

Migration de FDM vers FMC via FMT à l'aide du fichier Configuration.zip

Table des matières

[Introduction](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Informations générales](#)

[Considérations](#)

[Configuration](#)

[Demandes API - Postman](#)

[Outil de migration de pare-feu](#)

[Vérification FMC](#)

[Informations connexes](#)

Introduction

Ce document décrit comment générer le fichier de configuration.zip d'un Gestionnaire de périphériques de pare-feu sécurisé (FDM) à migrer vers un FMC à l'aide de FMT.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco Firewall Threat Defense (FTD)
- Cisco Firewall Management Center (FMC)
- Outil de migration de pare-feu (FMT)
- Plate-forme API Postman

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel ci-après.

DFT 7.4.2

FMC 7.4.2

FMT 7.7.0.1

Facteur 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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

- FDM peut désormais être migré vers FMC de différentes manières. Dans ce document, le scénario qui va être exploré est la génération du fichier .zip de configuration à l'aide de requêtes API et le téléchargement ultérieur de ce fichier vers FMT pour migrer la configuration vers FMC.
- Les étapes présentées dans ce document commencent à utiliser Postman directement, il est donc recommandé que Postman soit déjà installé. Le PC ou l'ordinateur portable que vous allez utiliser doit avoir accès à FDM et FMC, et FMT doit également être installé et en cours d'exécution.

Considérations

- Ce document se concentre sur la génération du fichier .zip de configuration plus que dans l'utilisation de FMT.
- La migration FDM à l'aide du fichier .zip de configuration est destinée aux migrations non actives et ne nécessite pas immédiatement un FTD de destination.

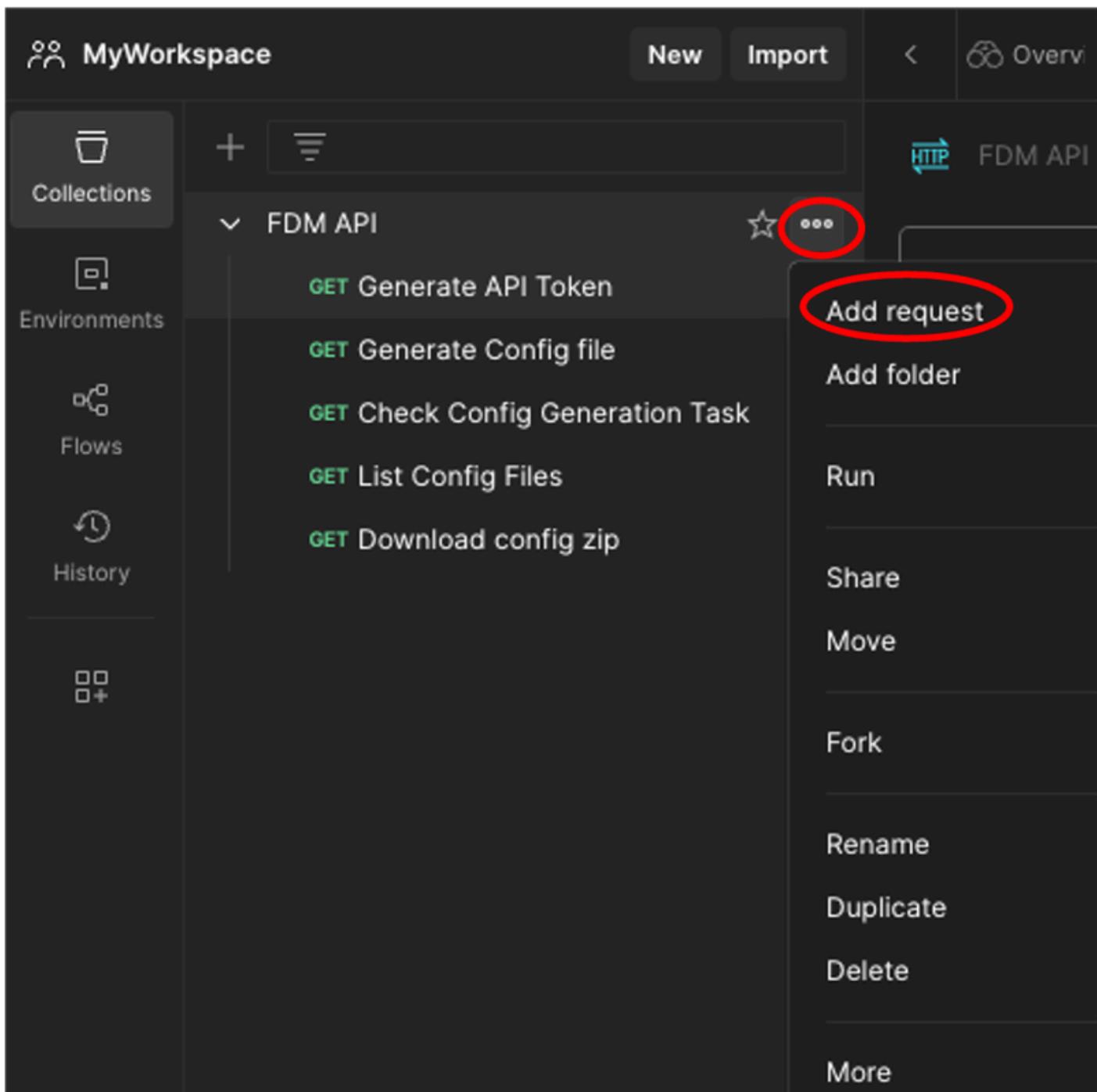


Avertissement : Le choix de ce mode permet de migrer uniquement la politique de contrôle d'accès (ACP), la politique de traduction d'adresses de réseau (NAT) et les objets. En ce qui concerne les objets, ceux-ci doivent être utilisés dans une règle ACP ou NAT, pour être migrés, sinon ils sont ignorés.

