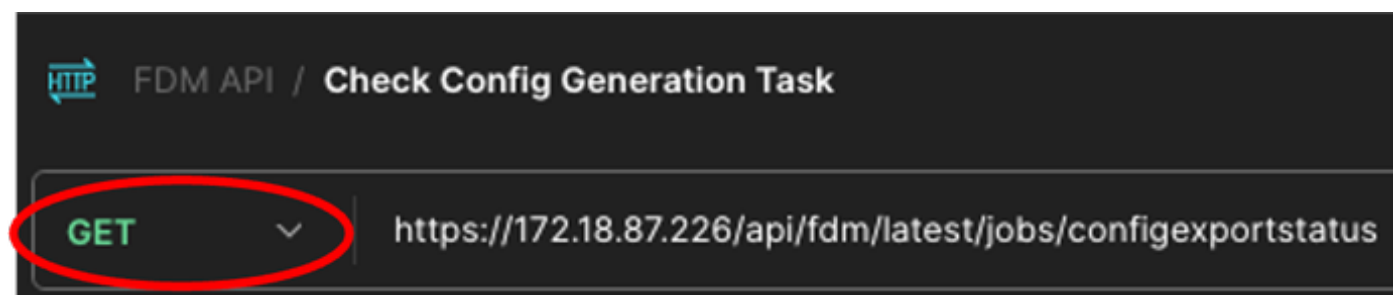


This IP address is the one that is connecting to the FTD through the requests.

Postman - Config File Request genereren - Uitvoer

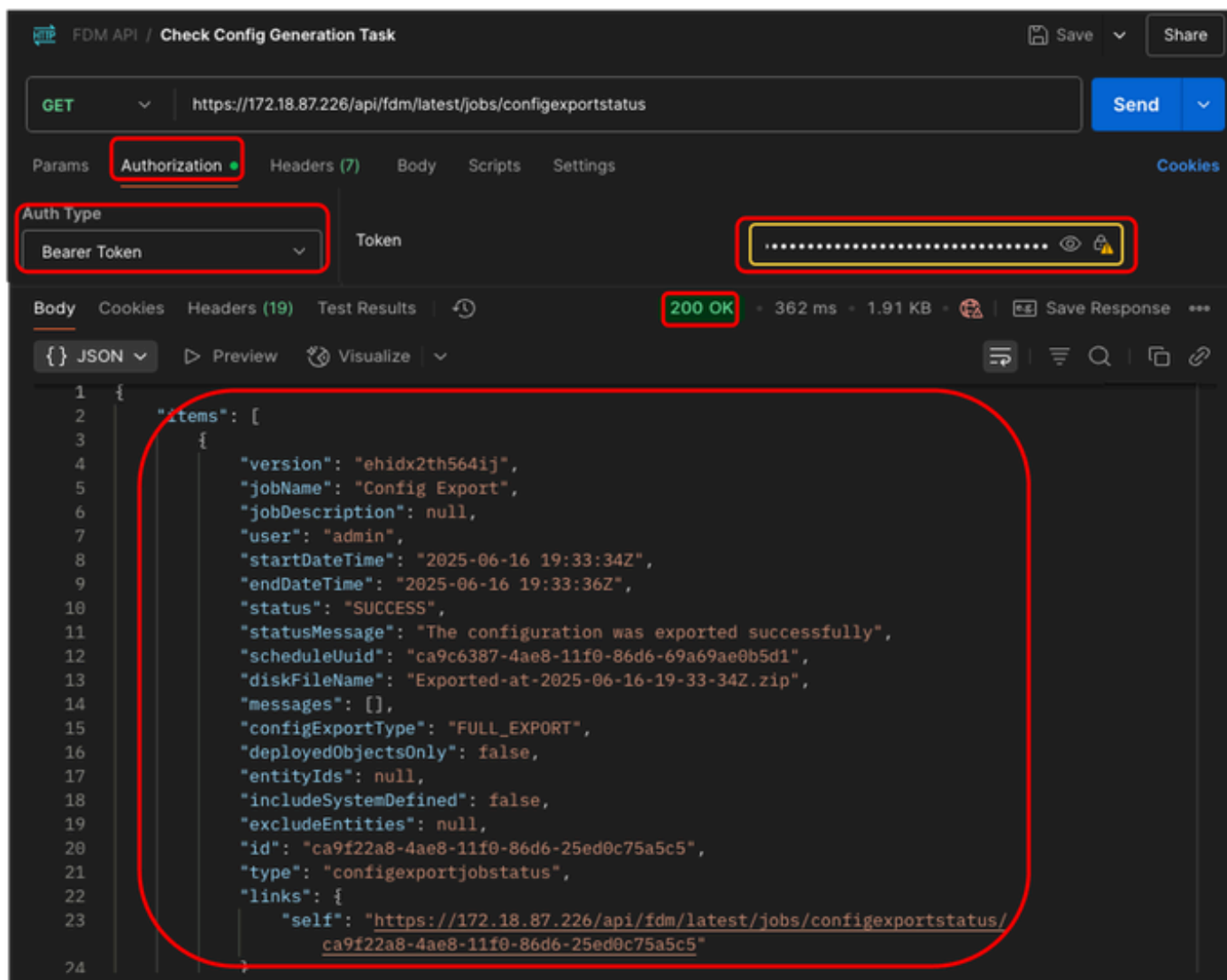
11. Herhaal stap 2 om een nieuw verzoek te maken. Deze keer wordt GET gebruikt.

