

# 使用Configuration.zip文件通过FMT将FDM迁移到FMC

## 目录

---

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[背景信息](#)

[考虑事项](#)

[配置](#)

[API请求 — Postman](#)

[防火墙迁移工具](#)

[FMC验证](#)

[相关信息](#)

---

## 简介

本文档介绍如何生成要使用FMT迁移到FMC的安全防火墙设备管理器(FDM)的configuration file.zip。

## 先决条件

### 要求

Cisco 建议您了解以下主题：

- 思科防火墙威胁防御(FTD)
- 思科防火墙管理中心(FMC)
- 防火墙迁移工具(FMT)
- Postman API平台

### 使用的组件

本文档中的信息是基于这些软件版本的。

FTD 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Postman 11.50.0

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 背景信息

- FDM现在可以通过不同方式迁移到FMC。在本文档中，将要探索的场景是使用API请求生成配置.zip文件，然后将该文件上传到FMT以将配置迁移到FMC。
- 本文档中显示的步骤直接使用Postman，因此建议您已经安装Postman。要使用的PC或笔记本电脑必须能够访问FDM和FMC，还必须安装和运行FMT。

## 考虑事项

- 本文档重点介绍配置.zip文件的生成，而不是在FMT中使用。
- 使用配置.zip文件的FDM迁移用于非实时迁移，不需要立即使用目标FTD。



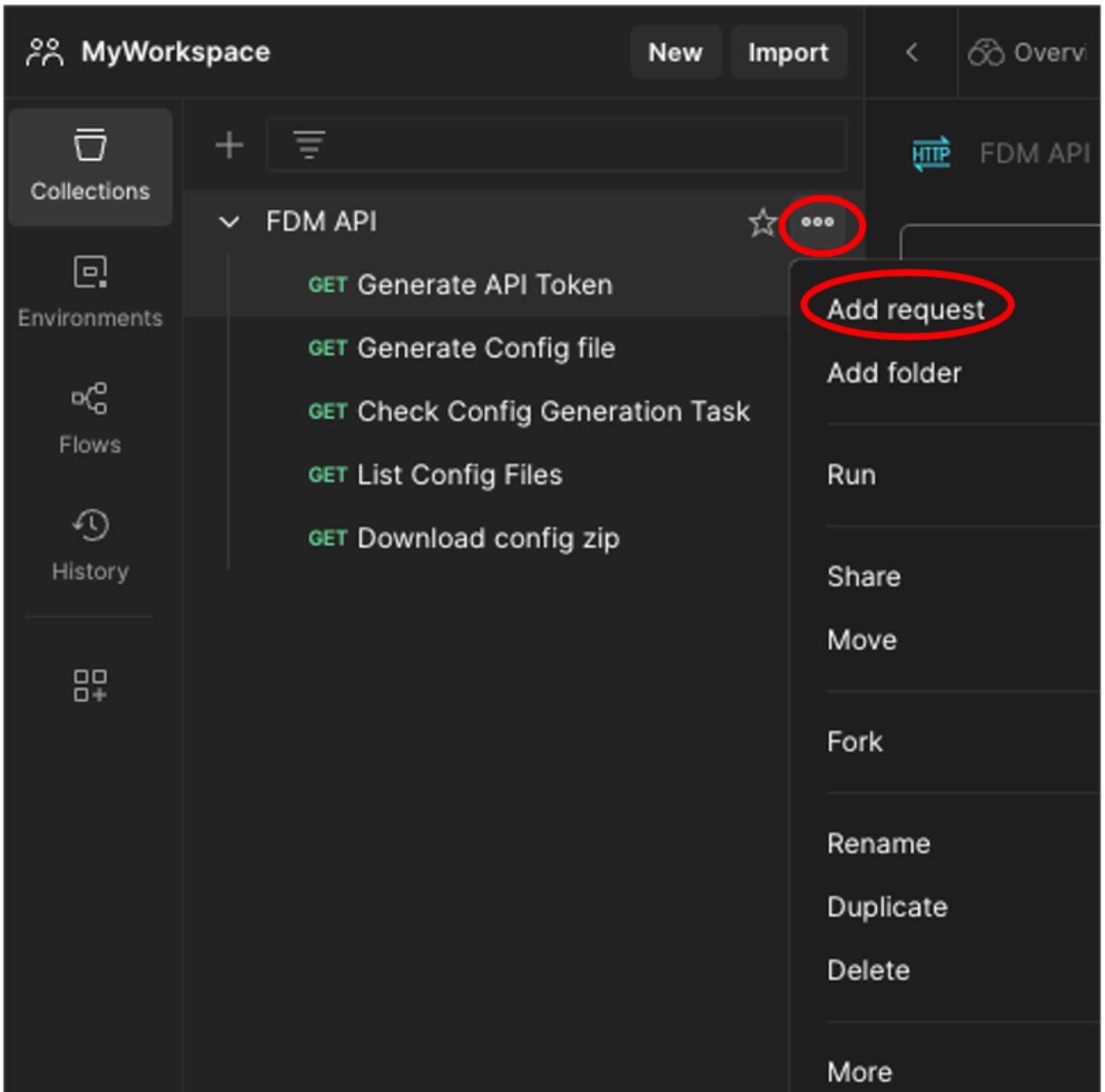
警告：选择此模式，仅允许迁移访问控制策略(ACP)、网络地址转换策略(NAT)和对象。对

于要迁移的ACP规则或NAT中必须使用的对象，否则将忽略这些对象。

## 配置

### API请求 — Postman

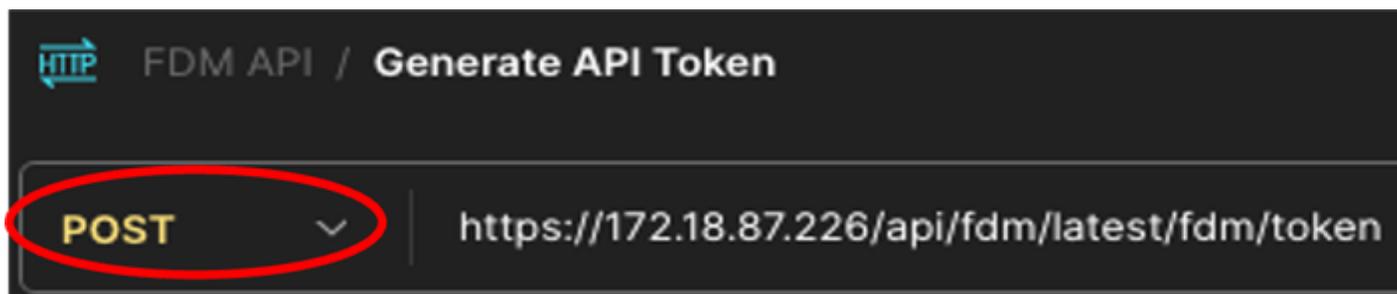
1. 在Postman中，创建新的集合（在此场景中使用FDM API）。
2. 单击3点，然后单击Add request。



Postman — 集合创建和请求添加

3. 调用此新请求：生成API令牌。它将被创建为GET请求，但在执行此请求时，必须从下拉菜单

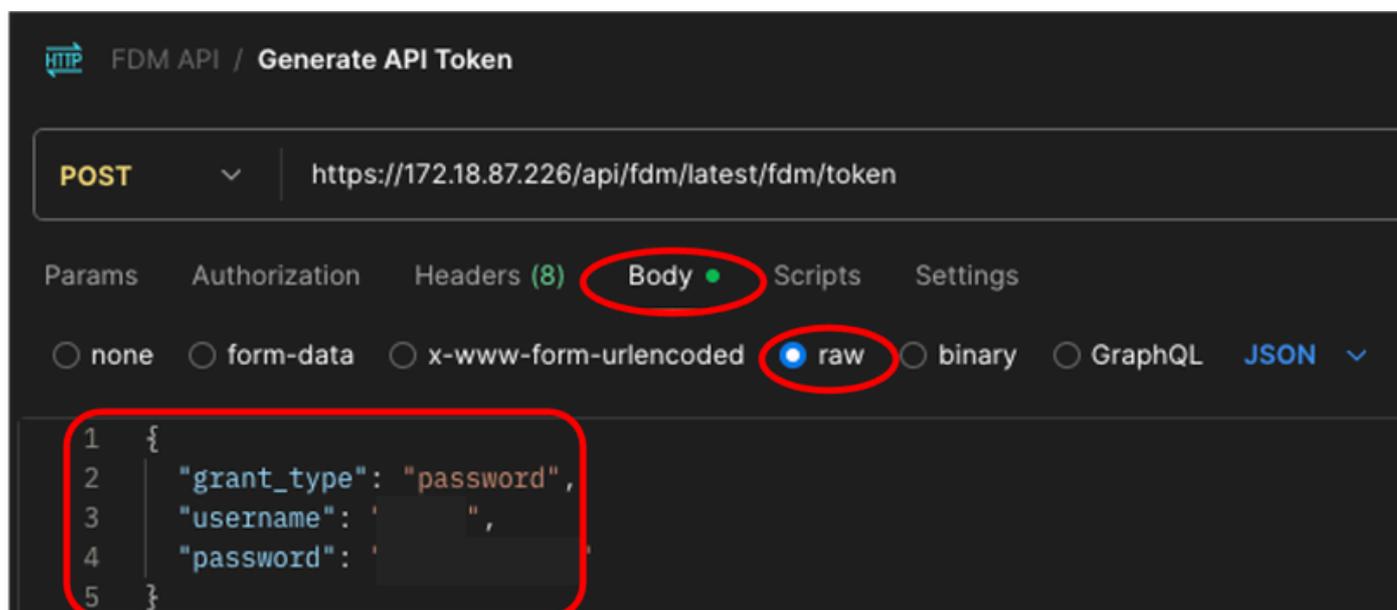
中选择POST。在POST旁边的文本框中，引入下一行https://<FDM IP  
ADD>/api/fdm/latest/fdm/token



