

Migrate FDM to FMC Through FMT Using Configuration.zip File

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Background Information](#)

[Considerations](#)

[Configuration](#)

[API Requests - Postman](#)

[Firewall Migration Tool](#)

[FMC Verification](#)

[Related Information](#)

Introduction

This document describes how to generate the configuration file.zip of a Secure Firewall Device Manager (FDM) to be migrated to an FMC using FMT.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

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

Components Used

The information in this document is based on these software versions.

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postman 11.50.0

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

- FDM can be migrated now to FMC in different ways. In this document, the scenario that is going to be explored is the generation of the configuration .zip file using API requests and later upload of that file to FMT to migrate the configuration to FMC.
- The steps shown in this document start using Postman directly so, it is recommended that you have Postman already installed. The PC or laptop you are going to use, must have access to FDM and FMC, also FMT must be installed and running.

Considerations

- This document is focused on the configuration .zip file generation more than in FMT use.
 - FDM migration using configuration .zip file, is for non-live migrations and do not require immediately a destination FTD.
-

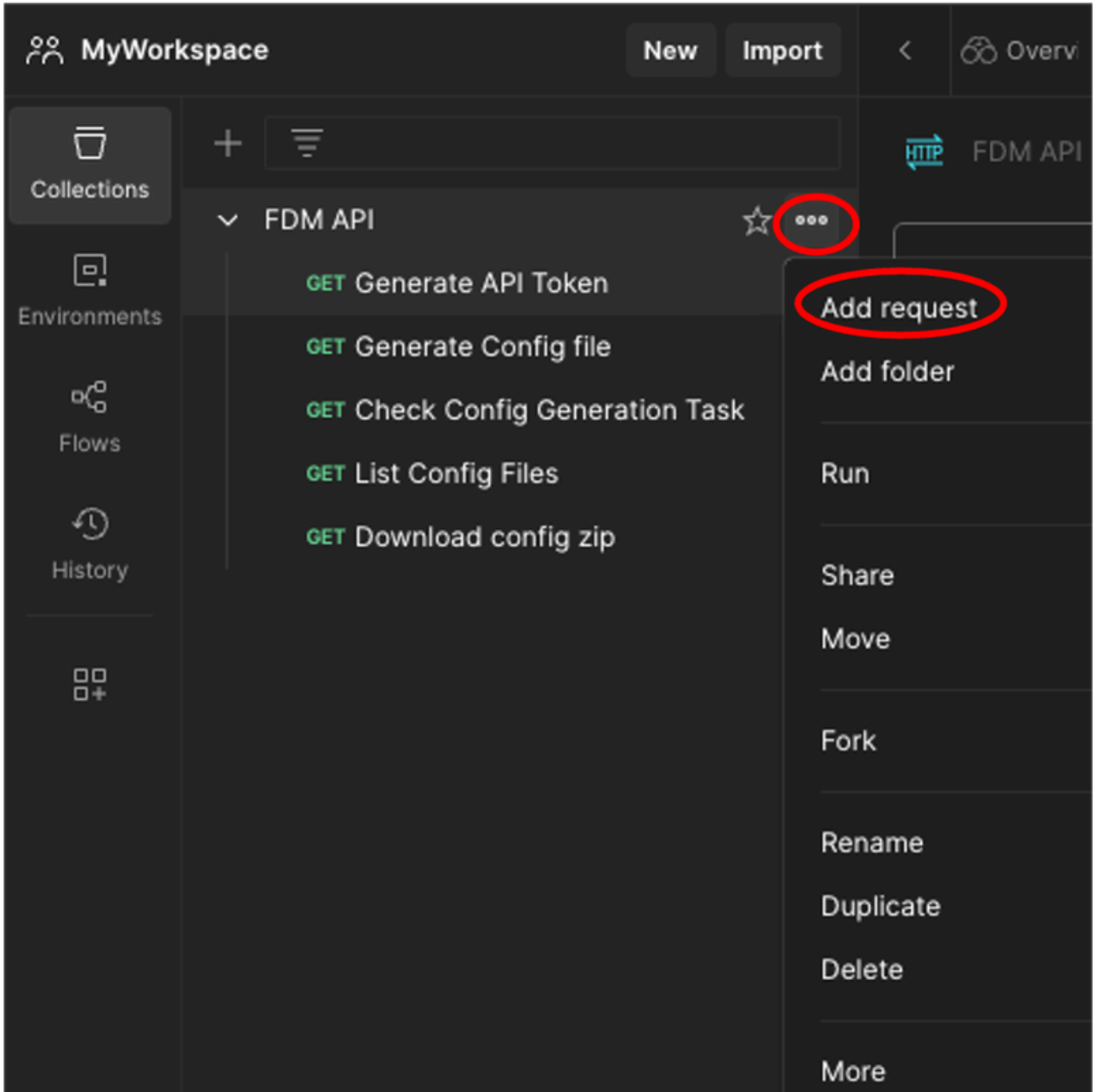


Warning: Choosing this mode, allows to migrate only Access Control Policy (ACP), Network Address Translation Policy (NAT) and Objects. In regards the objects those must be used in an ACP rule or NAT, to be migrated, otherwise those are ignored.

Configuration

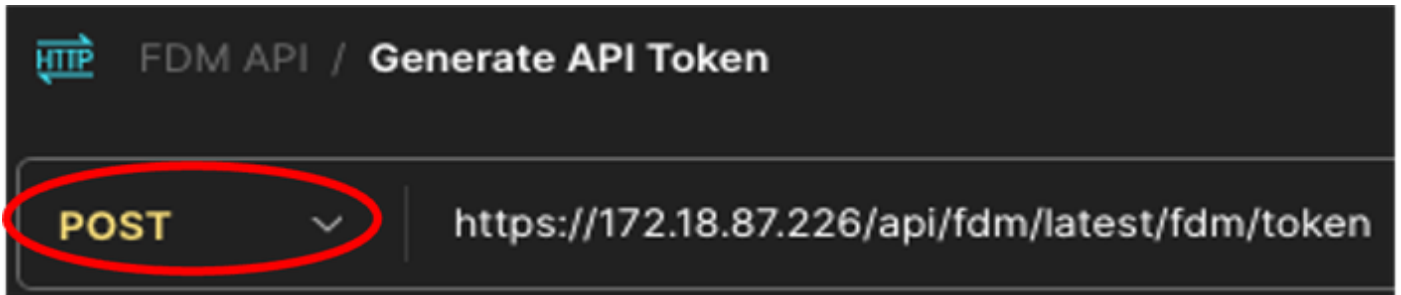
API Requests - Postman

1. In Postman, create a new **collection** (in this scenario FDM API is used).
2. Click the **3 dots** and after click **Add request**.



Postman - Collection Creation and Request Addition

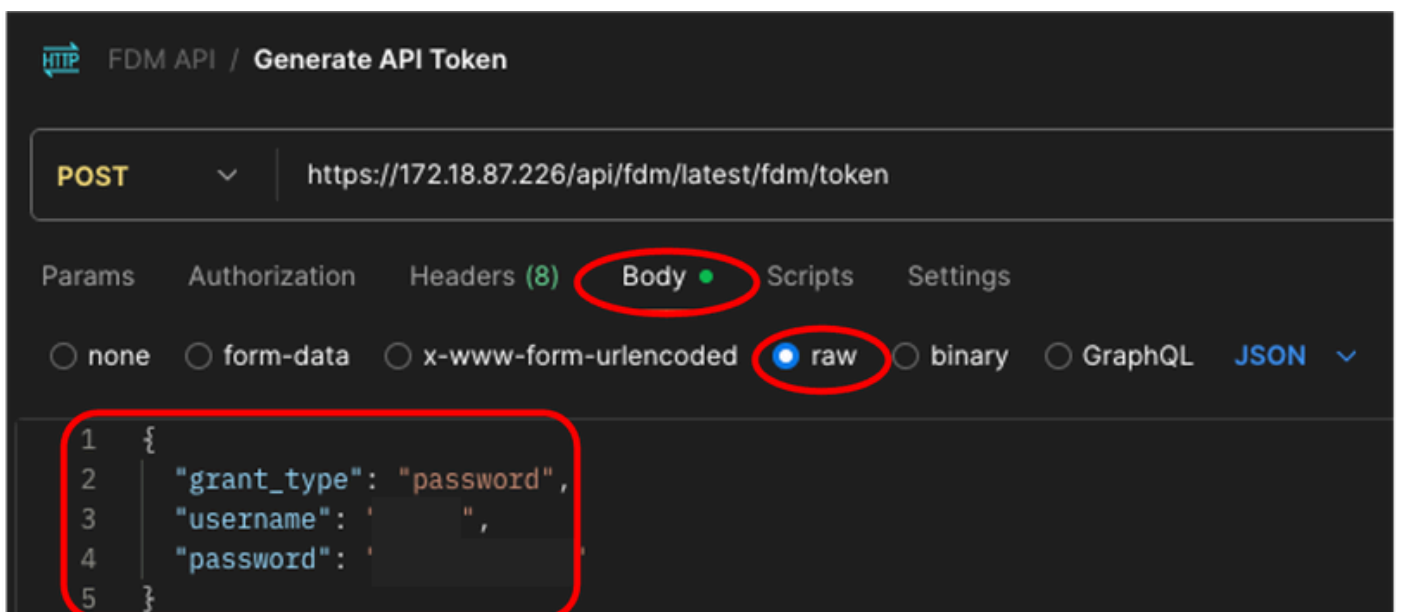
3. Call this new request: Generate API Token. It is going to be created as a GET request, but at the time you are executing this one, **POST** must be selected from the drop-down menu. In the text box next to **POST**, introduce the next line **https://<FDM IP ADD>/api/fdm/latest/fdm/token**