Configuration

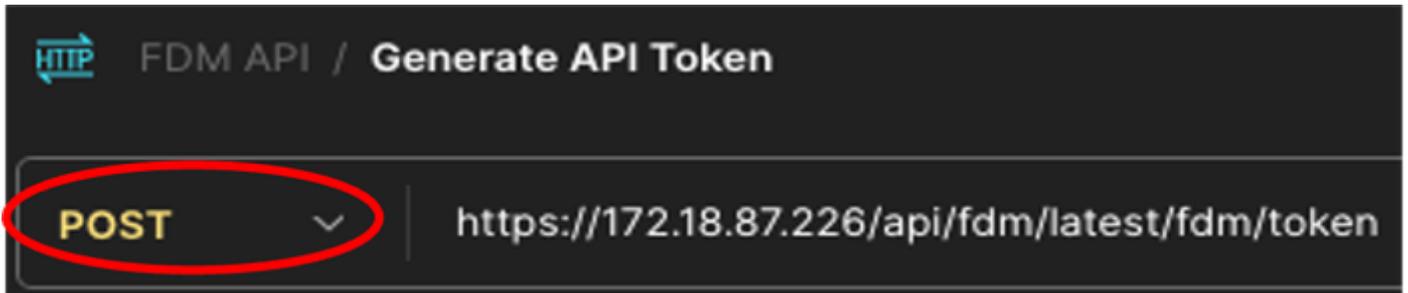
Demandes API - Postman

1. Dans Postman, créez une nouvelle collection (dans ce scénario, l'API FDM est utilisée).
2. Cliquez sur les 3 points, puis sur Ajouter la demande.



Postman - Création de collection et ajout de demande

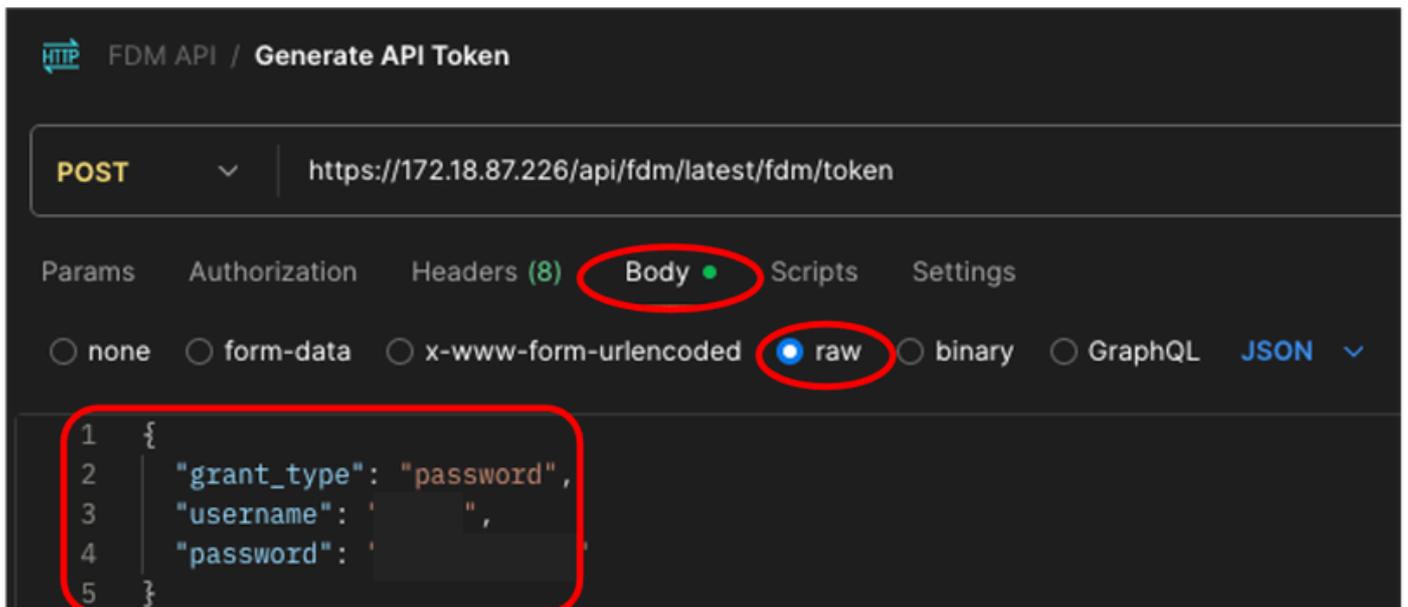
3. Appelez cette nouvelle demande : Générez un jeton API. Il va être créé en tant que requête GET, mais au moment où vous exécutez celle-ci, POST doit être sélectionné dans le menu déroulant. Dans la zone de texte à côté de POST, introduisez la ligne suivante `https://<FDM IP ADD>/api/fdm/last/fdm/token`