Postman — 令牌请求

4.在正文选项卡中，选择原始选项，并引入使用此格式访问FTD(FDM)设备的身份证明。

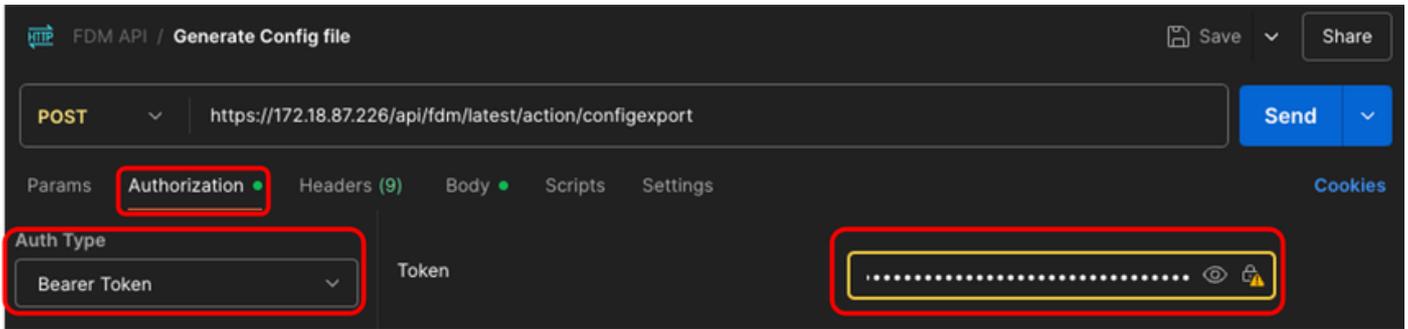
```
{  
  "grant_type": "password",  
  "username": "用户名",  
  "password": "密码"  
}
```



Postman — 令牌请求正文

5.最后，单击Send获取访问令牌。如果一切正常，您会收到200 OK响应。复制整个令牌（在双引号内），因为它将在后续步骤中使用。

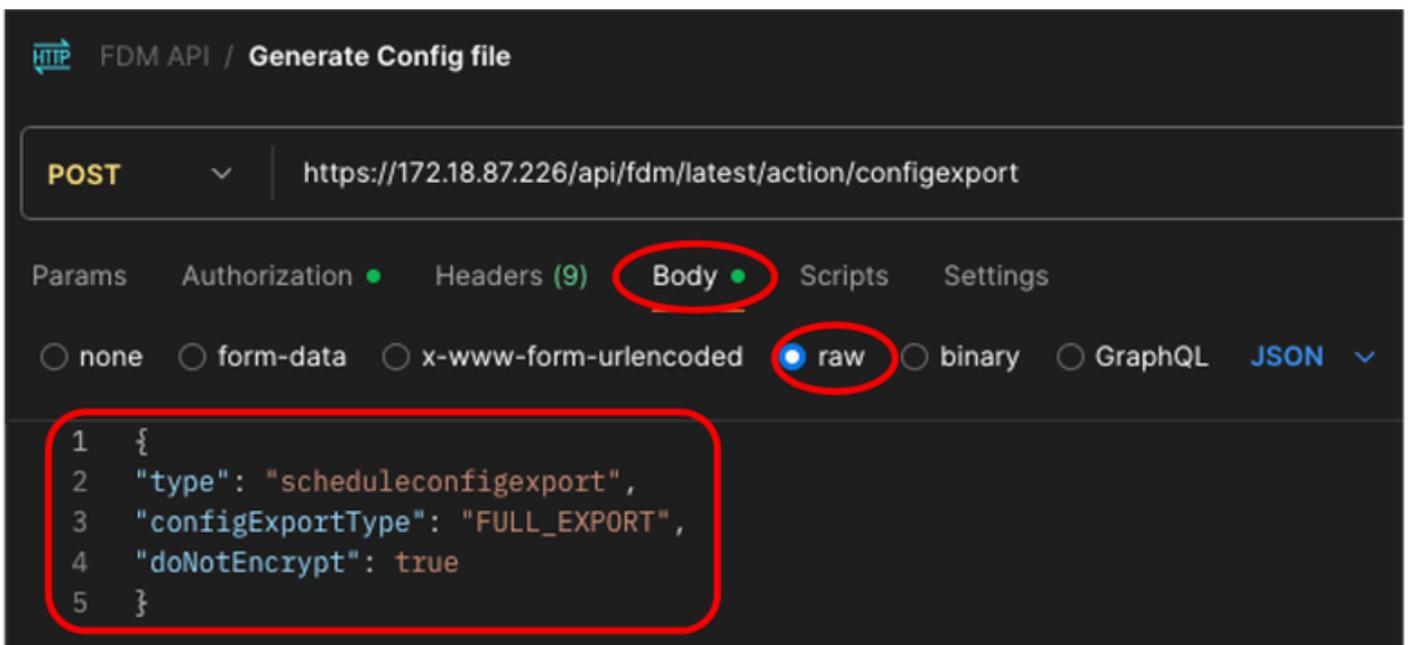




Postman — 生成配置文件请求 — 授权

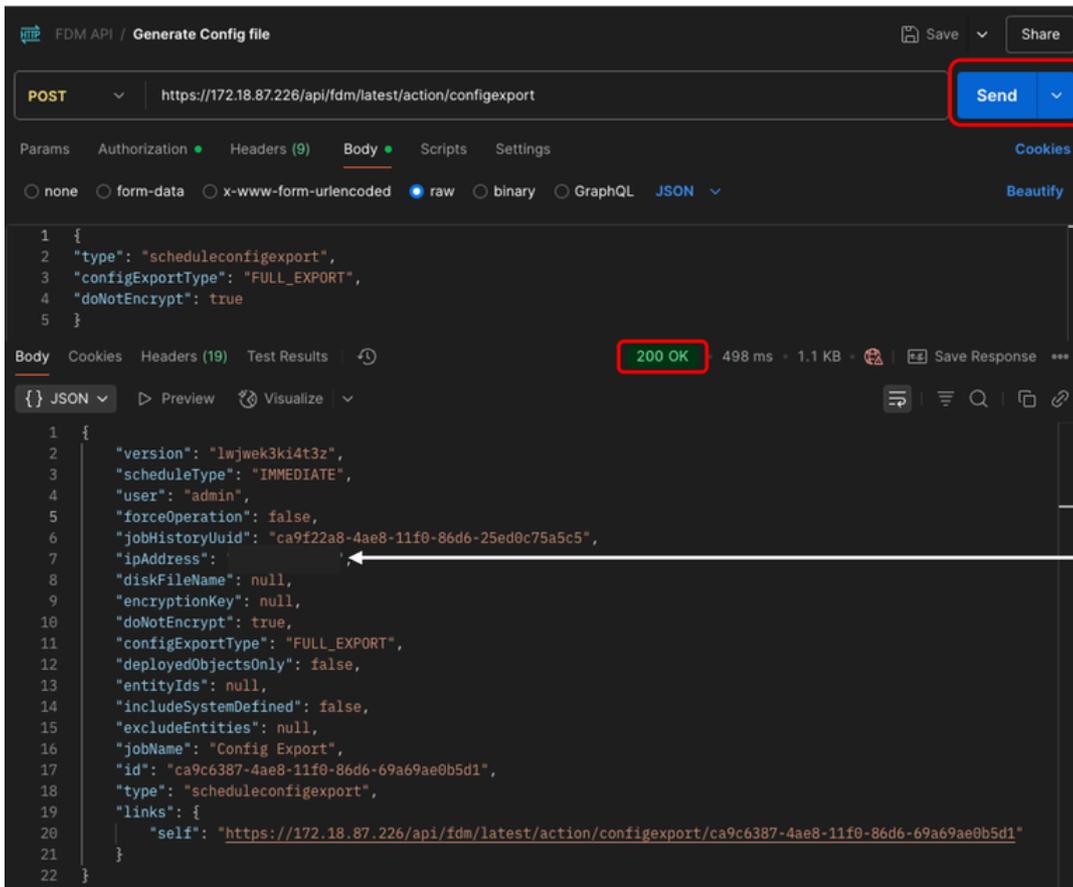
9.在正文选项卡中，选择原始选项并引入此信息。

```
{  
  "类型": "scheduleconfig导出",  
  "configExportType": "FULL_EXPORT",  
  "doNotEncrypt": true  
}
```