12. Bel dit nieuwe verzoek: Controleer de taak Config Generation. Het zal worden gemaakt als een GET-verzoek. Ook moet de tijd dat u deze uitvoert, GET worden geselecteerd in het vervolgkeuzemenu. In het tekstvak naast GET introduceert u de volgende regel `https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus`



Postman - Controleer de status van de exportstatus van de configuratie

13. Op het tabblad Autorisatie selecteert u Token aan toonder als Auth Type in de vervolgkeuzelijst en plakt u in het tekstvak naast Token het token dat in stap 5 is gekopieerd. Klik tot slot op Verzenden. Als alles in orde is, ontvangt u een 200 OK-reactie en in het JSON-veld zijn de taakstatus en andere details te zien.

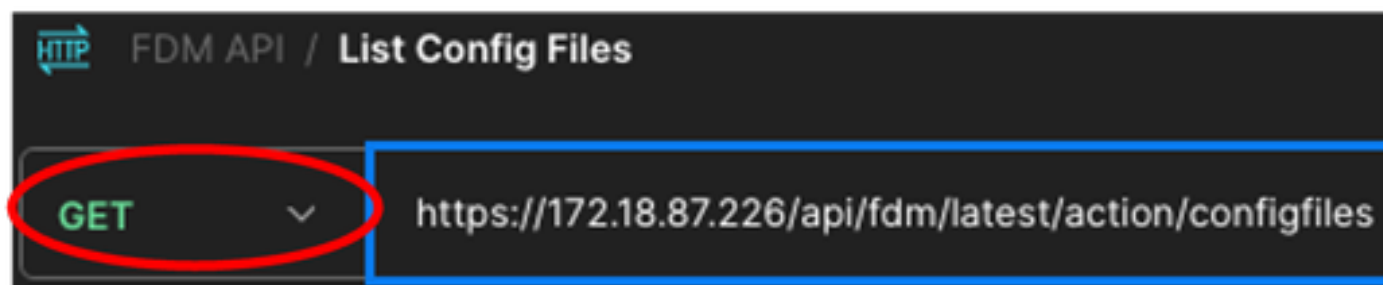


Postman - Verzoek om exportstatus configureren - Autorisatie en uitvoer

14. Herhaal stap 2, om een nieuw verzoek aan te maken, wordt GET ditmaal gebruikt.

15. Noem dit nieuwe verzoek: Lijst Config Files. Het wordt gemaakt als een GET-verzoek, ook op het moment dat u deze uitvoert, moet GET worden geselecteerd in het vervolgkeuzemenu. In het tekstvak naast GET introduceert u de volgende regel `https://<FDM IP`

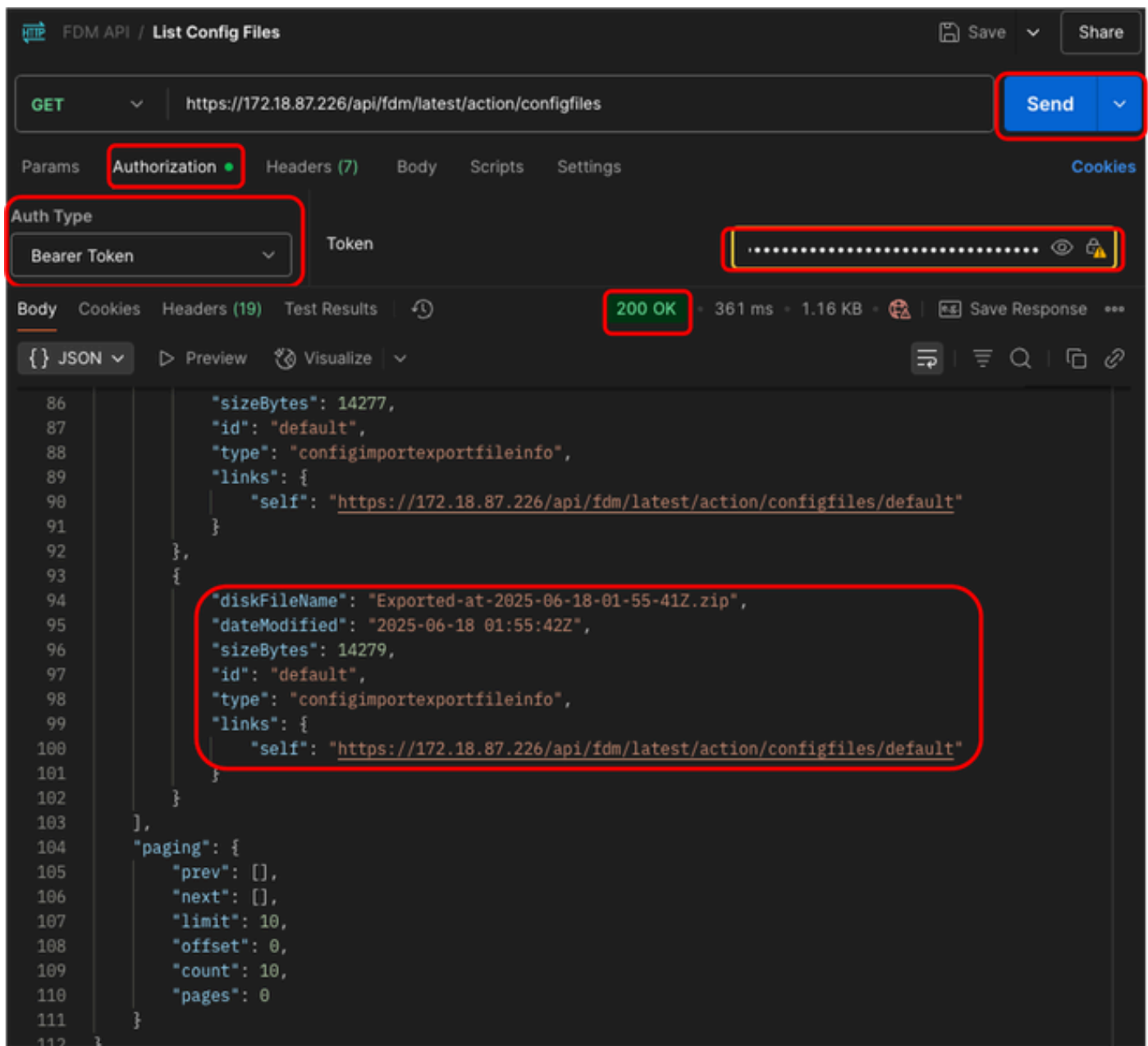
`ADD>/api/fdm/latest/action/configfiles`