Postman - Token Request

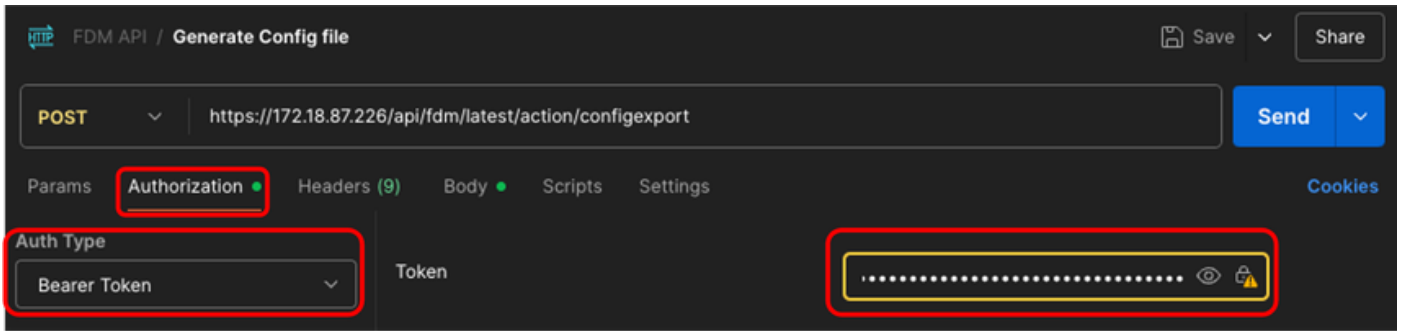
4. In the **Body** tab, select **raw** option and introduce the **credentials** to access FTD (FDM) device using this format.

```
{  
  "grant_type": "password",  
  "username": "username",  
  "password": "password"  
}
```



Postman - Token Request Body

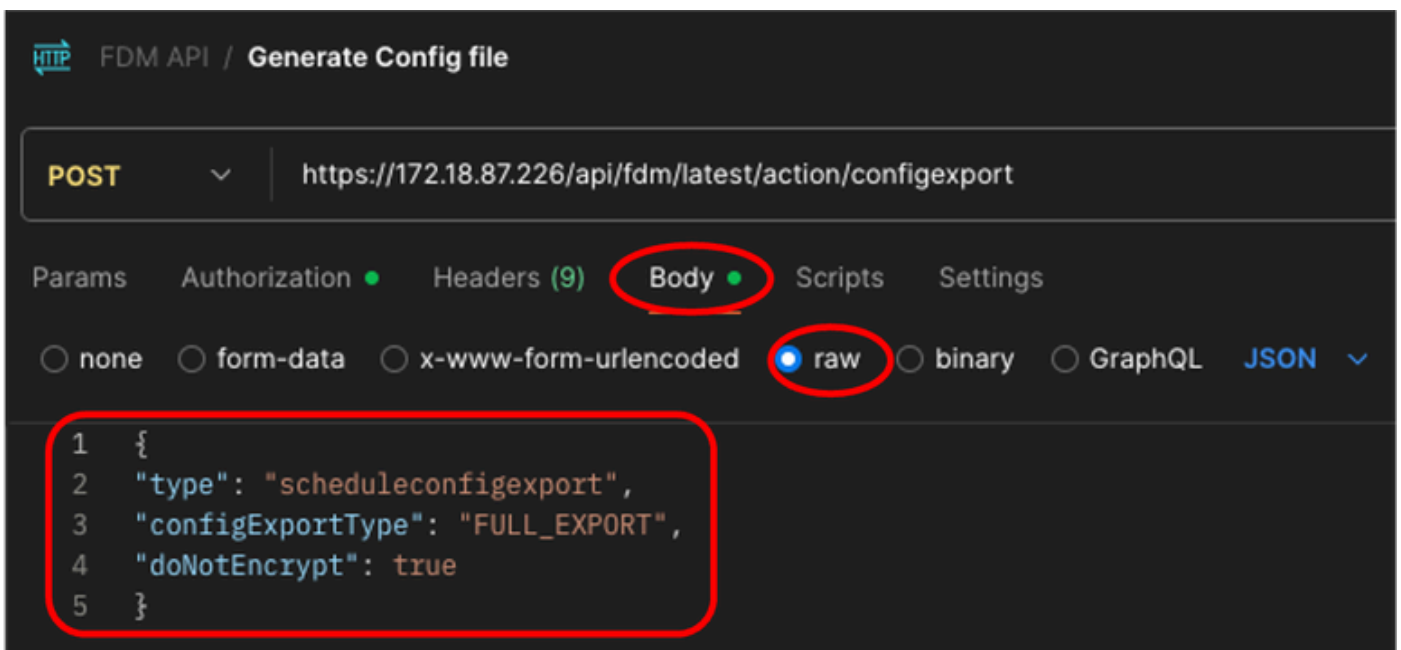
5. Finally, click **Send** to get your Access Token. If everything is fine, you receive a 200 OK response. Make a copy of the entire token (inside the double quotes) because it is going to be used in later steps.



Postman - Generate Config File Request - Authorization

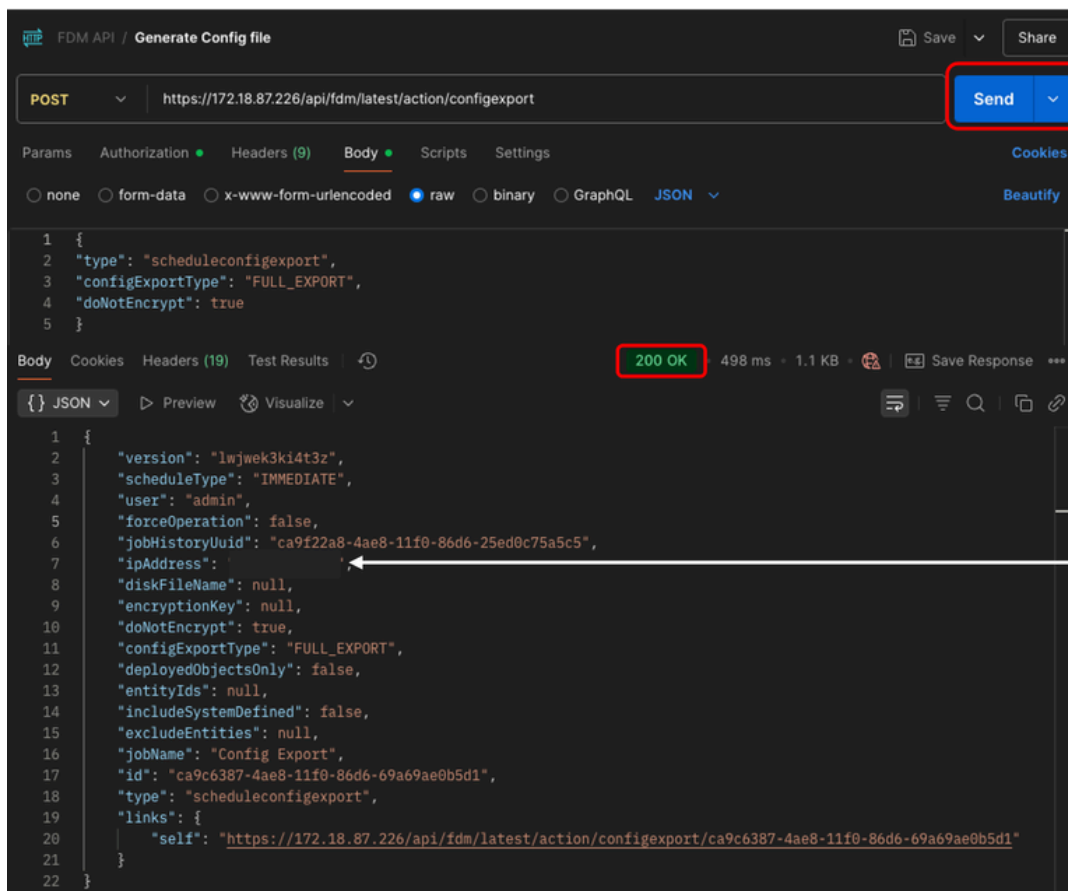
9. In **Body** tab, select **raw** option and introduce this information.