Postman — 生成配置文件请求 — 正文

10.最后，单击Send。如果一切正常，您会收到200 OK响应。

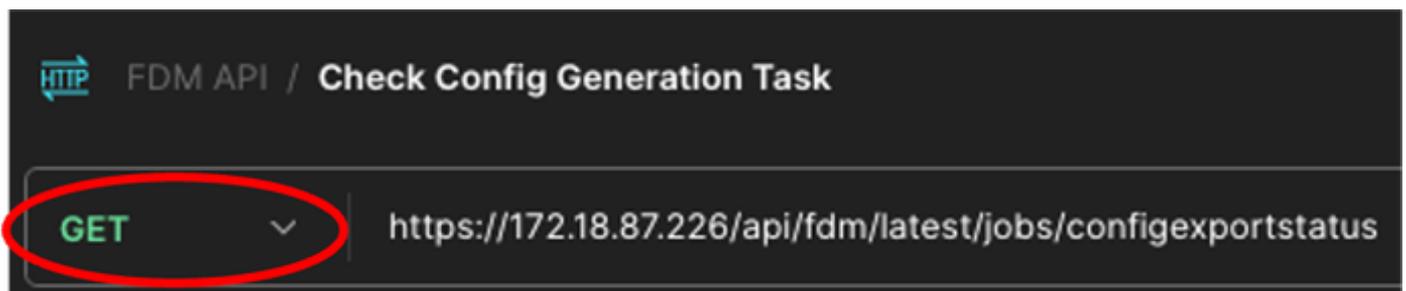


This IP address is the one that is connecting to the FTD through the requests.

Postman — 生成配置文件请求 — 输出

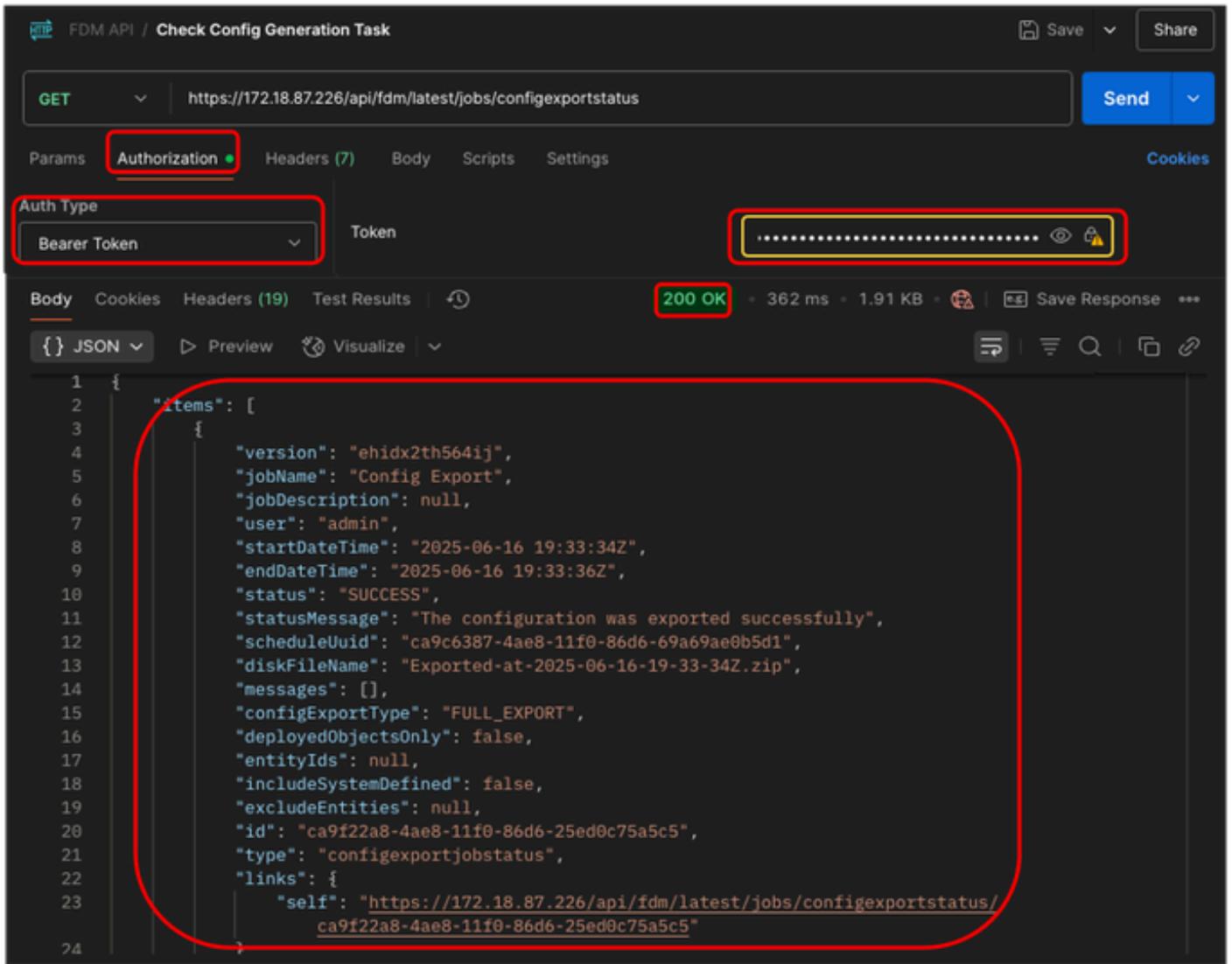
11. 重复步骤2，创建新的请求。这次将使用GET。

12. 将这个新请求称为：选中Config Generation Task。它将作为GET请求创建。此外，执行此命令时，必须从下拉菜单中选择GET。在GET旁边的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus



Postman — 检查配置导出状态请求

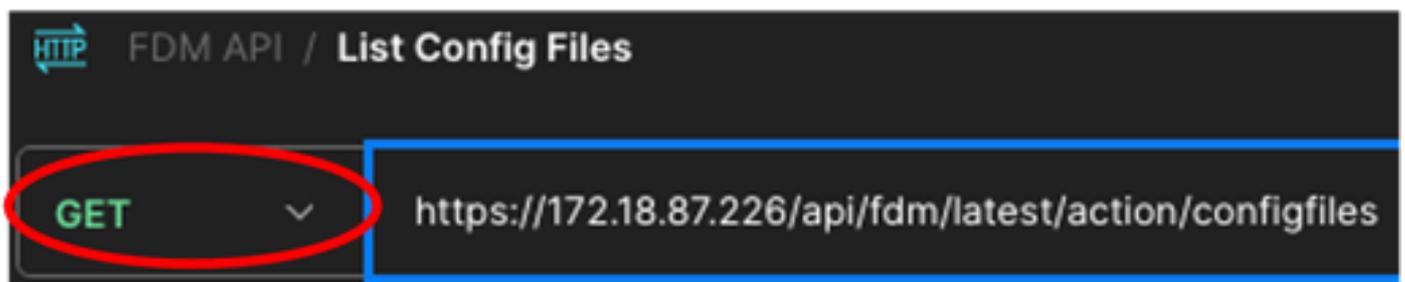
13. 在授权选项卡中，在下拉菜单中选择承载令牌作为身份验证类型，然后在“令牌”旁边的文本框中粘贴步骤5中复制的令牌。最后，单击发送。如果一切正常，您会收到200 OK响应，在JSON字段中可以看到任务状态和其他详细信息。