Postman - Lijst geëxporteerde configuratiebestanden aanvragen

16. Selecteer op het tabblad Autorisatie de optie Token aan toonder als Auth Type in het vervolgkeuzemenu en plak de token die in stap 5 is gekopieerd in het tekstvak naast Token. Klik

tot slot op Verzenden. Als alles in orde is, ontvangt u een 200 OK-reactie en in het JSON-veld wordt de lijst met de geëxporteerde bestanden weergegeven. De meest recente staat onderaan. Kopieer de nieuwste bestandsnaam (recentere datum in de bestandsnaam) omdat deze in de laatste stap wordt gebruikt.

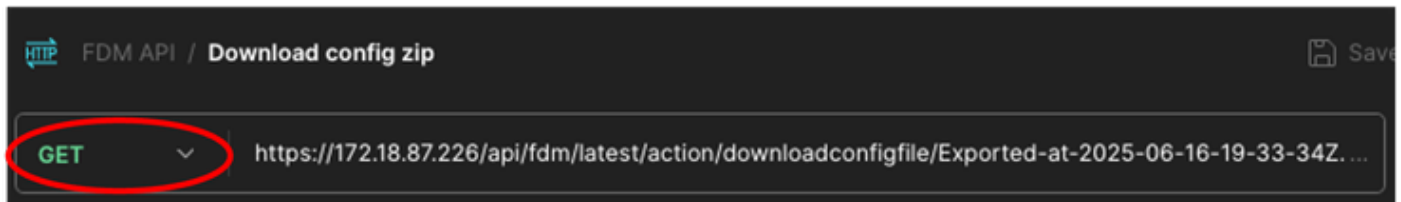


Postman - Lijst geëxporteerde Config-bestanden aanvragen - Autorisatie en uitvoer

17. Herhaal stap 2, om een nieuw verzoek aan te maken, wordt GET ditmaal gebruikt.

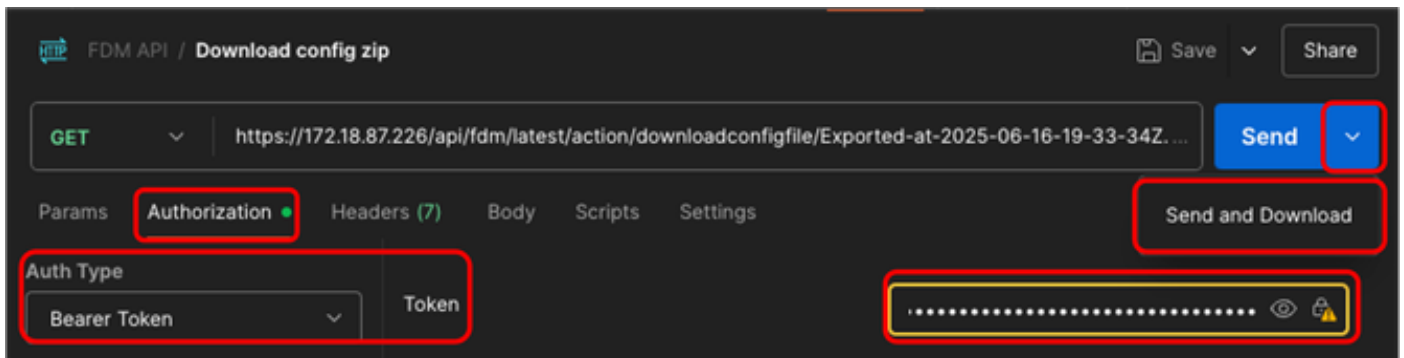
18. Bel dit nieuwe verzoek: Download config zip. Het wordt gemaakt als een GET-verzoek, ook op het moment dat u deze uitvoert, moet GET worden geselecteerd in het vervolgkeuzemenu. In het tekstvak naast GET introduceert u de volgende regel en plakt u aan het einde de bestandsnaam die u hebt gekopieerd in stap 16. `https://<FDM IP`

`ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip>`



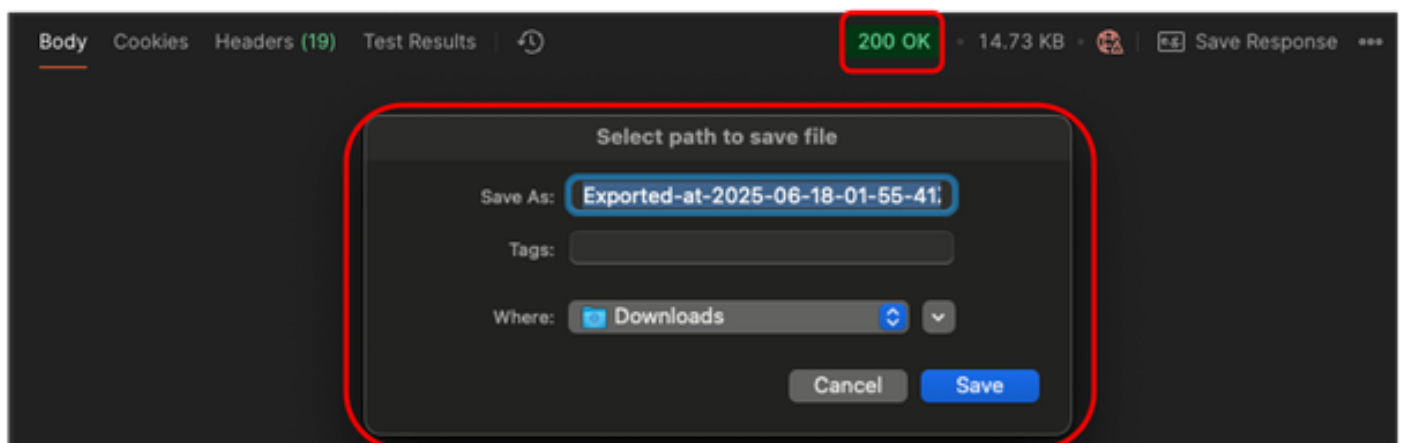
Postman - Bestandsaanvraag Config.zip downloaden

19. Op het tabblad Autorisatie selecteert u Token aan toonder als Auth Type in de vervolgkeuzelijst en plakt u in het tekstvak naast Token het token dat in stap 5 is gekopieerd. Klik ten slotte op de pijl omlaag naast Verzenden en kies Verzenden en Downloaden.



Postman - Config.zip File Request downloaden - Autorisatie

20. Als alles in orde is, ontvangt u een 200 OK-antwoord en wordt er een pop-upvenster weergegeven waarin wordt gevraagd naar de doelmap waarin het bestand configuration.zip wordt opgeslagen. Dit .zip-bestand kan nu worden geüpload naar de Firewall Migration Tool.



Postman - Config.zip File Request downloaden - Opslaan

Firewall Migration Tool

21. Open Firewall Migration Tool en selecteer Cisco Secure Firewall Device Manager (7.2+) in het vervolgkeuzemenu Select Source Configuration (Bronconfiguratie selecteren) en klik op Migratie starten.

Firewall Migration Tool (Version 7.7)

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-selectie

22. Controleer eerst het keuzerondje Firewall Device Manager migreren (Alleen gedeelde configuraties) en klik op Doorgaan.

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 - Alleen gedeelde FDM-migratieconfiguraties

23. Klik in het linkerdeelvenster (Handmatige configuratie uploaden) op Uploaden.

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>.