Facteur - Demande de jeton

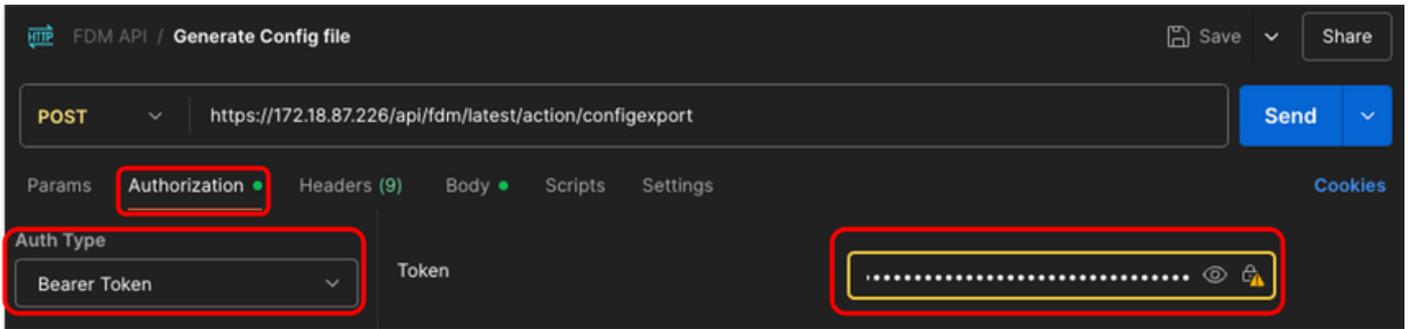
4. Dans l'onglet Body, sélectionnez l'option raw et présentez les informations d'identification pour accéder au périphérique FTD (FDM) à l'aide de ce format.

```
{  
  "grant_type": "mot de passe",  
  "nom d'utilisateur": »nom d'utilisateur",  
  "mot de passe": »mot de passe"  
}
```



Postman - Corps de la demande de jeton

5. Enfin, cliquez sur Send pour obtenir votre jeton d'accès. Si tout va bien, vous recevez une réponse 200 OK. Faites une copie de l'ensemble du jeton (entre guillemets doubles), car il sera utilisé dans les étapes ultérieures.



Postman - Demande de génération de fichier de configuration - Autorisation

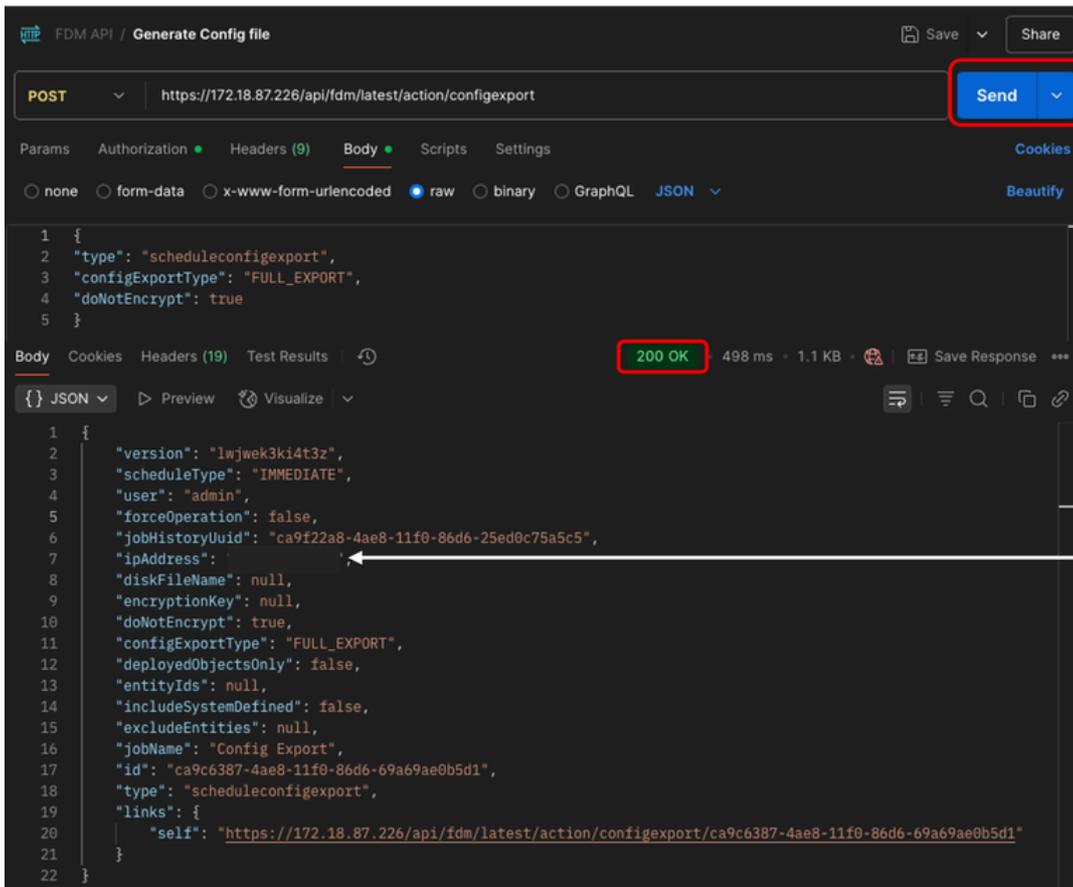
9. Dans l'onglet Corps, sélectionnez l'option brute et présentez ces informations.

```
{  
  "type": "schedule onfigexport",  
  "configExportType": "EXPORT_COMPLET",  
  "doNotEncrypt": vrai  
}
```