Postman — 配置导出状态请求 — 授权和输出

14. 重复第2步，要创建新的请求，这次将使用GET。

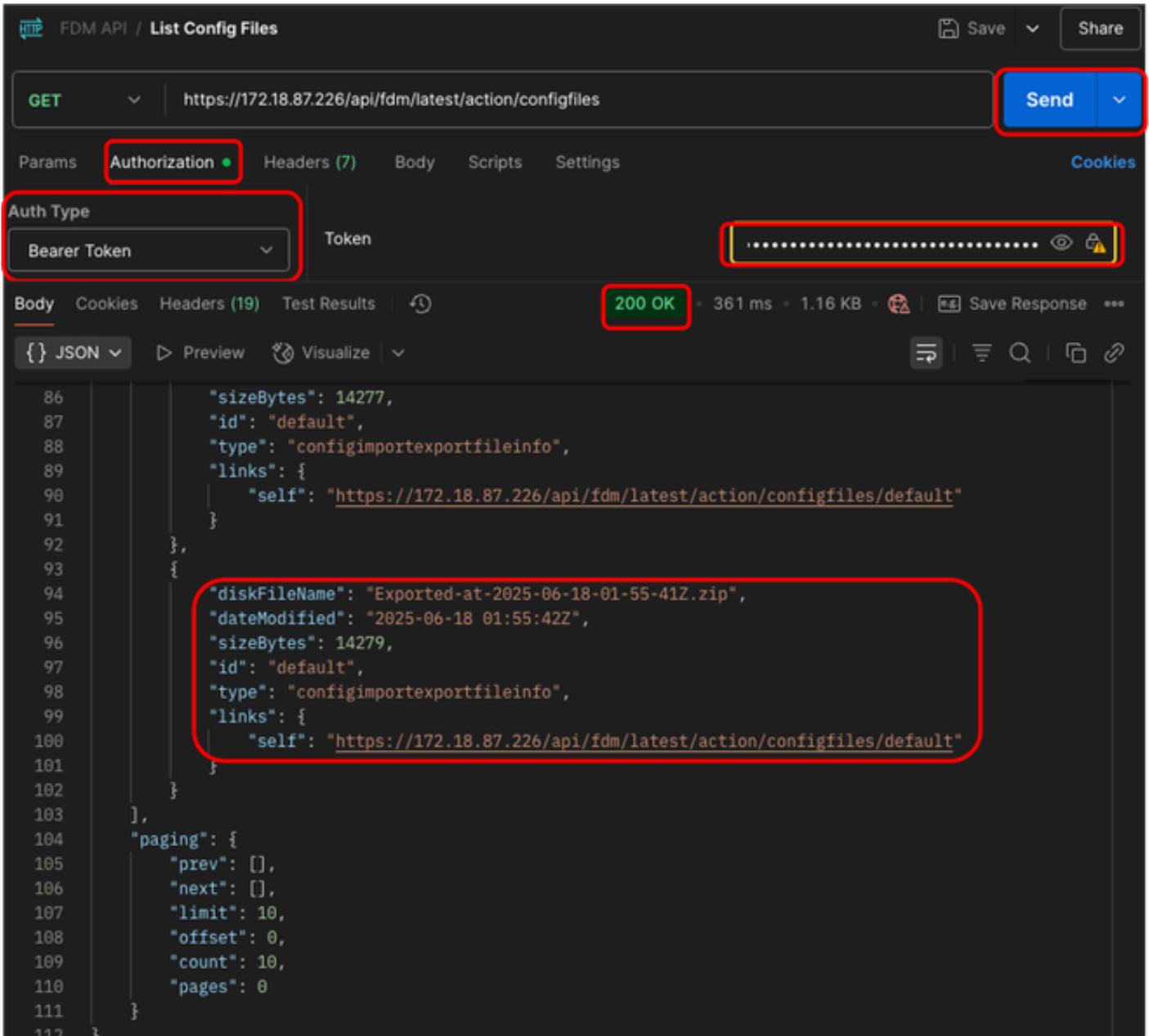
15. 将这个新请求称为：列出配置文件。它将被创建为GET请求，并且当您执行此请求时，必须从下拉菜单中选择GET。在GET旁边的文本框中，引入下一行https://<FDM IP ADD>/api/fdm/latest/action/configfiles



Postman — 列出导出的配置文件请求

16. 在授权选项卡中，从下拉菜单中选择承载令牌(Bearer Token)作为身份验证类型，然后在“令牌”(Token)旁边的文本框中粘贴步骤5中复制的令牌。最后，单击Send。如果一切正常，您将收到200 OK响应，并在JSON字段中显示导出文件的列表。最新的版本列在底部。复制最新文件名（文件名

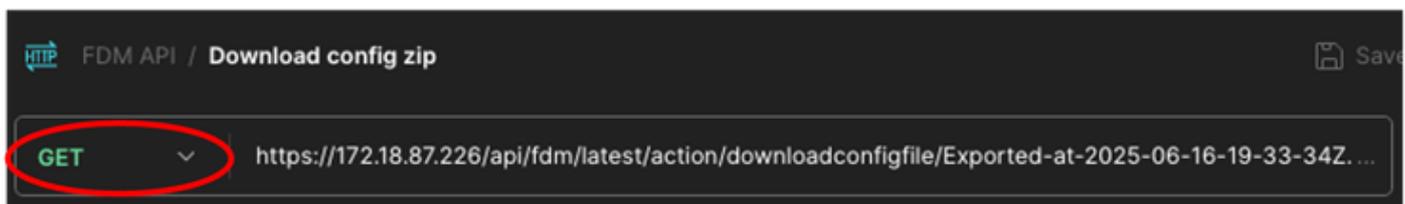
中的最近日期)，因为该文件将在最后一步中使用。



Postman — 列出导出的配置文件请求 — 授权和输出

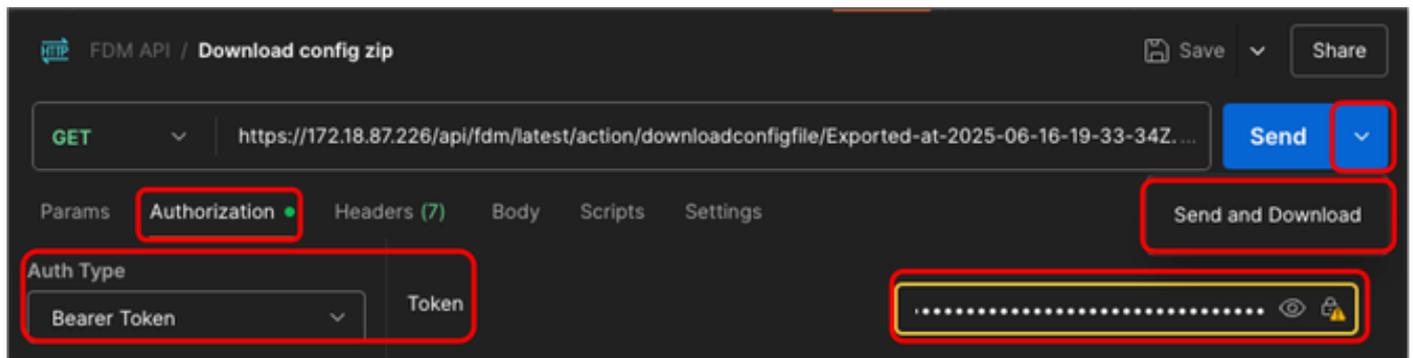
17.重复第2步，要创建新的请求，这次将使用GET。

18.将这个新请求称为：下载配置zip。它将被创建为GET请求，并且当您执行此请求时，必须从下拉菜单中选择GET。在GET旁边的文本框中，引入下一行，在末尾粘贴您在第16步中复制的文件名。 https://<FDM IP ADD>/api/fdm/latest/action/downloadconfigfile/<Exported\_File\_name.zip >



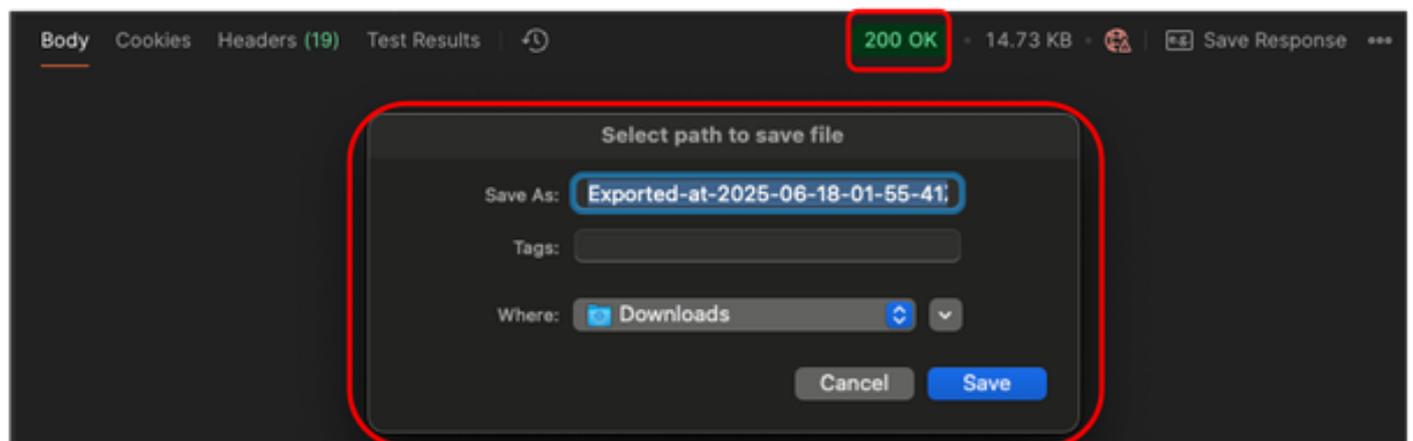
Postman — 下载Config.zip文件请求

19.在“授权”选项卡中，从下拉菜单中选择承载令牌(Bearer Token)作为“身份验证类型”，然后在“令牌”(Token)旁边的文本框中粘贴步骤5中复制的令牌。最后，单击“发送”(Send)旁边的向下箭头，然后选择Send and Download。



Postman — 下载Config.zip文件请求 — 授权

20.如果一切正常，您会收到200 OK响应，并显示一个弹出窗口，询问要将configuration.zip文件保存到的目标文件夹。现在可以将此.zip文件上传到防火墙迁移工具。



Postman — 下载Config.zip文件请求 — 保存

## 防火墙迁移工具

21.打开“防火墙迁移工具”，在“选择源配置”下拉菜单中，选择Cisco Secure Firewall Device Manager(7.2+)，然后单击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.
  - 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选择