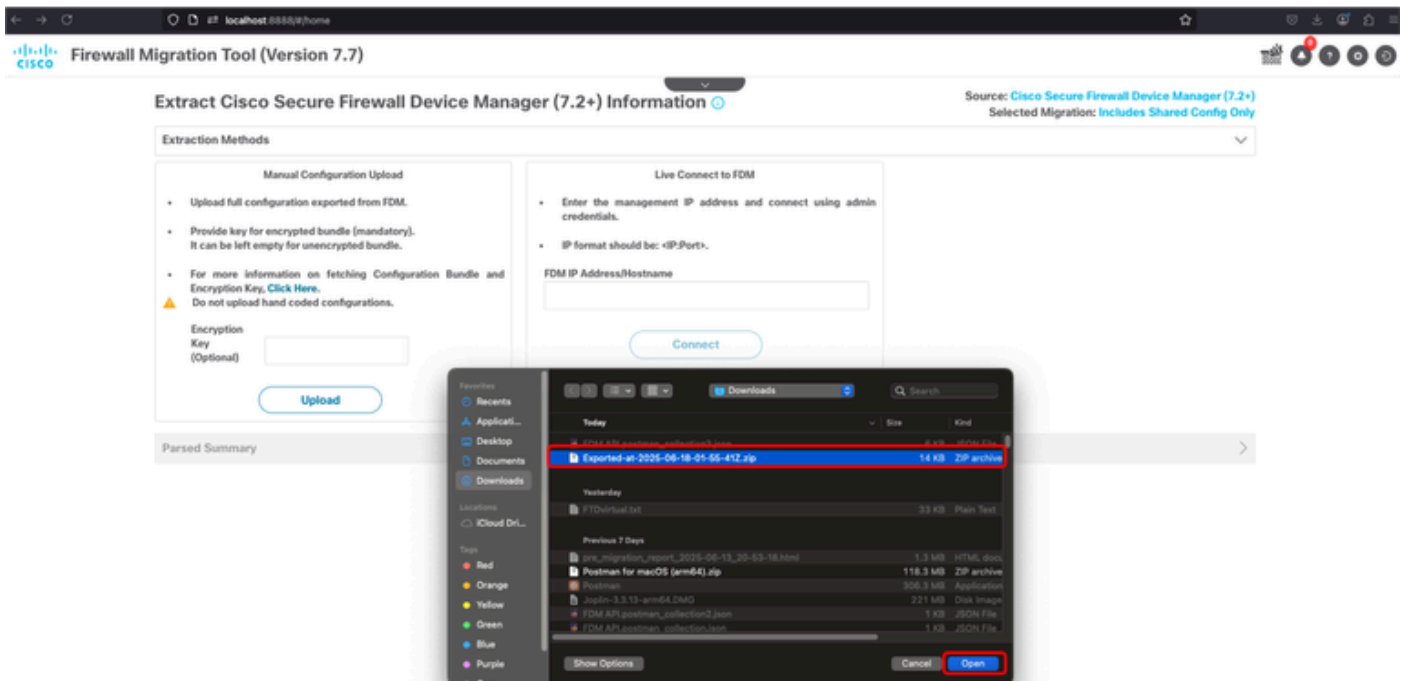
FDM IP Address/Hostname

Connect

Parsed Summary

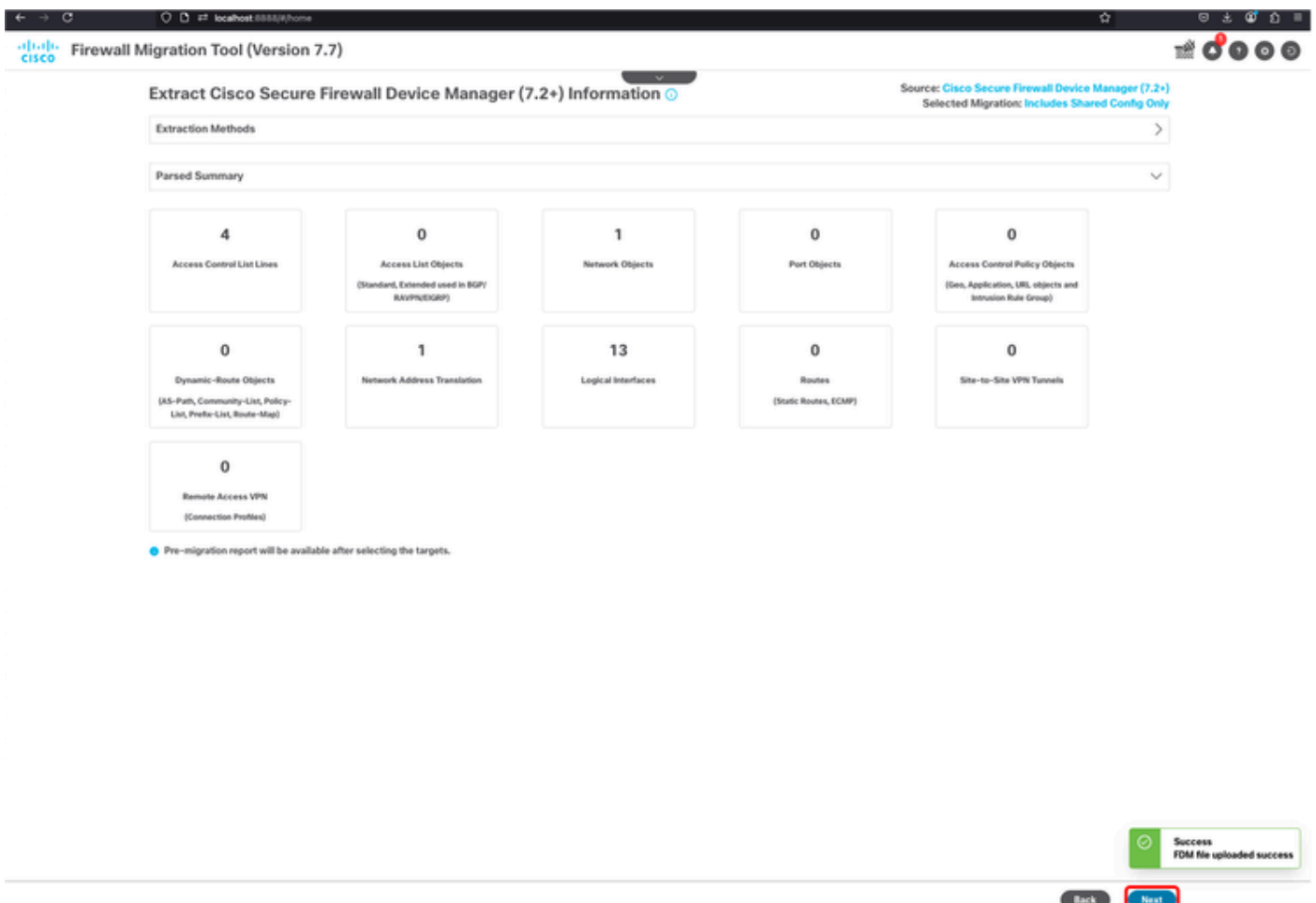
FMT - Config.zip-bestand uploaden

24. Selecteer het geëxporteerde zip-configuratiebestand in de map die u eerder hebt opgeslagen en klik op Openen.



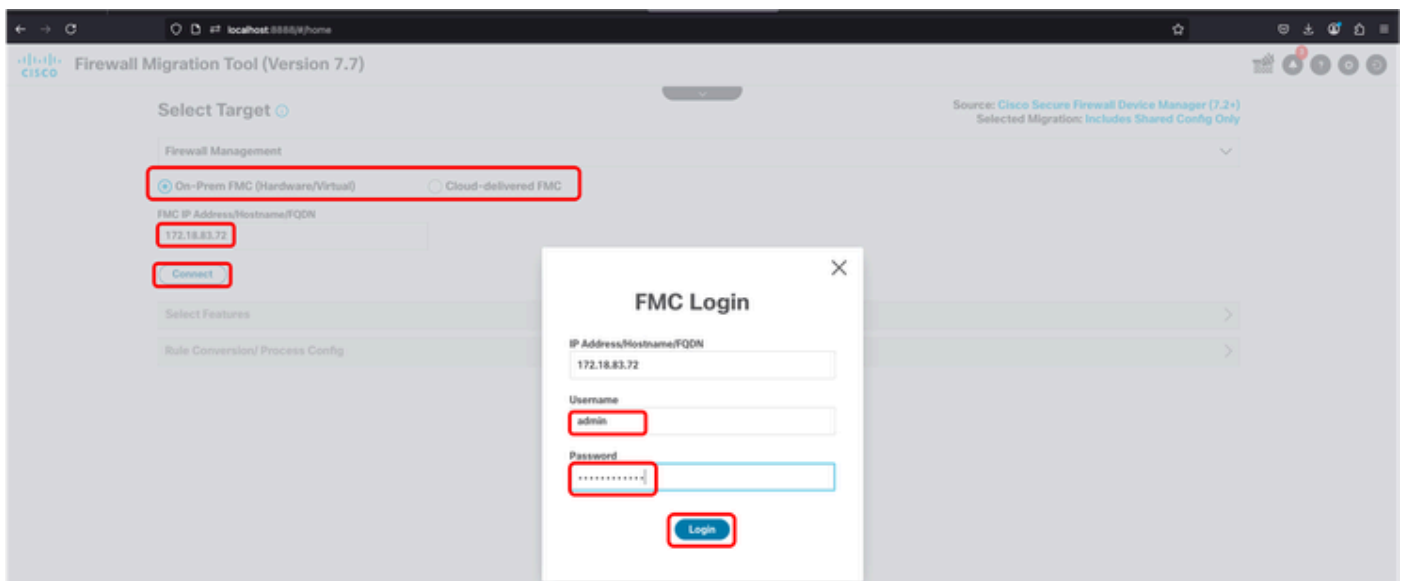
FMT - Bestandselectie Config.zip

25. Als alles verloopt zoals verwacht, wordt de samenvatting weergegeven. In de rechterbenedenhoek is ook een pop-up te zien