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



Postman - Generate Config File Request - Body

10. Finally, click **Send**. If everything is fine, you receive a 200 OK response.

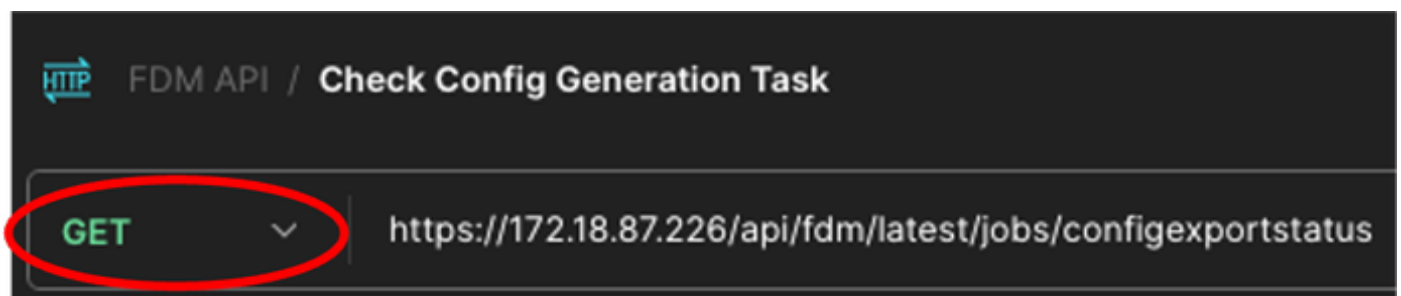


This IP address is the one that is connecting to the FTD through the requests.

Postman - Generate Config File Request - Output

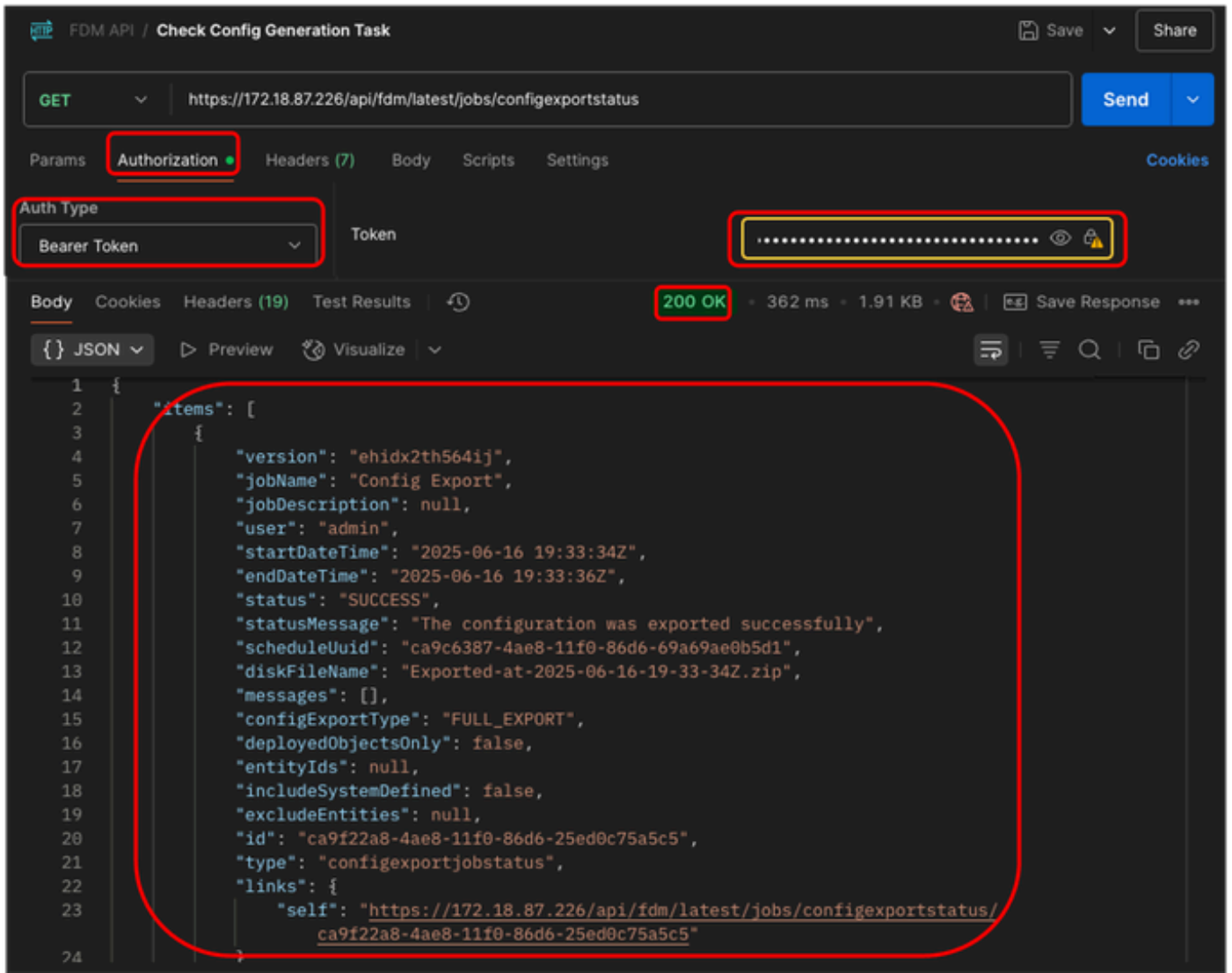
11. Repeat step 2, to create a new **request**. **GET** is going to be used this time.

12. Call this new request: Check Config Generation Task. It is going to be created as a **GET** request. Also, the time you are executing this one, **GET** must be selected from the drop-down menu. In the text box next to **GET**, introduce the next line **https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus**



Postman - Check Config Export Status Request

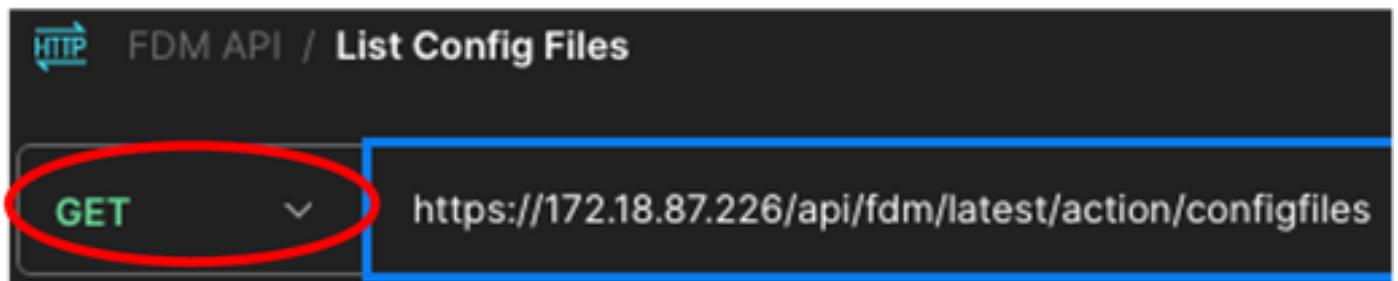
13. In **Authorization** tab, select **Bearer Token** as Auth Type in the drop down menu, and in the text box next to Token paste the **token** copied in step 5. Finally, click **Send**. If everything is fine, you receive a 200 OK response and in the JSON field, the task status and other details can be seen.