22.选中第一个单选按钮Migrate Firewall Device Manager(Shared Configurations Only) , 然后单击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) ➤

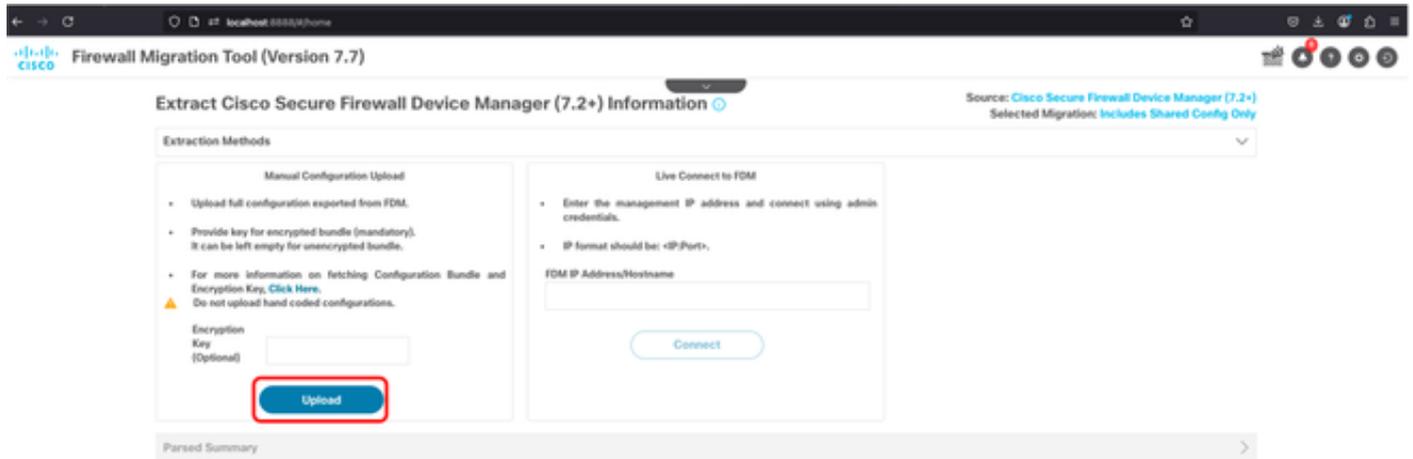
### Note :