die aangeeft dat het FDM-bestand met succes is geüpload. Klik op Next (Volgende).



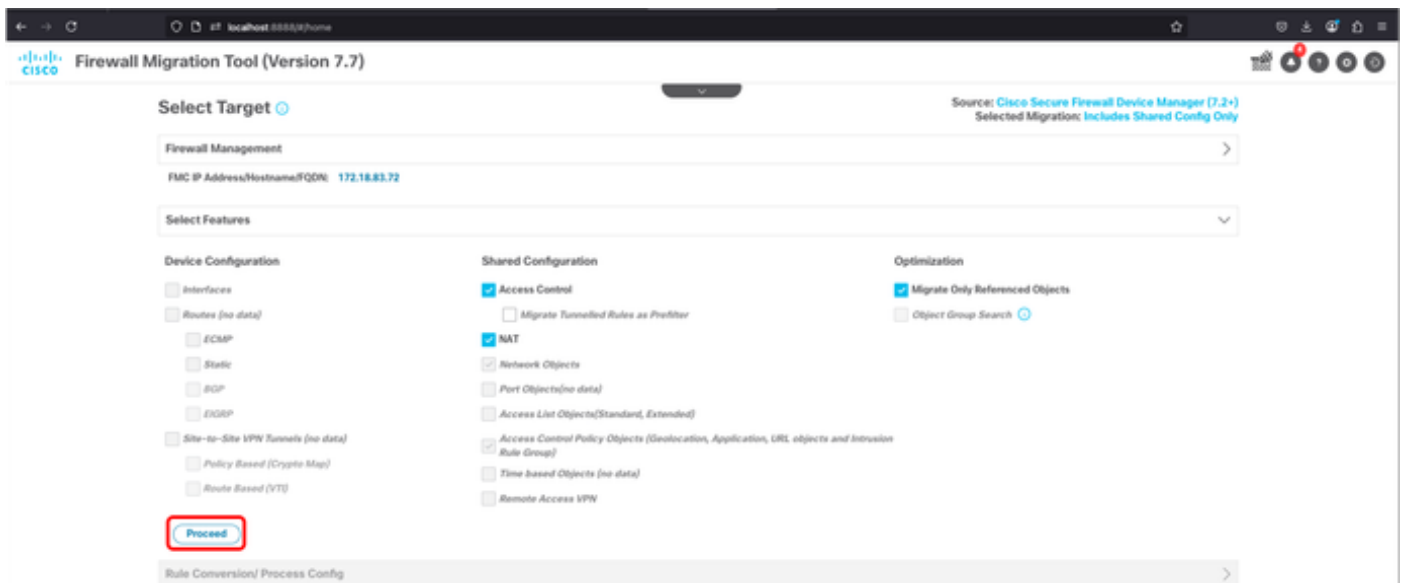
FMT - Samenvatting ontleden

26. Controleer de optie die beter bij uw omgeving past (On-Prem FMC of Cd-FMC). In dit scenario wordt een On-Prem FMC gebruikt. Typ het IP-adres van de FMC en klik op Verbinden. Er verschijnt een nieuw pop-upvenster waarin om FMC-referenties wordt gevraagd, waarna u op Login klikt nadat u deze informatie hebt ingevoerd.