Postman - Générer une demande de fichier de configuration - Corps

10. Enfin, cliquez sur Envoyer. Si tout va bien, vous recevez une réponse 200 OK.

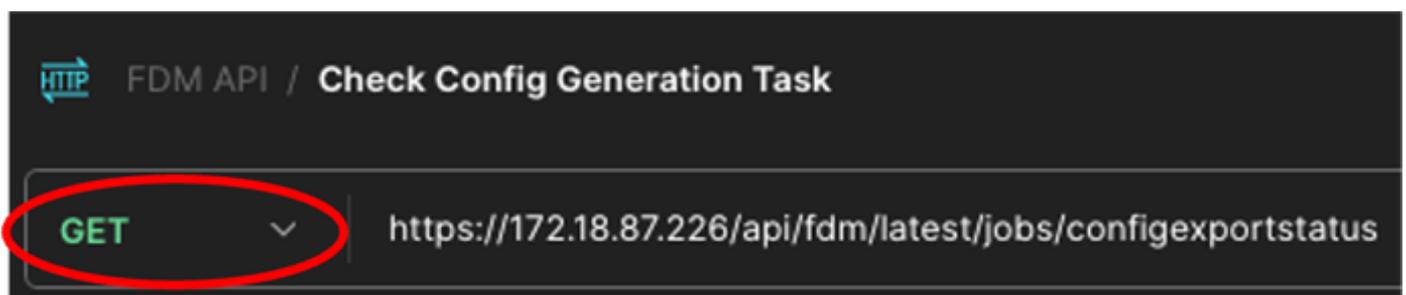


This IP address is the one that is connecting to the FTD through the requests.

Postman - Demande de génération de fichier de configuration - Sortie

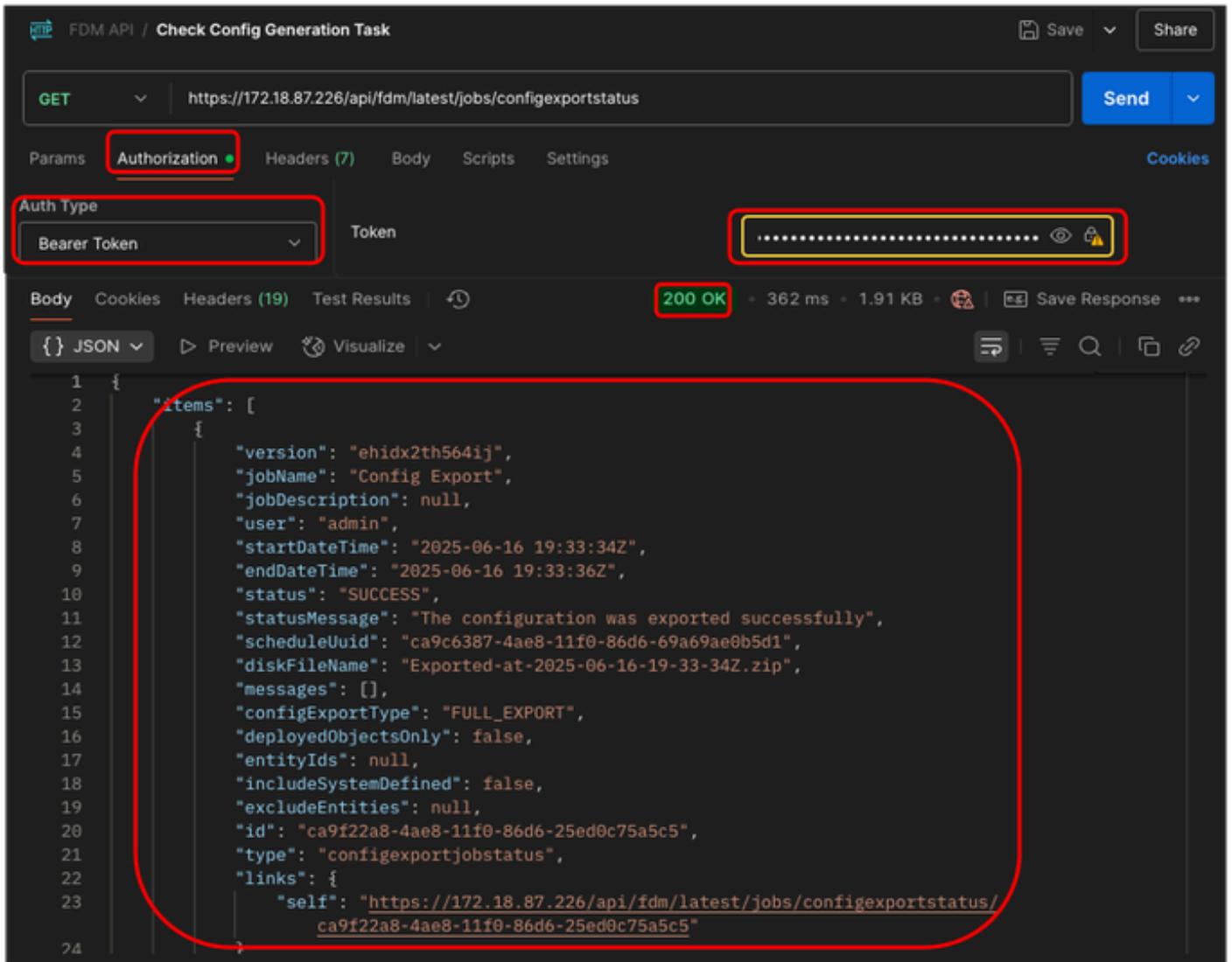
11. Répétez l'étape 2 pour créer une nouvelle demande. GET va être utilisé cette fois.