Postman - Config Export Status Request - Authorization and Output

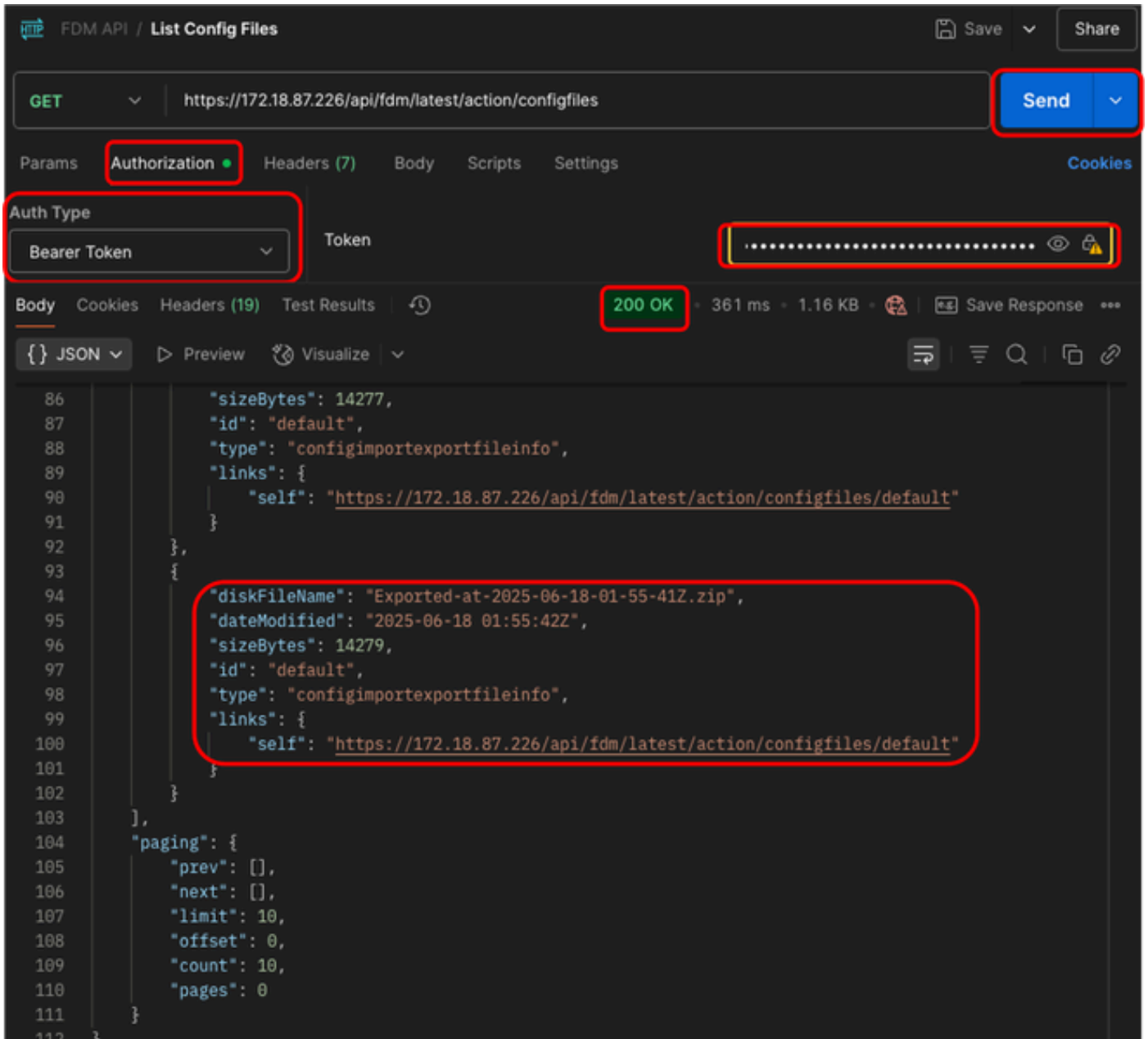
14. Repeat step 2, to create a new **request**, **GET** is going to be used this time.

15. Call this new request: List Config Files. It is going to be created as a **GET** request, also at the time you are executing this one, **GET** must be selected from the drop-down menu. In the text box next to **GET**, introduce the next line **https://<FDM IP ADD>/api/fdm/latest/action/configfiles**



Postman - List Exported Config Files Request

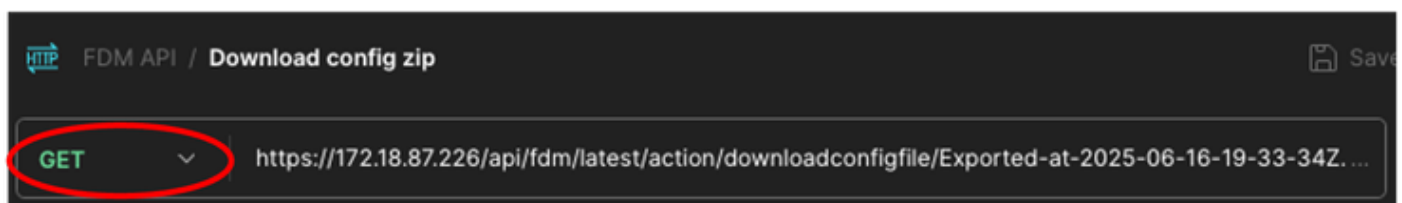
16. In **Authorization** tab, select **Bearer Token** as Auth Type in the drop down menu, and in the text box next to Token paste the **token** copied in step 5. Finally, click **Send**. If everything is fine, you receive a 200 OK response and in the JSON field, the list of the exported files is shown. The more recent one is listed at the bottom. Copy the latest **file name** (more recent date in the file name) because it is going to be used in the last step.



Postman - List Exported Config Files Request - Authorization and Output

17. Repeat step 2, to create a new request, **GET** is going to be used this time.

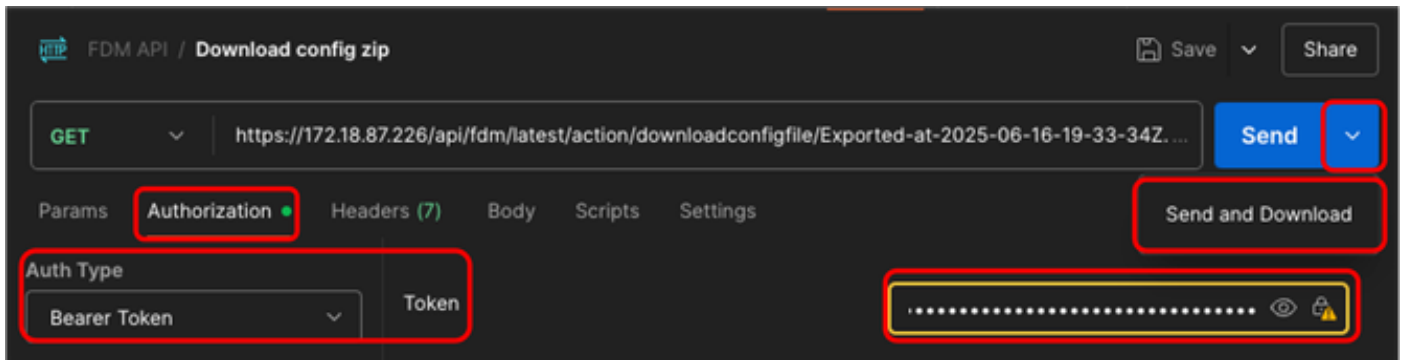
18. Call this new request: Download config zip. It is going to be created as a **GET** request, also at the time you are executing this one, **GET** must be selected from the drop-down menu. In the textbox next to **GET**, introduce the next line, pasting at the end the **file name** you copied in step 16. **https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported_File_name.zip >**



Postman - Download Config.zip File Request

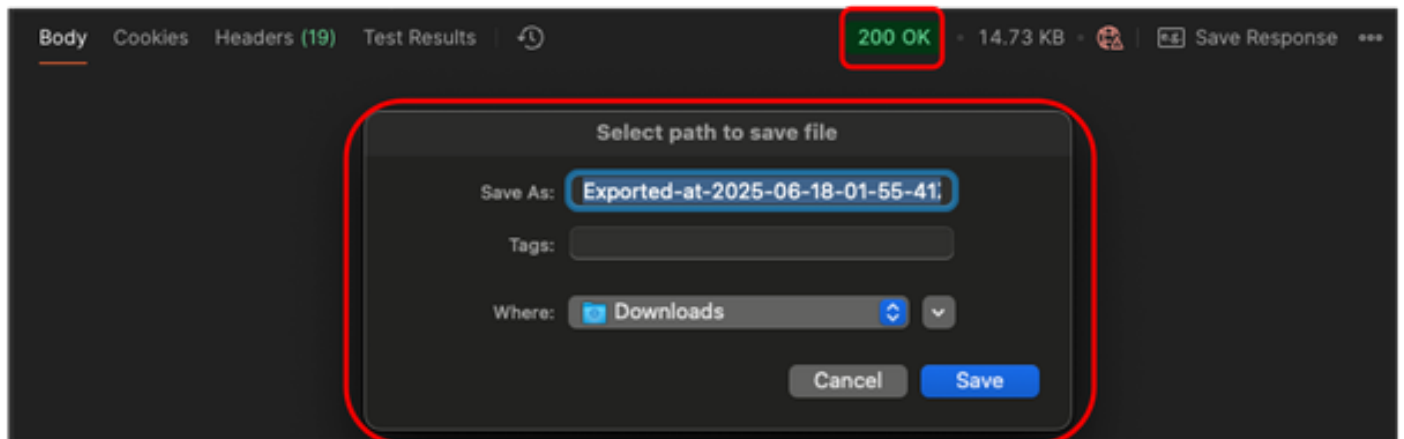
19. In **Authorization** tab, select **Bearer Token** as Auth Type in the drop down menu, and in the text box next to Token paste the **token** copied in step 5. Finally, click the **down arrow** next to Send and choose **Send**

and Download.