Inloggen bij FMT - FMC Target

27. Het volgende scherm toont de beoogde FMC en de functies die zullen worden gemigreerd. Klik op Doorgaan.



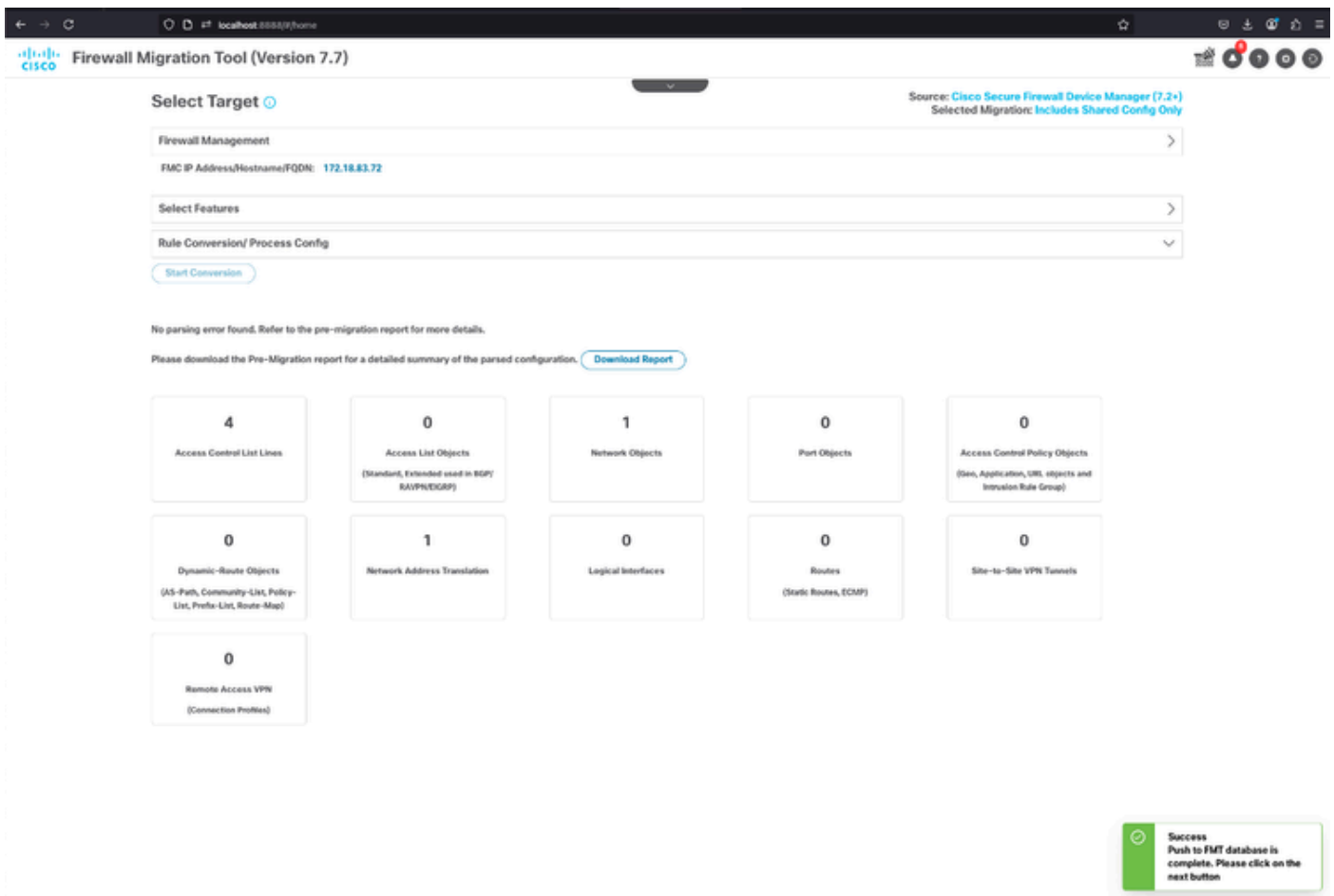
FMT - FMC-doel - Selectie van functies

28. Zodra het doel van de FMC is bevestigd, klikt u op de knop Conversie starten.



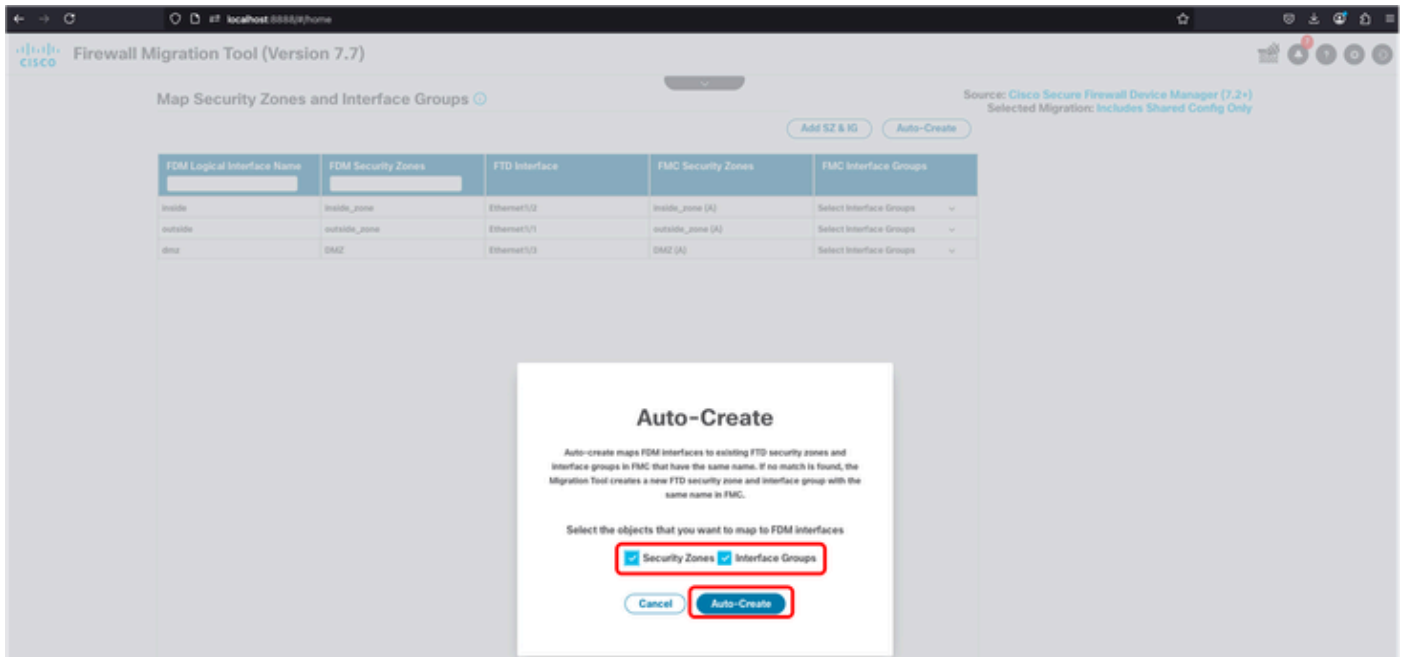
FMT - Config-conversie starten

29. Als alles verloopt zoals verwacht, wordt in de rechterbenedenhoek een pop-up weergegeven met de mededeling dat de push naar de FMT-database is voltooid. Klik op Next (Volgende).



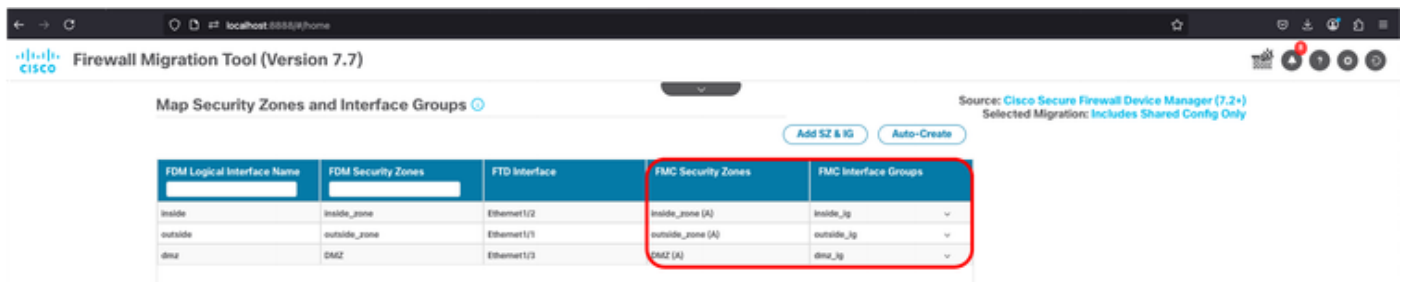
FMT - Database-push voltooid

30. In het volgende scherm moet u de beveiligingszones en interfacegroepen handmatig maken of de optie Automatisch maken kiezen. In dit scenario wordt automatisch maken gebruikt.



FMT - Automatische creatie van beveiligingszones en interfacegroepen

31. Na voltooiing worden in de tabel in de vierde en vijfde kolom respectievelijk de beveiligingszone en de interfacegroep weergegeven.



FMT - Beveiligingszones en interfacegroepen met succes gemaakt

32. In het volgende scherm kunt u ACL optimaliseren of alleen ACP, Objecten en NAT valideren. Als u klaar bent, klikt u op de knop Valideren.

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 Actions Save

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 - ACL optimaliseren - migratie valideren

33. Het duurt een paar minuten voordat de validering is voltooid.

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 Actions Save

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 - Validatie in uitvoering