12. Appelez cette nouvelle demande : Cochez Tâche de génération de configuration. Il va être créé en tant que demande GET. En outre, l'heure à laquelle vous exécutez celui-ci, GET doit être sélectionné dans le menu déroulant. Dans la zone de texte à côté de GET, introduisez la ligne suivante `https://<FDM IP ADD>/api/fdm/latest/jobs/configexportstatus`



Postman - Vérifier la demande d'état d'exportation de configuration

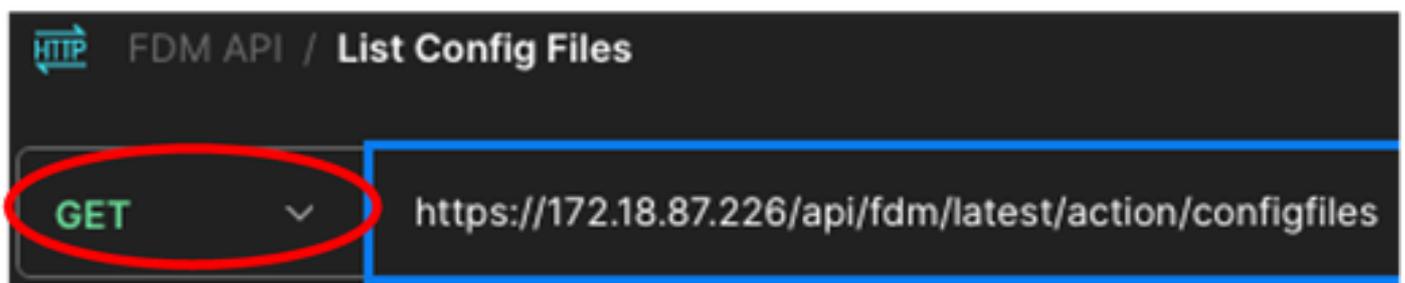
13. Dans l'onglet Autorisation, sélectionnez Bearer Token as Auth Type dans le menu déroulant, et dans la zone de texte à côté de Token, collez le jeton copié à l'étape 5. Enfin, cliquez sur Send. Si tout va bien, vous recevez une réponse 200 OK et dans le champ JSON, l'état de la tâche et d'autres détails peuvent être vus.