Postman - Download Config.zip File Request - Authorization

20. If everything is fine, you receive a 200 OK response and a pop-up window is displayed asking for the destination folder where the configuration.zip file is going to be saved. This .zip file can now be uploaded to the Firewall Migration Tool.



Postman - Download Config.zip File Request - Save

Firewall Migration Tool

21. Open Firewall Migration Tool and in the Select Source Configuration drop down menu, select **Cisco Secure Firewall Device Manager (7.2+)** and click **Start Migration**.

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.
 - 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)**
 - 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 Selection

22. Check first Radio Button, **Migrate Firewall Device Manager (Shared Configurations Only)** and click **Continue**.

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. In the left panel (**Manual Configuration Upload**) click **Upload**.

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.

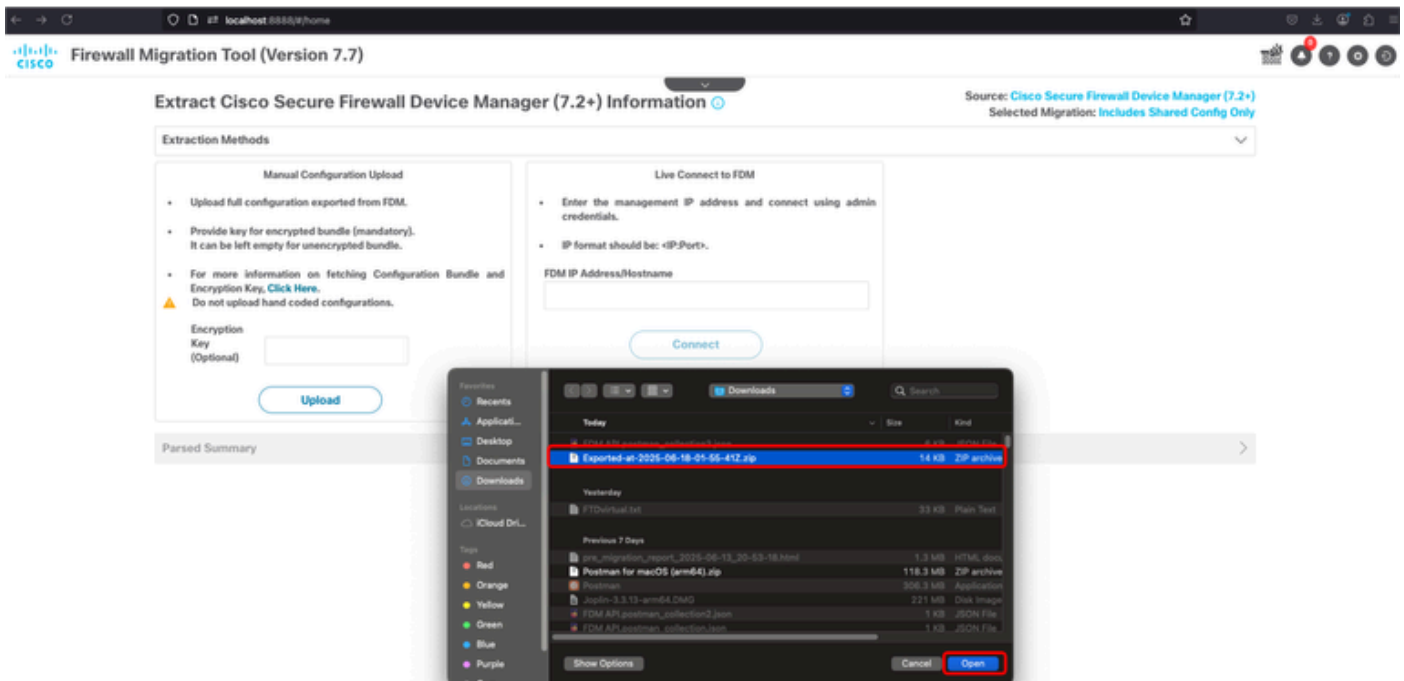
FDM IP Address/Hostname

Connect

Parsed Summary

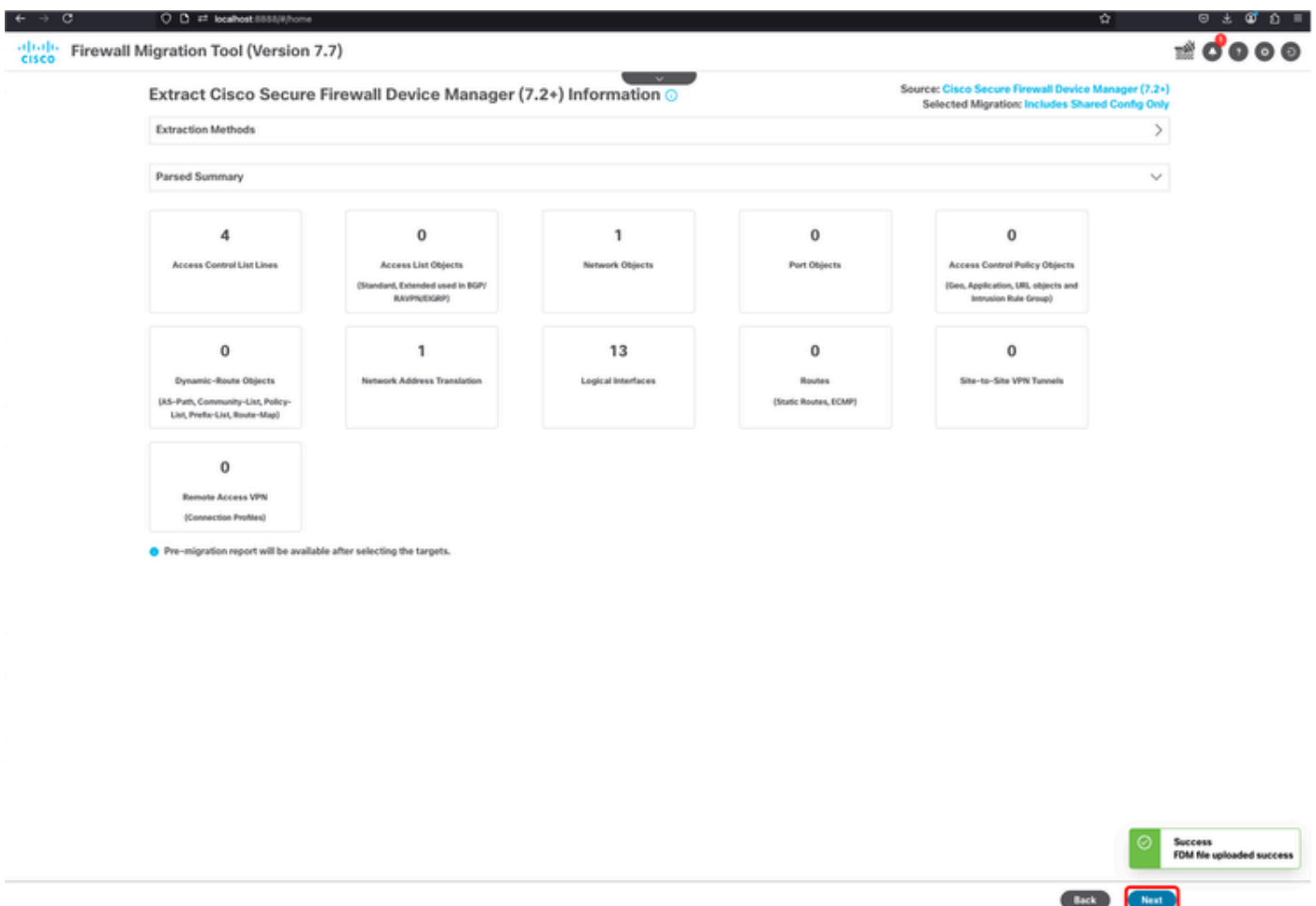
FMT - Upload Config.zip File

24. Select the **exported zip config file** in the folder you previously saved and click **Open**.



FMT - Config.zip File Selection

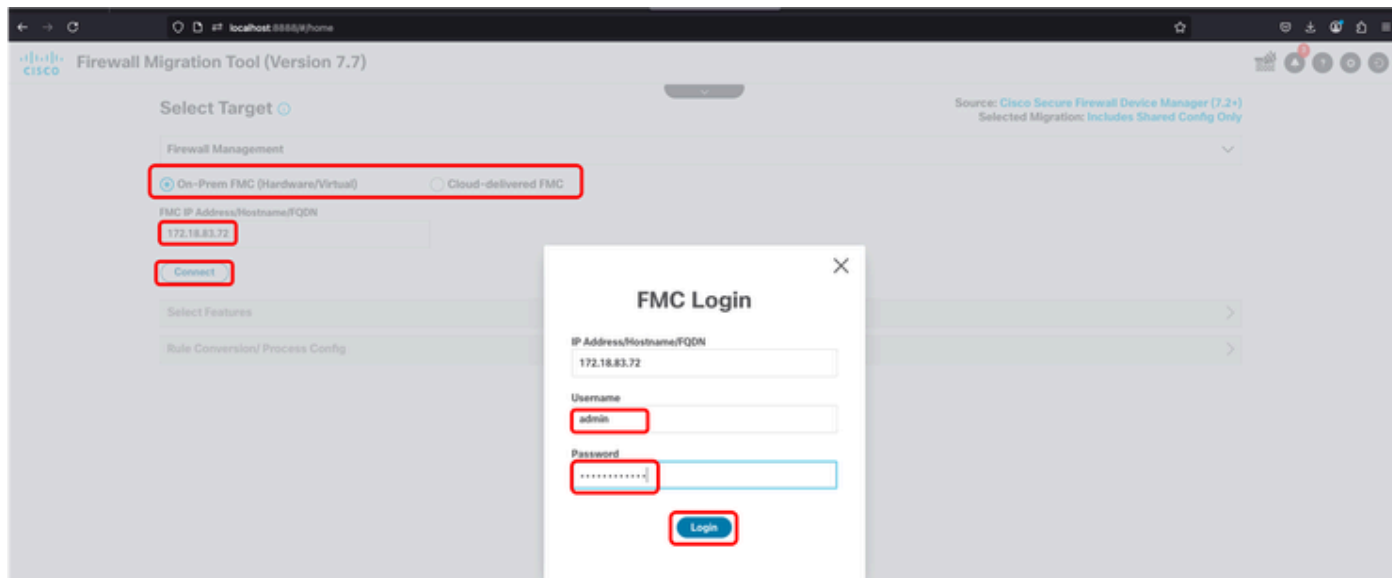
25. If everything goes as expected, the Parsed Summary is shown. Also, in the down right corner a pop-up can be seen informing FDM file was successfully uploaded. Click **Next**.



FMT - Parsing Summary

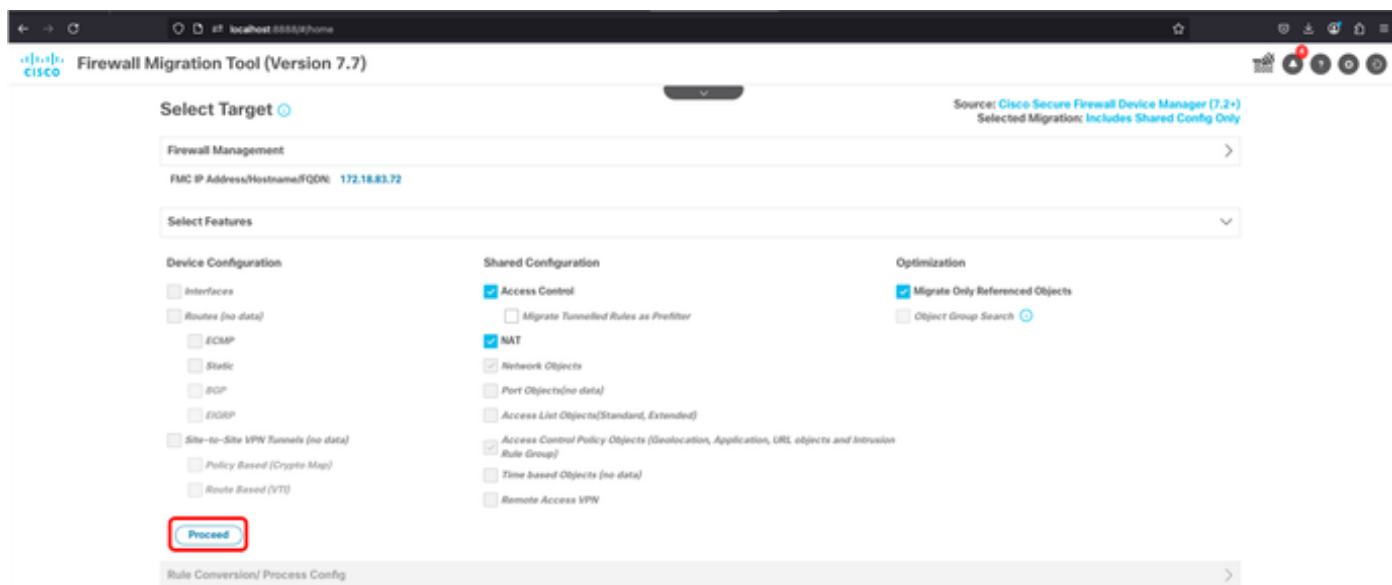
26. Check the option that better suits to your environment (On-Prem FMC or Cd-FMC). In this scenario, an

On-Prem FMC is used. Type the **FMC IP address** and click **Connect**. A new pop-up comes and asks for **FMC credentials**, after entering this information, click **Login**.