34. Wanneer u klaar bent, laat FMT u weten dat de configuratie met succes is gevalideerd en de volgende stap is op de knop Configuratie indrukken klikken.

×

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 - Validatie geslaagd - Configuratie naar FMC duwen

35. Klik ten slotte op de knop Doorgaan.

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 - Ga verder met Config Push

36. Als alles verloopt zoals verwacht, wordt de melding Migratie geslaagd weergegeven. FMT vraagt u om in te loggen bij FMC en het gemigreerde beleid naar FTD te implementeren.

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 BGP, NAT/NoNAT)	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	1	Not selected for migration	Not selected for migration	Not selected for migration
Dynamic-Route Objects (IS-Path, Community-List, Policy-List, Prefix-List, Route-Map)	Network Address Translation	Logical Interfaces	Routers (Static Routes, EIGRP)	Site-to-Site VPN Tunnels
Not selected for migration				
Remote Access VPN (Connection Profiles)				

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 - Melding van geslaagde migratie

VCC-verificatie

37. Na de aanmelding bij het VCC worden de ACS-en NAT-beleidslijnen weergegeven als FTD-Mig. Nu kunt u doorgaan met het implementeren van de nieuwe FTD.

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

VCC - ACS gemigreerd

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-1750297649	Threat Defense	Targeting 0 device(s)

FMC - NAT-beleid gemigreerd

Gerelateerde informatie

- [FMT - Gids voor FDM-migratie naar FMC](#)
- [Opmerkingen bij FMT-release](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.