Postman - Demande d'état d'exportation de configuration - Autorisation et sortie

14. Répétez l'étape 2. Pour créer une nouvelle demande, GET sera utilisé cette fois-ci.

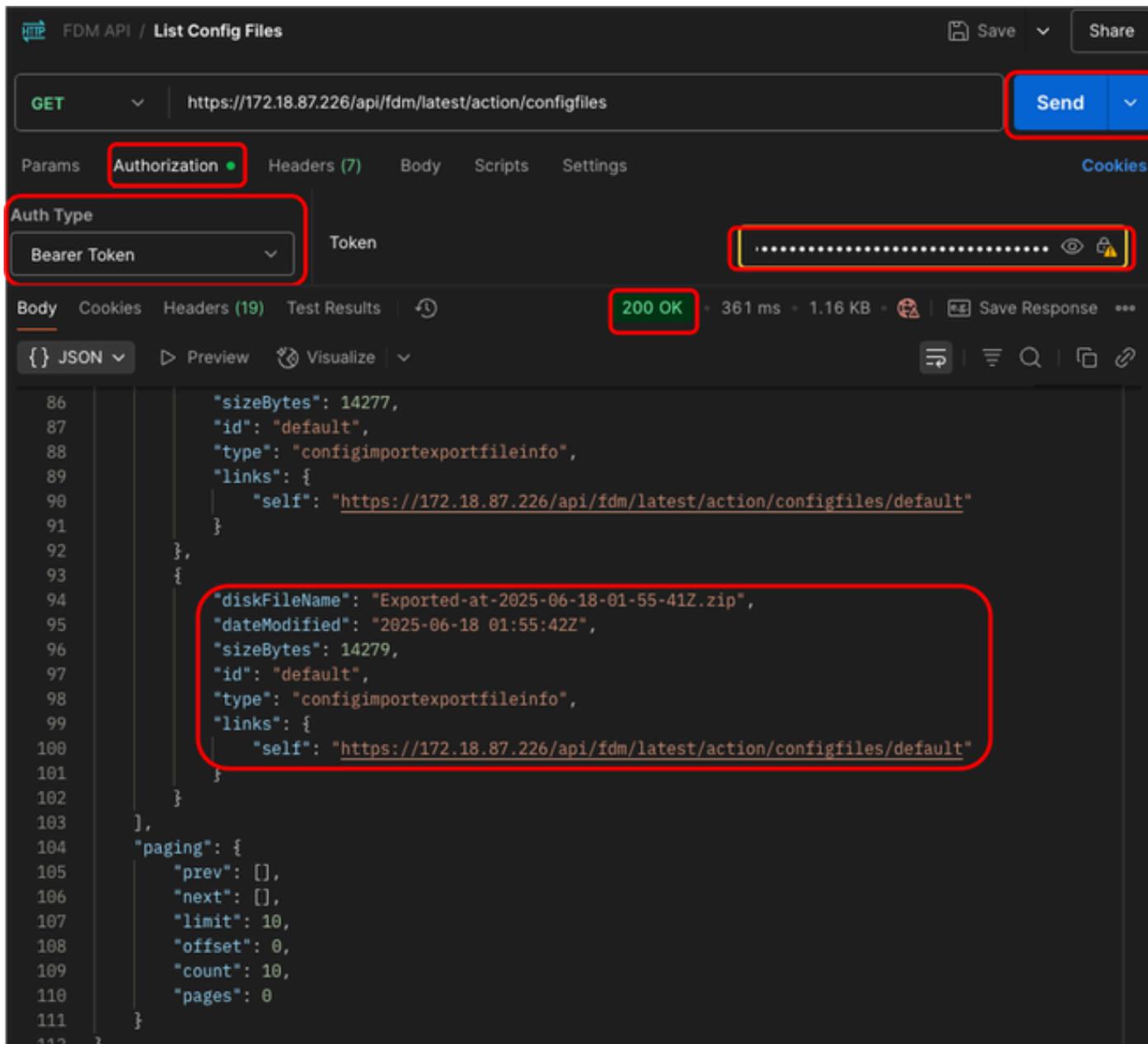
15. Appelez cette nouvelle demande : Répertoriez les fichiers de configuration. Il va être créé en tant que requête GET, également au moment où vous exécutez celle-ci, GET doit être sélectionné dans le menu déroulant. Dans la zone de texte à côté de GET, introduisez la ligne suivante `https://<FDM IP ADD>/api/fdm/last/action/configfiles`



Postman - Demande de liste des fichiers de configuration exportés

16. Dans l'onglet Autorisation, sélectionnez Bearer Token as Auth Type dans le menu déroulant, et dans la zone de texte à côté de Token, collez le jeton copié à l'étape 5. Enfin, cliquez sur Send.

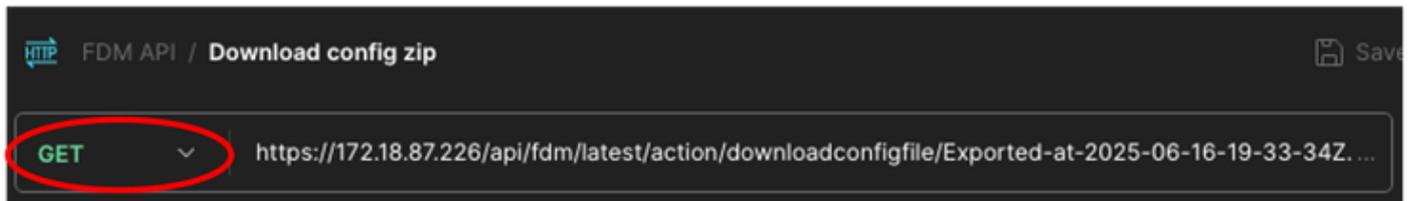
Si tout va bien, vous recevez une réponse 200 OK et dans le champ JSON, la liste des fichiers exportés s'affiche. La plus récente est répertoriée en bas de l'écran. Copiez le dernier nom de fichier (date plus récente dans le nom de fichier) car il sera utilisé à la dernière étape.