- 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

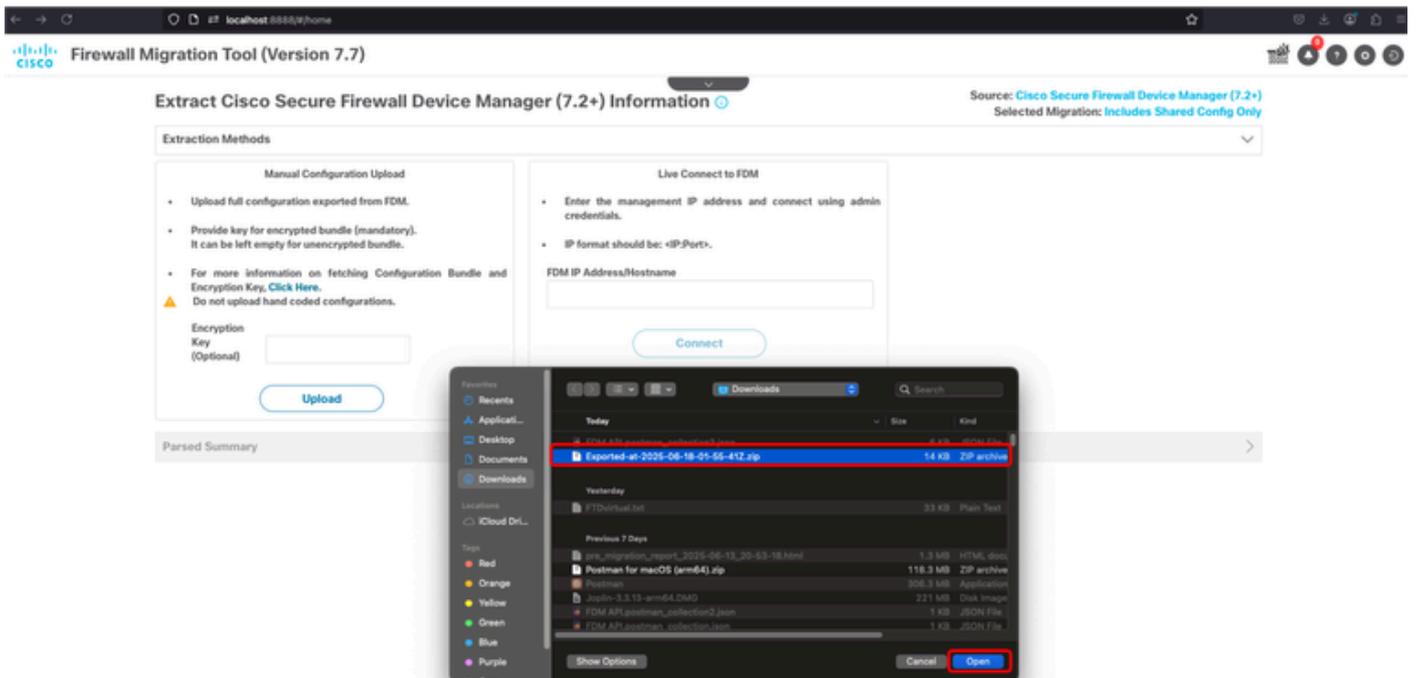
FMT — 仅限FDM迁移共享配置

23. 在左侧面板(手动配置上传)中，单击上传。



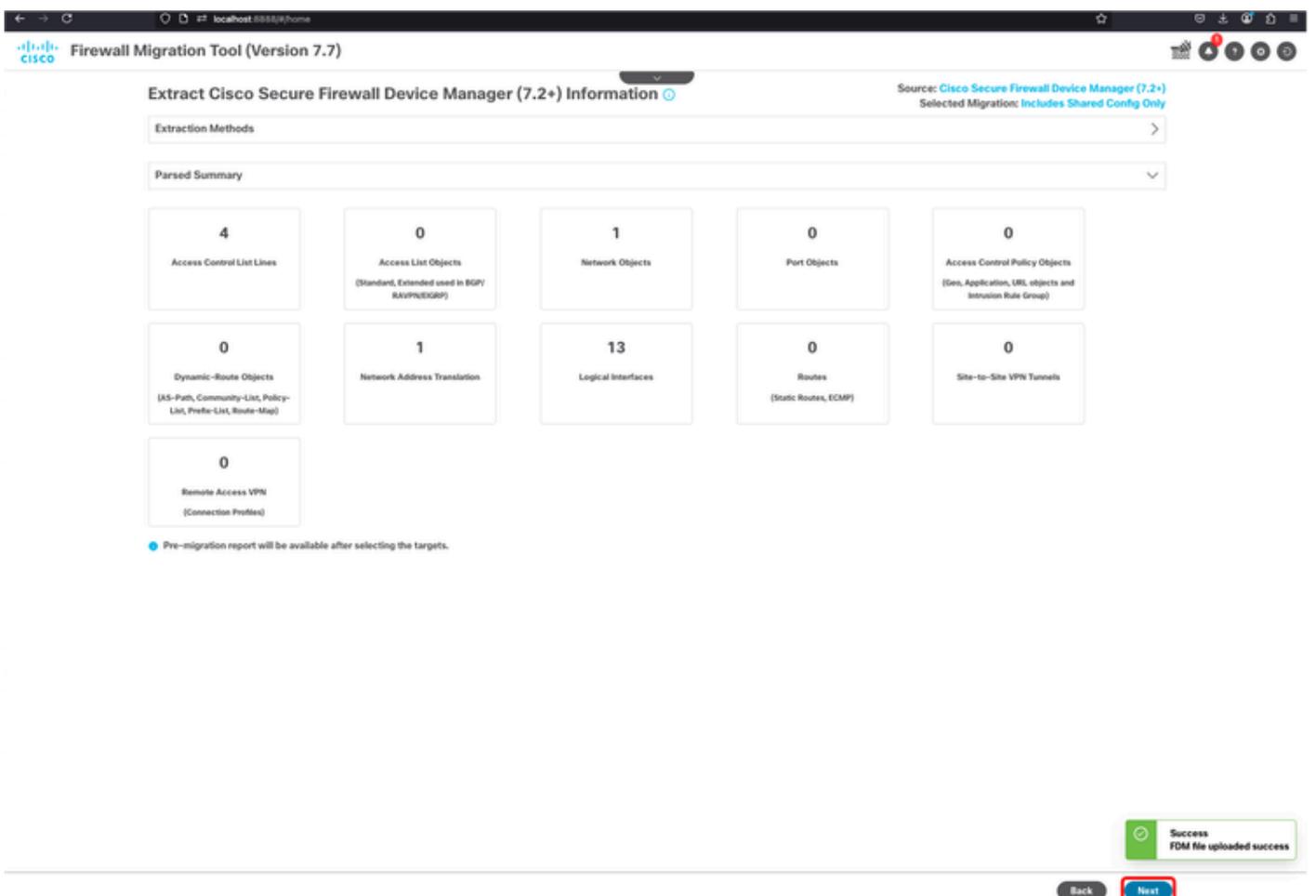
FMT — 上传Config.zip文件

24. 在先前保存的文件夹中选择导出的zip配置文件，然后单击打开。



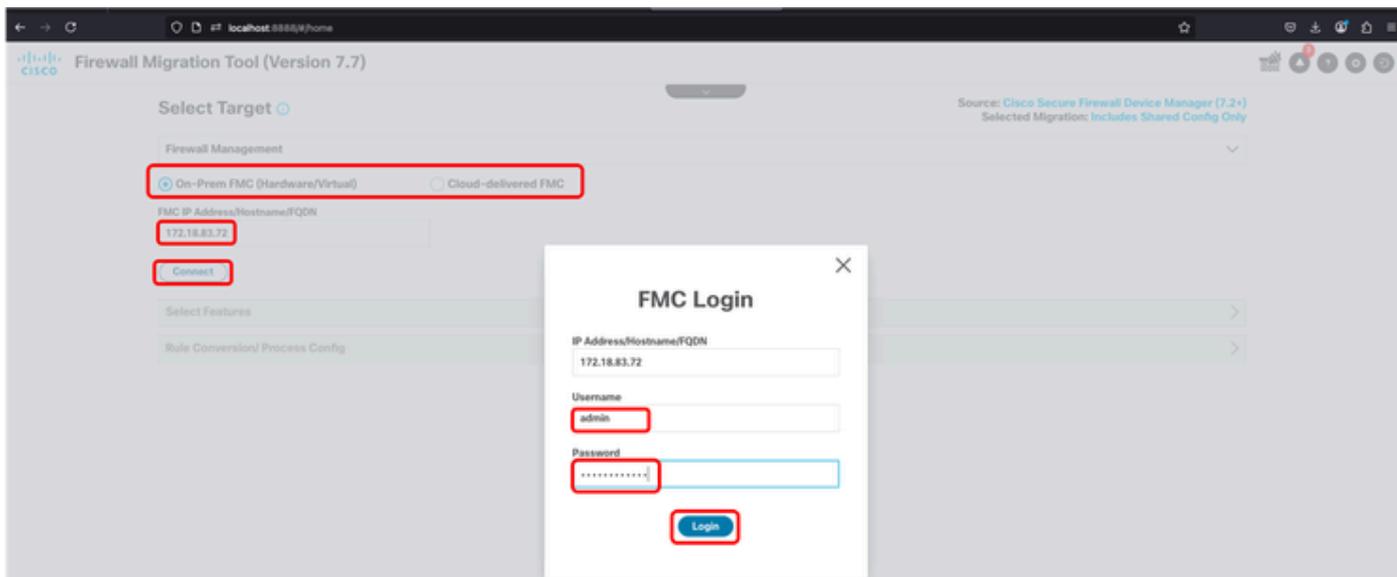
FMT - Config.zip文件选择

25.如果一切如期进行，则显示分析摘要。此外，在右下角可以看到一个弹出窗口，通知FDM文件已成功上传。单击 Next。



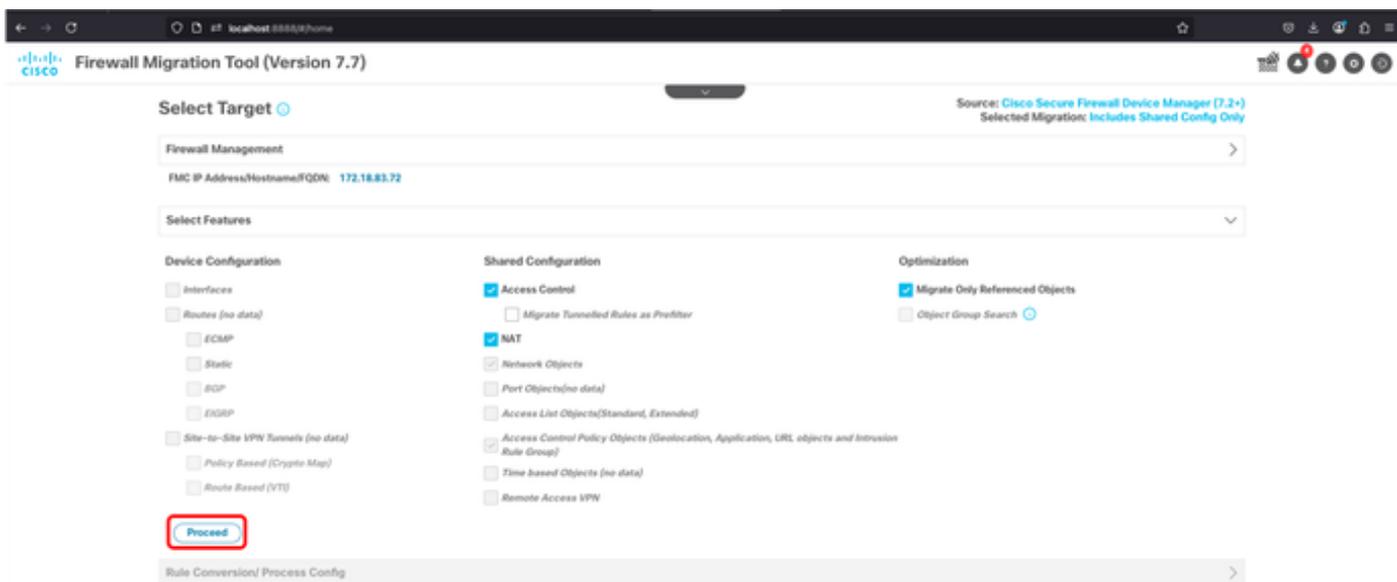
FMT — 分析摘要

26.选择更适合您环境的选项（内部FMC或Cd-FMC）。在此场景中，使用内部FMC。键入FMC IP地址，然后单击Connect。系统将显示新的弹出窗口，要求FMC凭证，在输入此信息后，单击Login。