FMT - FMC Target log in

27. Next screen shows the target FMC and the features that are going to be migrated. Click **Proceed**.



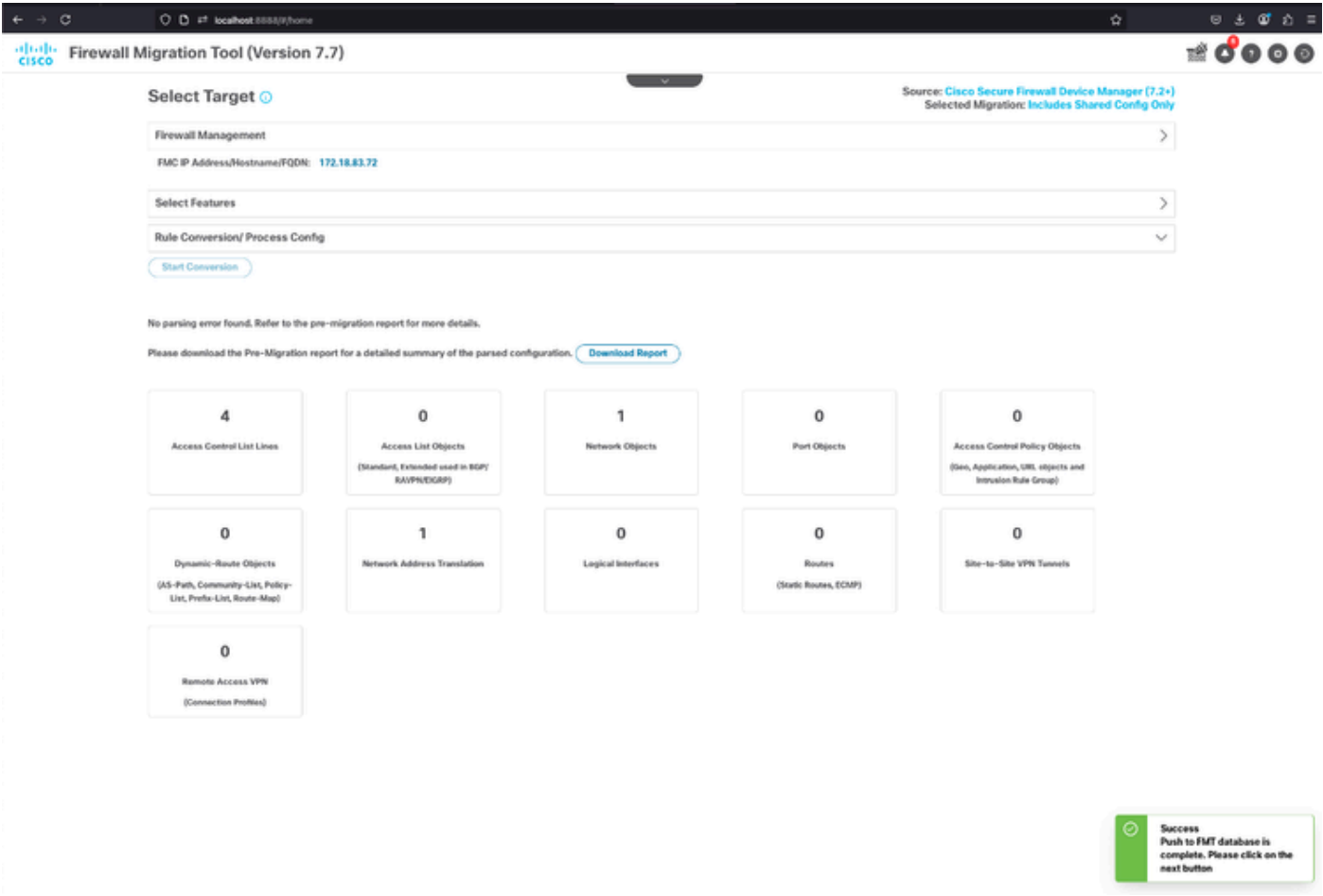
FMT - FMC Target - Features Selection

28. Once FMC Target is confirmed, click **Start Conversion** button.



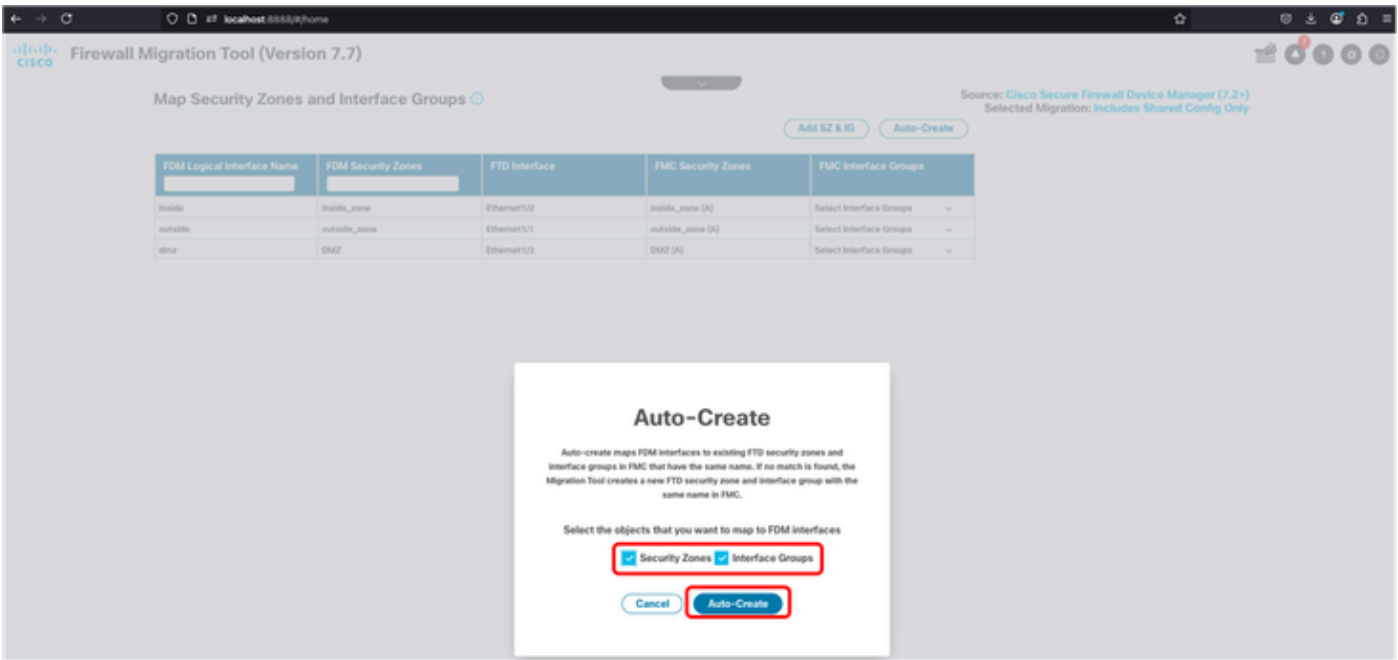
FMT - Starting Config Conversion

29. If everything goes as expected, a pop-up is shown in the down right corner informing that push to FMT database is complete. Click **Next**.



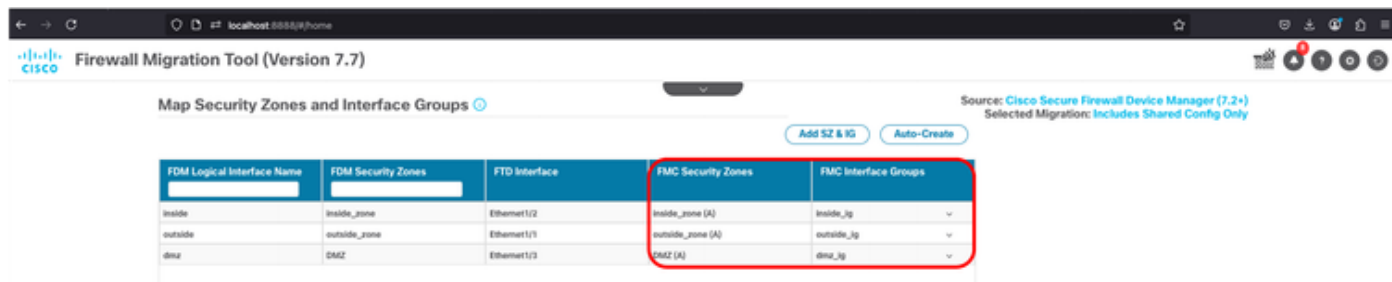
FMT - Database Push Successfully Completed

30. In the next screen, you must manually create, or choose auto-create the security zones and interface groups. In this scenario, auto-create is used.



FMT - Auto Creating Security Zones and Interface Groups

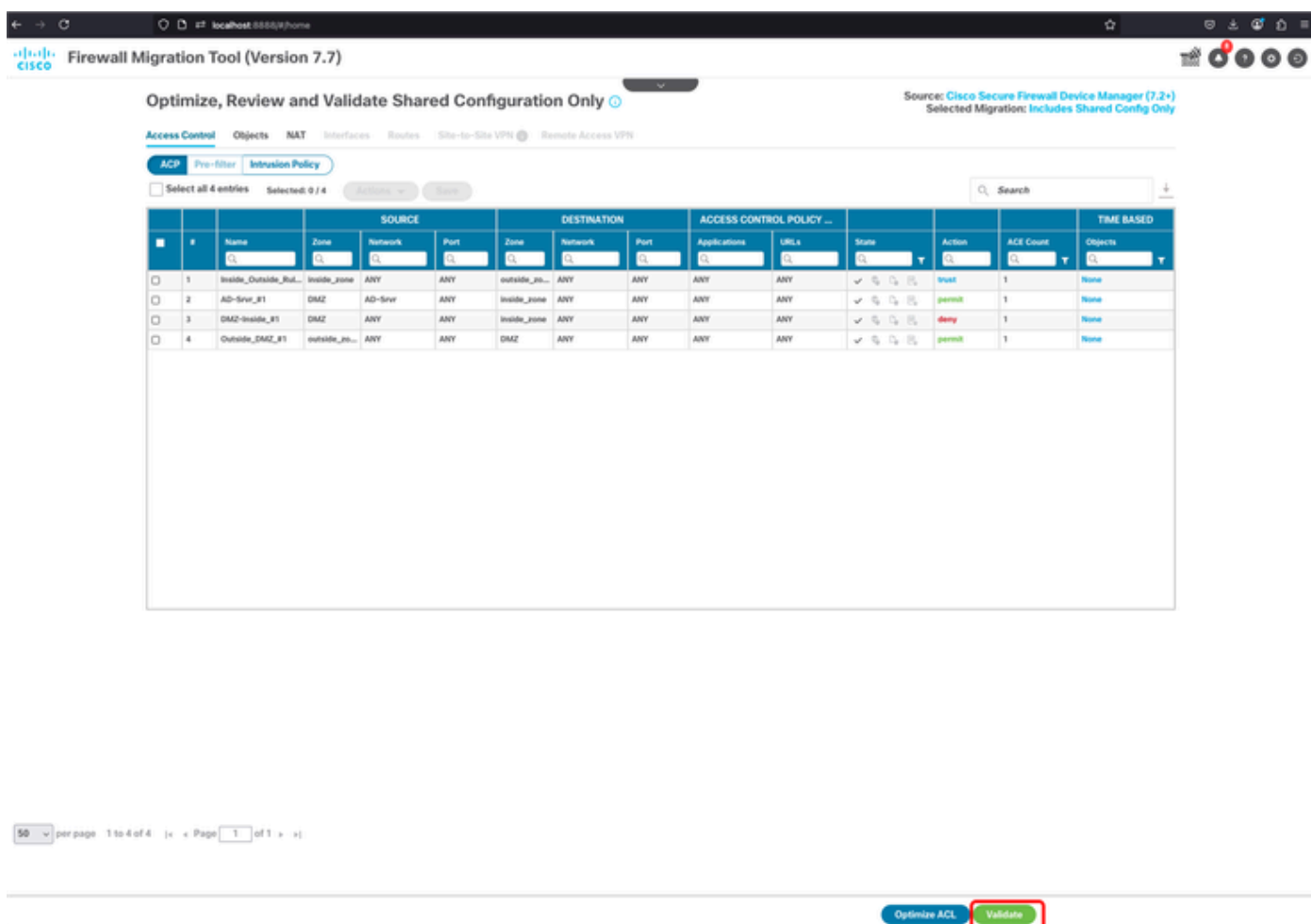
31. Once completed, the table shows in the 4th and 5th column, the Security Zone and Interface Group respectively.