Postman - List Exported Config Files Request - Autorisation et sortie

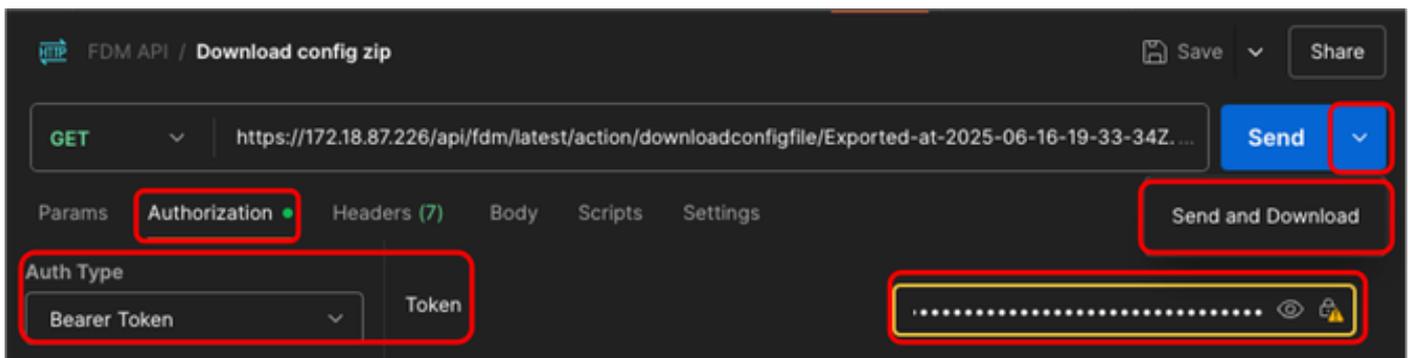
17. Répétez l'étape 2. Pour créer une nouvelle demande, GET sera utilisé cette fois-ci.

18. Appelez cette nouvelle demande : Téléchargez le fichier zip config. Il va être créé en tant que requête GET, également au moment où vous exécutez celle-ci, GET doit être sélectionné dans le menu déroulant. Dans la zone de texte en regard de GET, introduisez la ligne suivante, en collant à la fin le nom de fichier que vous avez copié à l'étape 16. `https://<FDM IP ADD>/api/fdm/last/action/downloadconfigfile/<Exported_File_name.zip >`



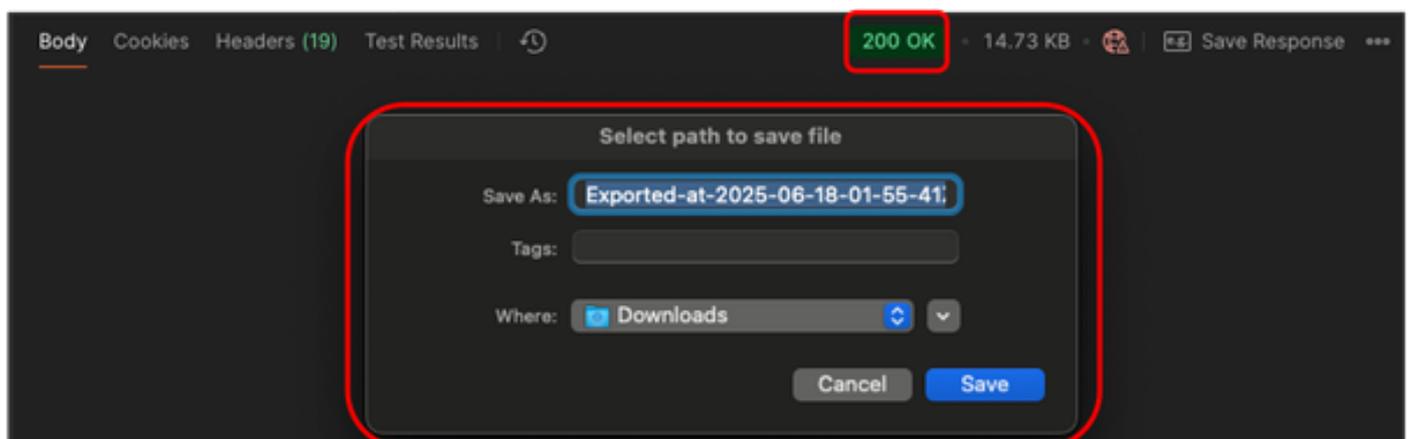
Postman - Télécharger la demande de fichier Config.zip

19. Dans l'onglet Autorisation, sélectionnez Bearer Token as Auth Type dans le menu déroulant, et dans la zone de texte à côté de Token, collez le jeton copié à l'étape 5. Enfin, cliquez sur la flèche vers le bas à côté de Send et choisissez Send and Download.



Postman - Télécharger le fichier Config.zip - Demande d'autorisation

20. Si tout va bien, vous recevez une réponse 200 OK et une fenêtre contextuelle s'affiche pour vous demander le dossier de destination dans lequel le fichier configuration.zip va être enregistré. Ce fichier .zip peut désormais être téléchargé vers l'outil de migration du pare-feu.



Postman - Télécharger la demande de fichier Config.zip - Enregistrer

Outil de migration de pare-feu

21. Ouvrez l'outil de migration de pare-feu et, dans le menu déroulant Sélectionner la configuration source, sélectionnez Cisco Secure Firewall Device Manager (7.2+) et cliquez sur Démarrer la 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 - Sélection FDM

22. Cochez la première case d'option, Migrate Firewall Device Manager (Shared Configurations Only) et cliquez sur 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)