FMT - FMC目标登录

27.下一个屏幕显示目标FMC和要迁移的功能。单击Proceed。

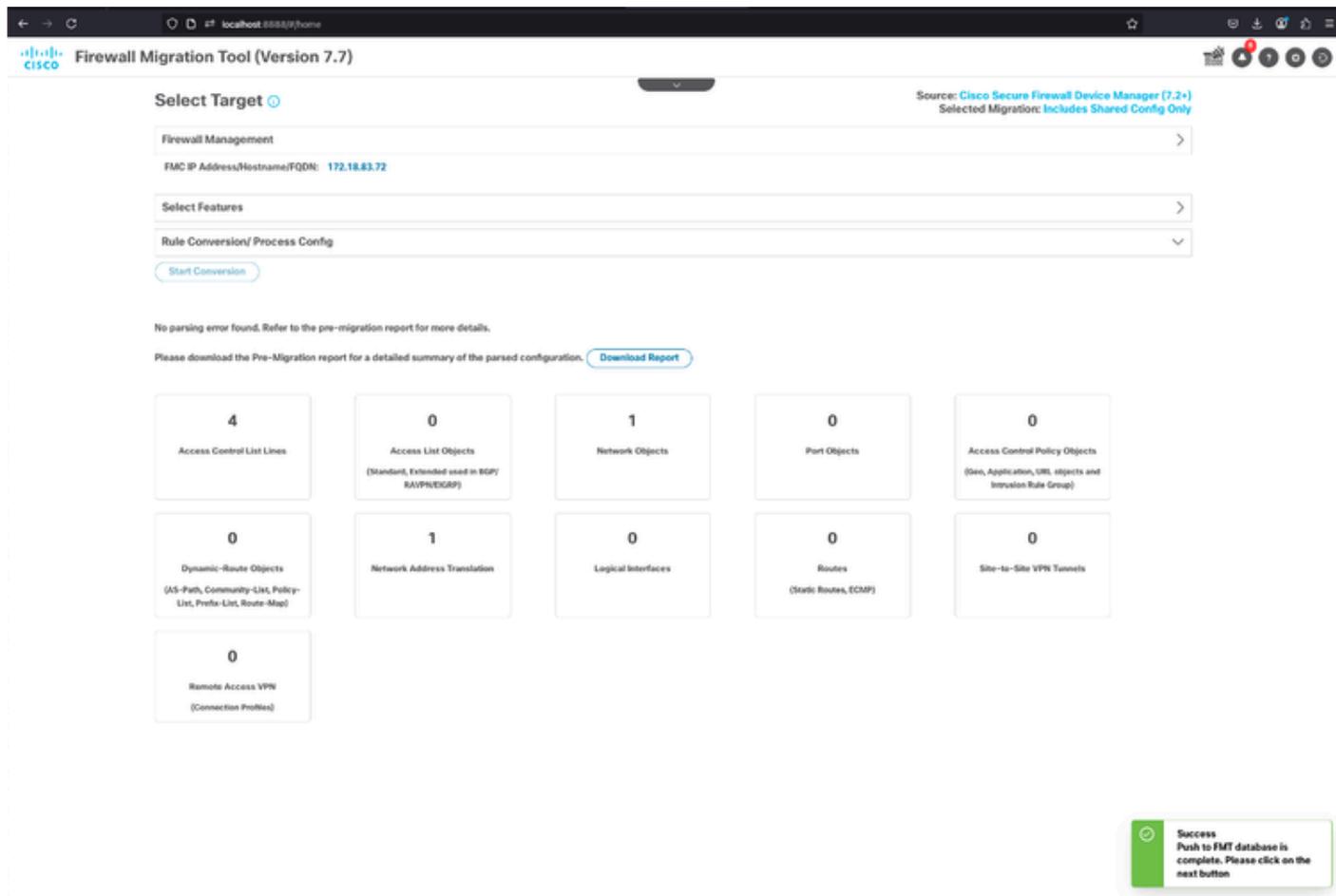


FMT - FMC目标 — 功能选择

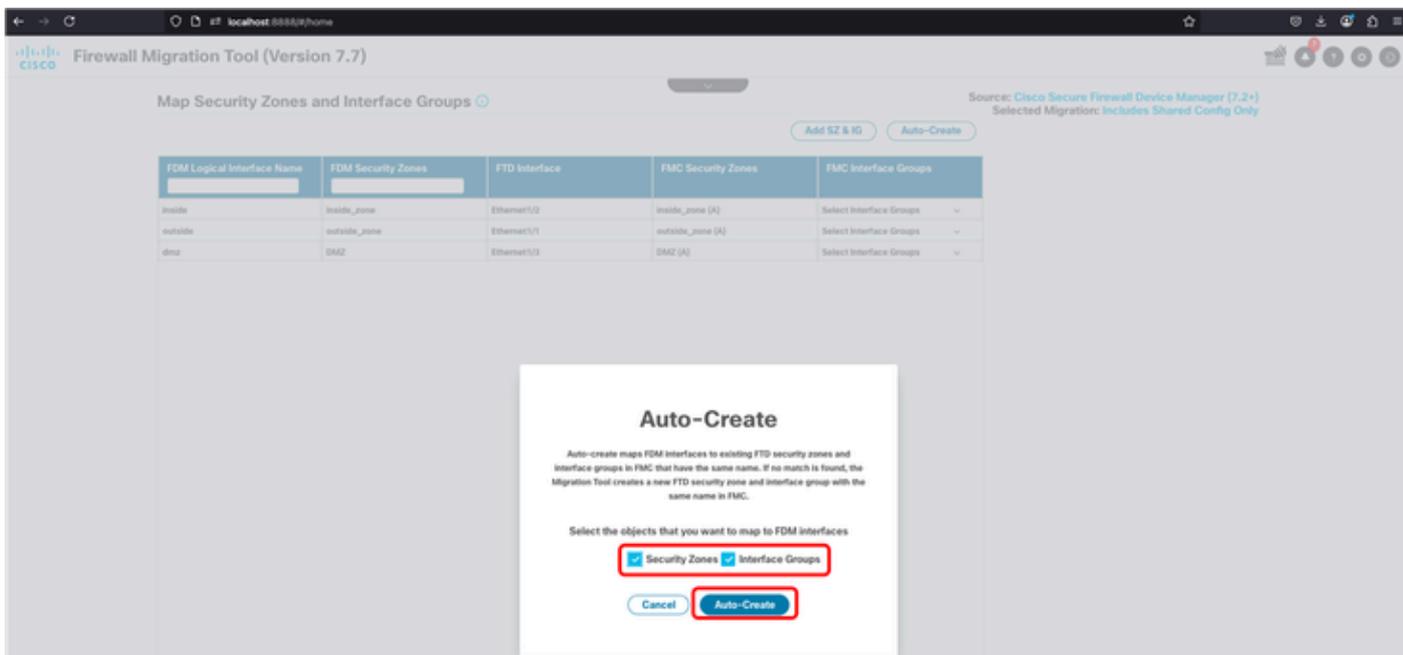
28.确认FMC目标后，单击Start Conversion按钮。



29.如果一切按预期进行，右下角将显示一个弹出窗口，通知向FMT数据库的推送已完成。单击Next。

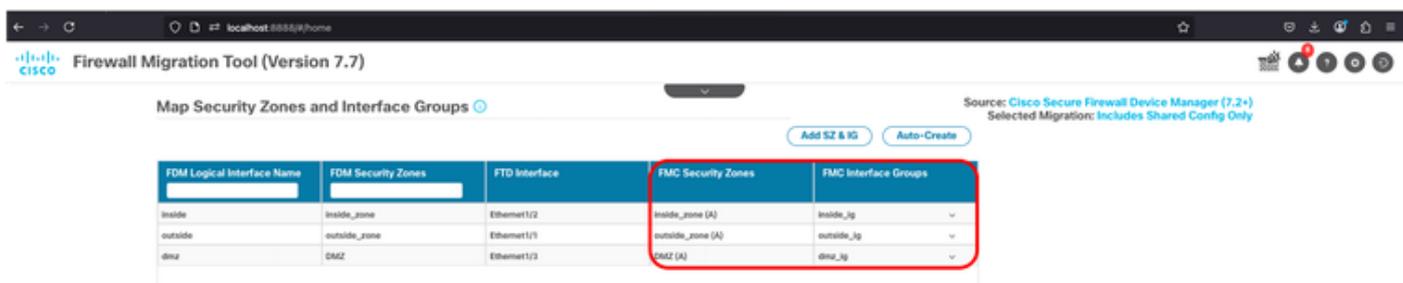


30.在下一个屏幕中，您必须手动创建，或选择自动创建安全区域和接口组。在此场景中，使用自动创建。



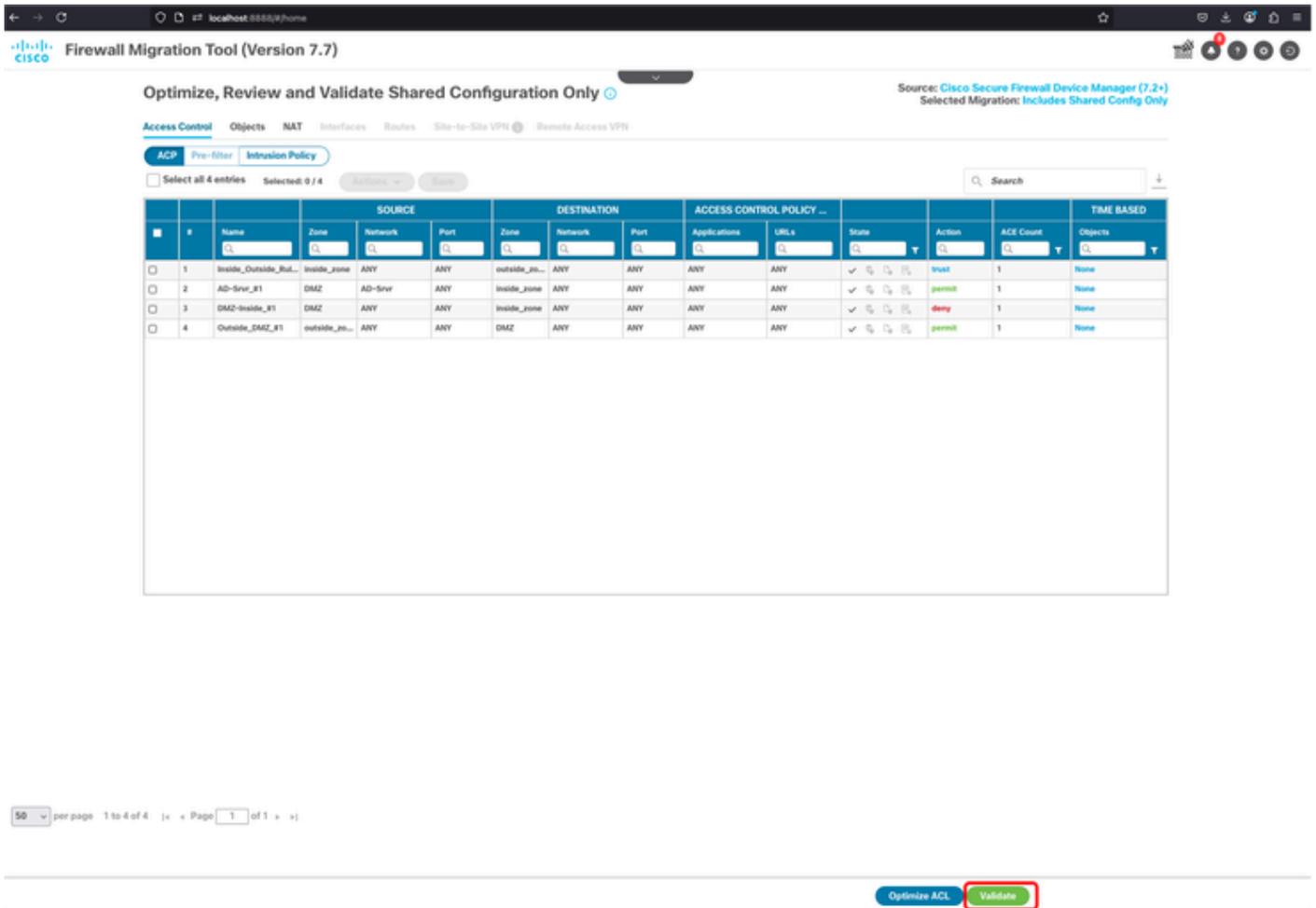
FMT — 自动创建安全区域和接口组

31.表格一经填写，分别在第4栏和第5栏，即安全区和接口组显示。



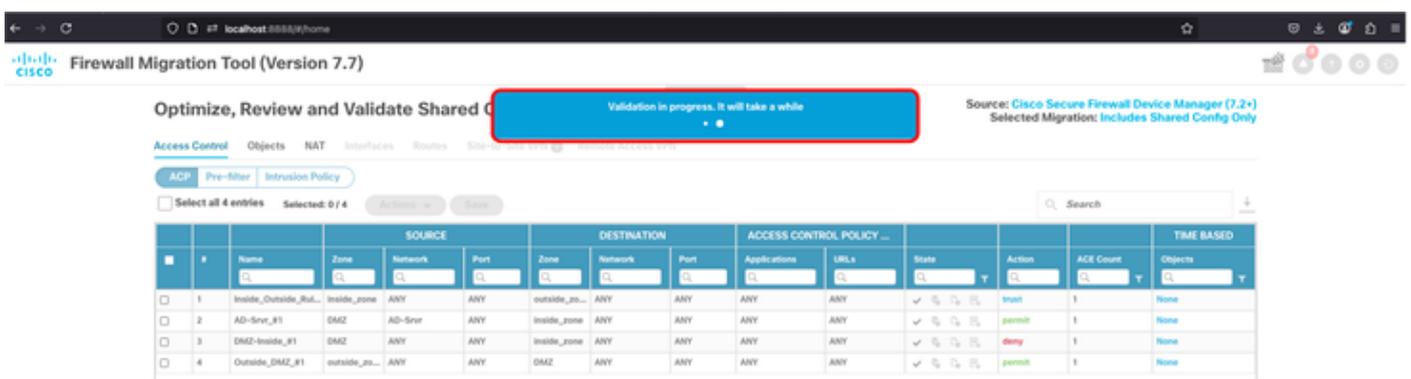
FMT — 安全区域和接口组已成功创建

32.在下一个屏幕中，您可以优化ACL或仅验证ACP、对象和NAT。完成后，单击Validate按钮。



FMT — 优化ACL — 验证迁移

33.验证需要几分钟才能完成。



FMT — 正在进行验证

34.完成后，FMT让您知道配置已成功验证，下一步是单击Push Configuration按钮。

# Validation Status



 Successfully Validated