FDM Logical Interface Name	FDM Security Zones	FTD Interface	FMC Security Zones	FMC Interface Groups
inside	inside_zone	Ethernet1/2	inside_zone (A)	inside_jg
outside	outside_zone	Ethernet1/1	outside_zone (A)	outside_jg
dmz	DMZ	Ethernet1/3	DMZ (A)	dmz_jg

FMT - Security Zones and Interface Groups Successfully Created

32. In the next screen, you can optimize ACL or just validate ACP, Objects and NAT. Once done, click **Validate** button.



#	Name	Zone	Network	Port	Zone	Network	Port	Applications	URLs	State	Action	ACE Count	Objects
1	Inside_Outside_But...	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 - Optimize ACL - Validate Migration

33. Validation take couple minutes to be completed.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration

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

ACP Pre-filter Intrusion Policy

Select all 4 entries Selected: 0 / 4 Actions Save

Search

	#	Name	Zone	Source	Port	Destination	Port	Access Control Policy	Applications	URLs	State	Action	ACE Count	Objects
<input type="checkbox"/>	1	Inside_Outside_Rol...	inside_zone	ANY	ANY	outside_zone	ANY	ANY	ANY	ANY	✓	trust	1	None
<input type="checkbox"/>	2	AD-Srvr_R1	DMZ	AD-Srvr	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	permit	1	None
<input type="checkbox"/>	3	DMZ-Inside_R1	DMZ	ANY	ANY	inside_zone	ANY	ANY	ANY	ANY	✓	deny	1	None
<input type="checkbox"/>	4	Outside_DMZ_R1	outside_zone	ANY	ANY	DMZ	ANY	ANY	ANY	ANY	✓	permit	1	None

FMT - Validation in Progress

34. Once done, FMT lets you know configuration has been successfully validated and next step is click **Push Configuration** button.

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 - Validation Succeeded - Push Configuration to FMC

35. Finally, click **Proceed** button.

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.



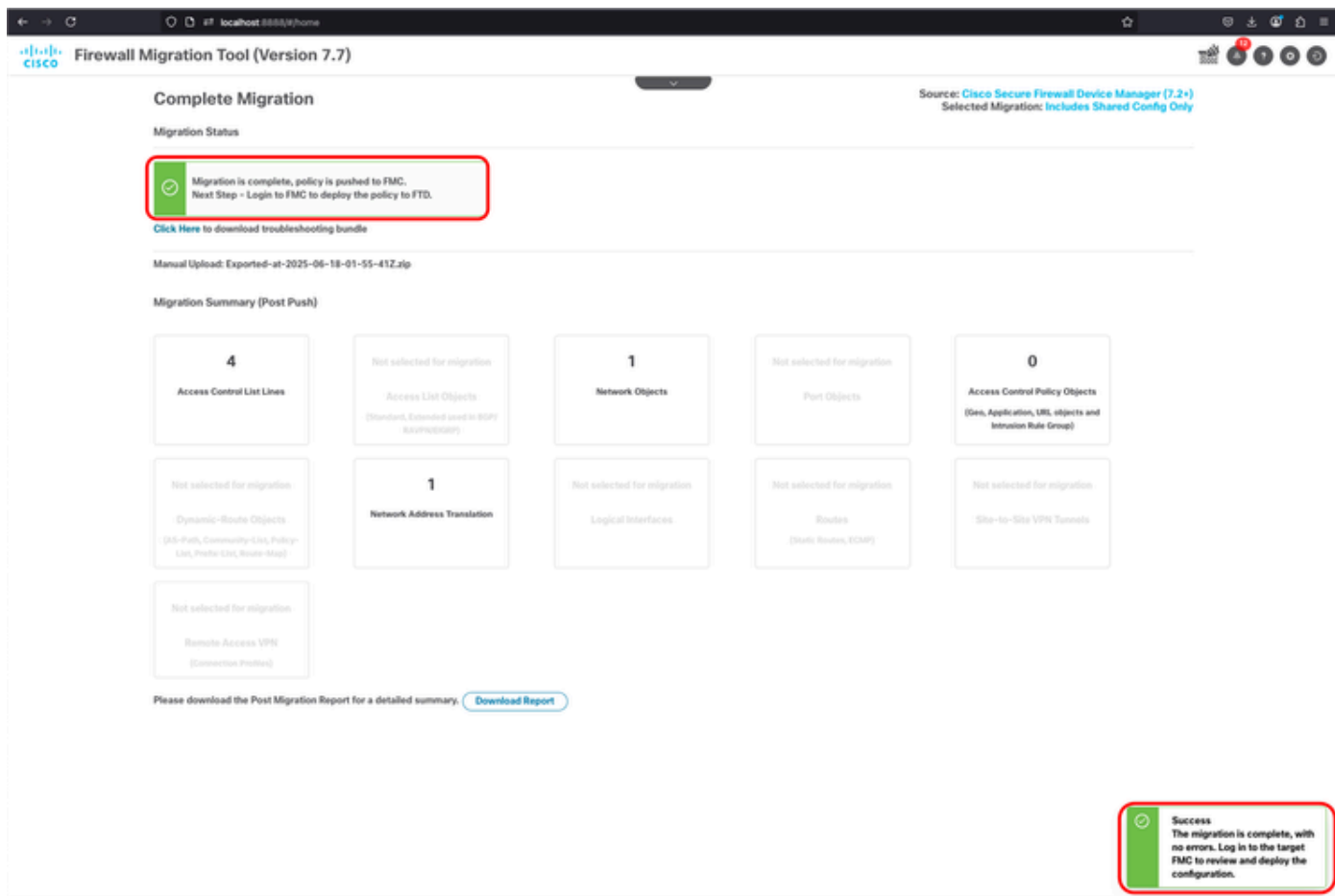
Click on Proceed to continue.

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 - Proceed With Config Push

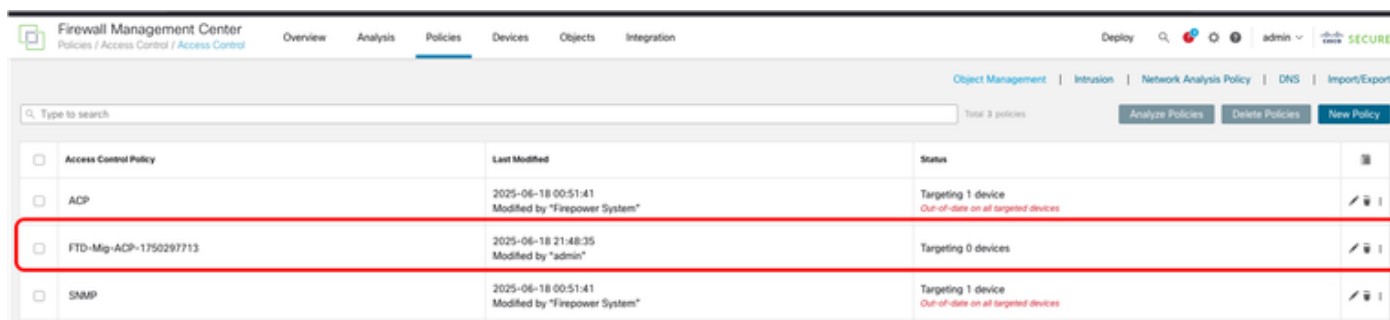
36. If everything goes as expected, Migration succeeded notification is shown. FMT asks you to log in to FMC and deploy the migrated policy to FTD.



FMT - Migration Succeeded Notification

FMC Verification

37. After log in to FMC, the ACP and NAT policies are shown as FTD-Mig. Now, you can proceed deploying to the new FTD.



FMC - ACP Migrated



FMC - NAT Policy Migrated

Related Information

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