## Validation Summary (Pre-push)

<b>4</b> Access Control List Lines	Not selected for migration Access List Objects (Standard, Extended used in BGP/RAVPN/EIGRP)	<b>1</b> Network Objects	Not selected for migration Port Objects	<b>0</b> 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)	<b>1</b> 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 — 验证成功 — 将配置推送到FMC

35.最后，单击Proceed按钮。



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.

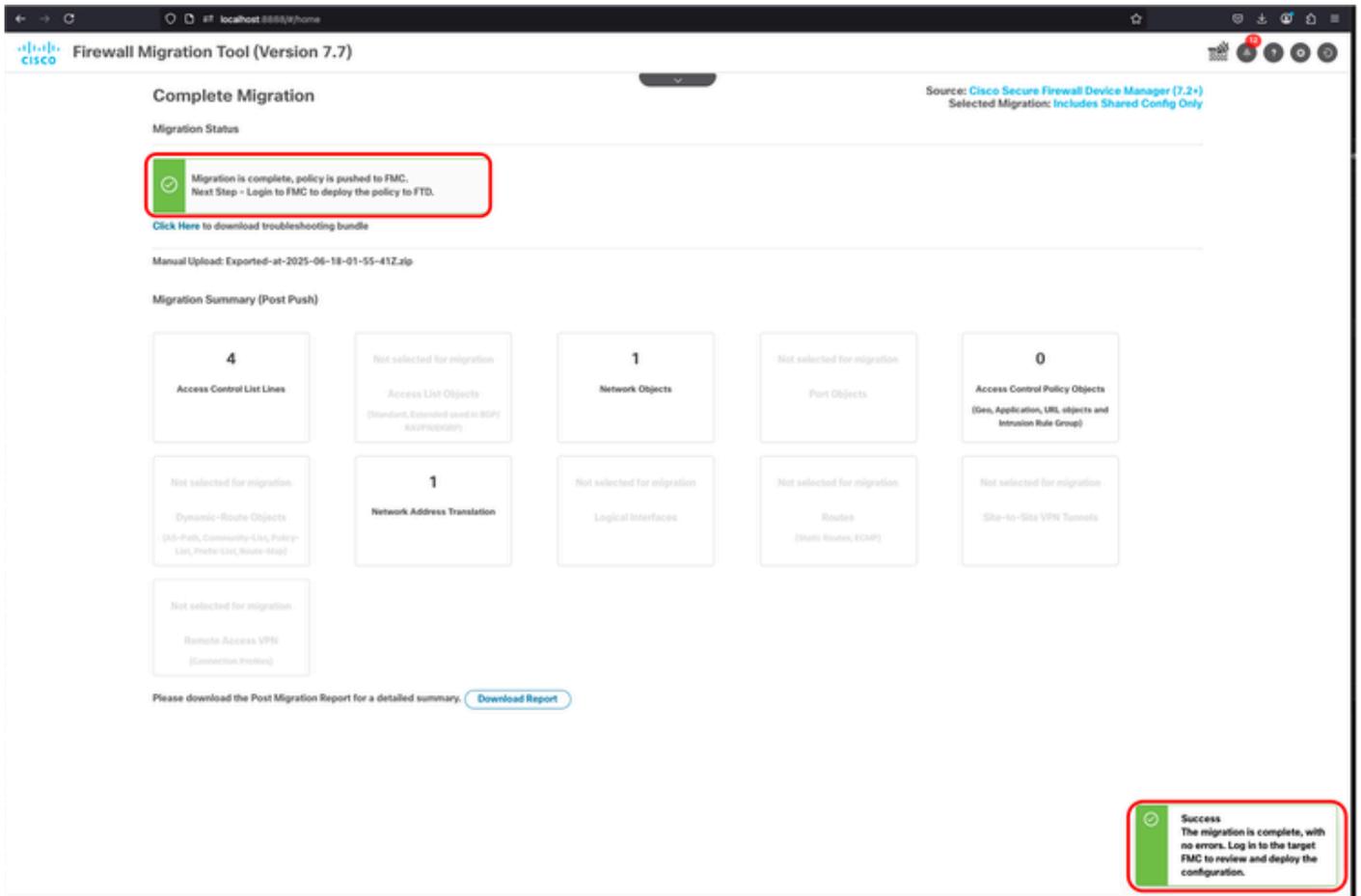
Click on Proceed to continue.

**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 — 继续配置推送

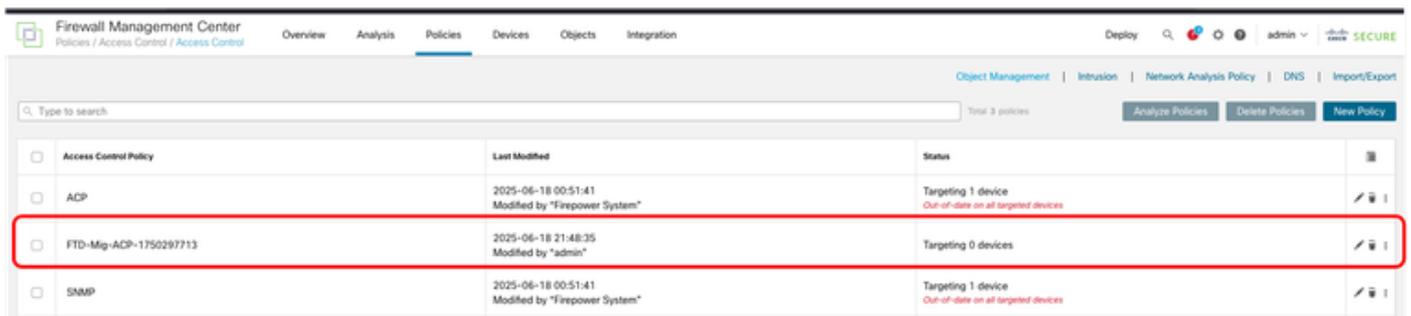
36.如果一切如期进行，将显示迁移成功通知。FMT要求您登录FMC并将迁移的策略部署到FTD。



FMT — 迁移成功通知

## FMC验证

37. 登录FMC后，ACP和NAT策略显示为FTD-Mig。现在，您可以继续部署到新的FTD。



FMC - ACP已迁移



FMC - NAT策略已迁移

## 相关信息

- [FMT - FDM迁移指南 — FMC](#)
- [FMT版本说明](#)

## 关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。