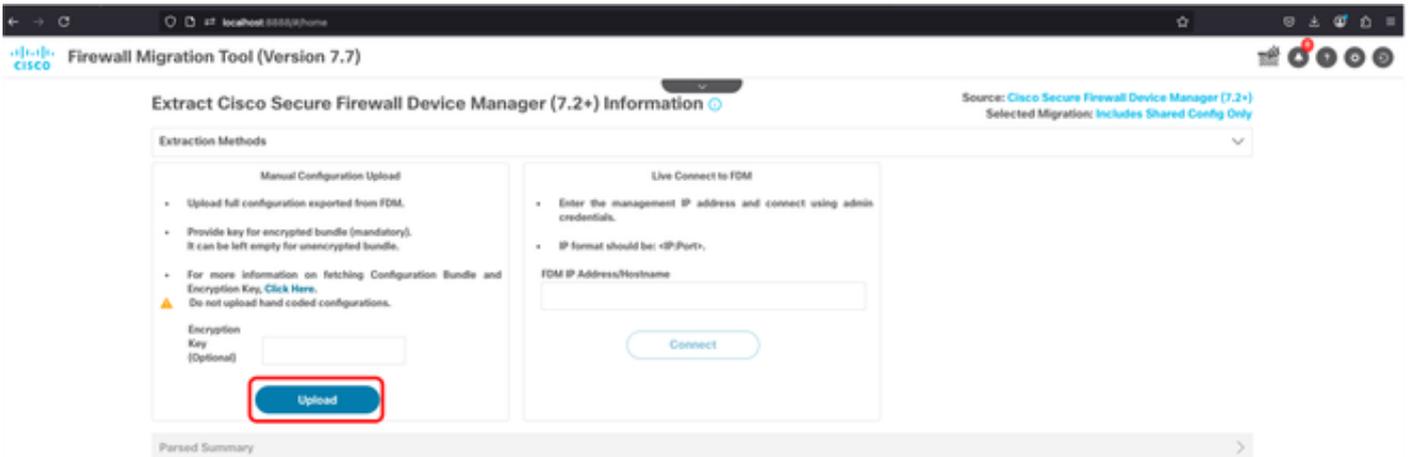
Note :

- 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

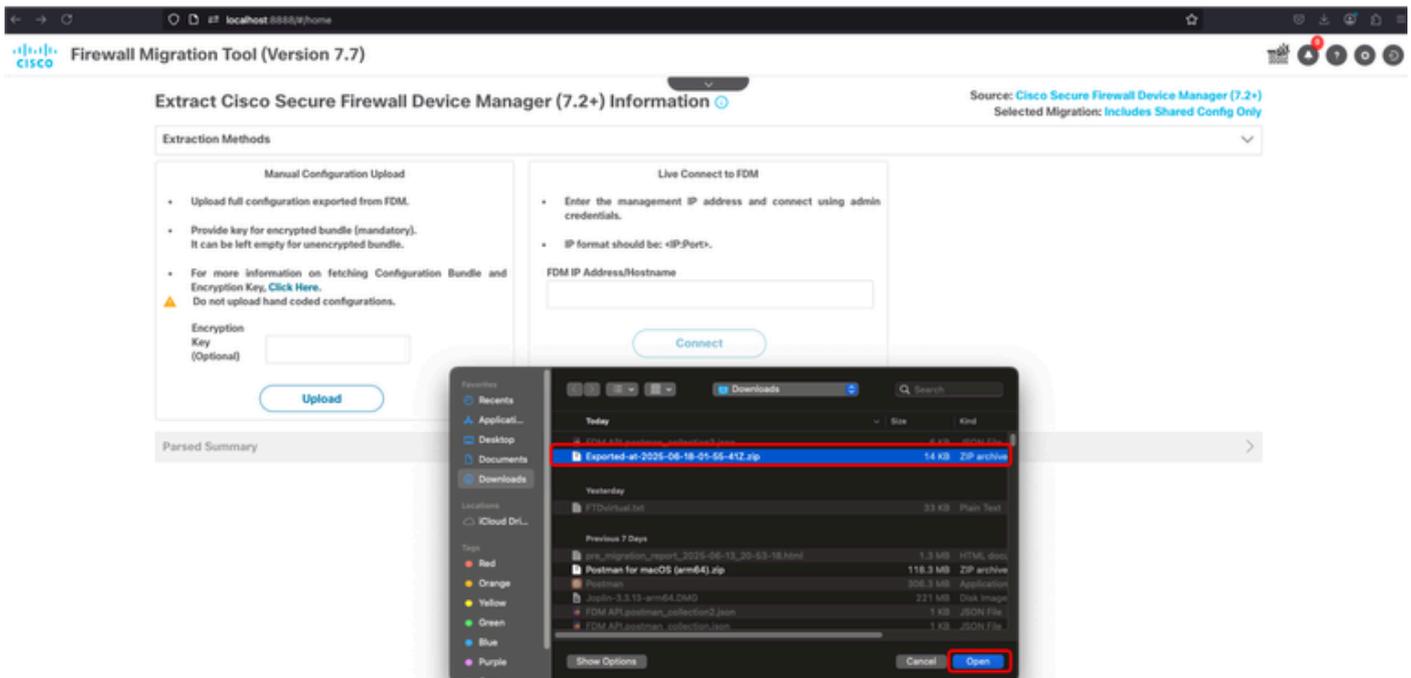
FMT - Configurations partagées de migration FDM uniquement

23. Dans le volet de gauche (Manual Configuration Upload), cliquez sur Upload.



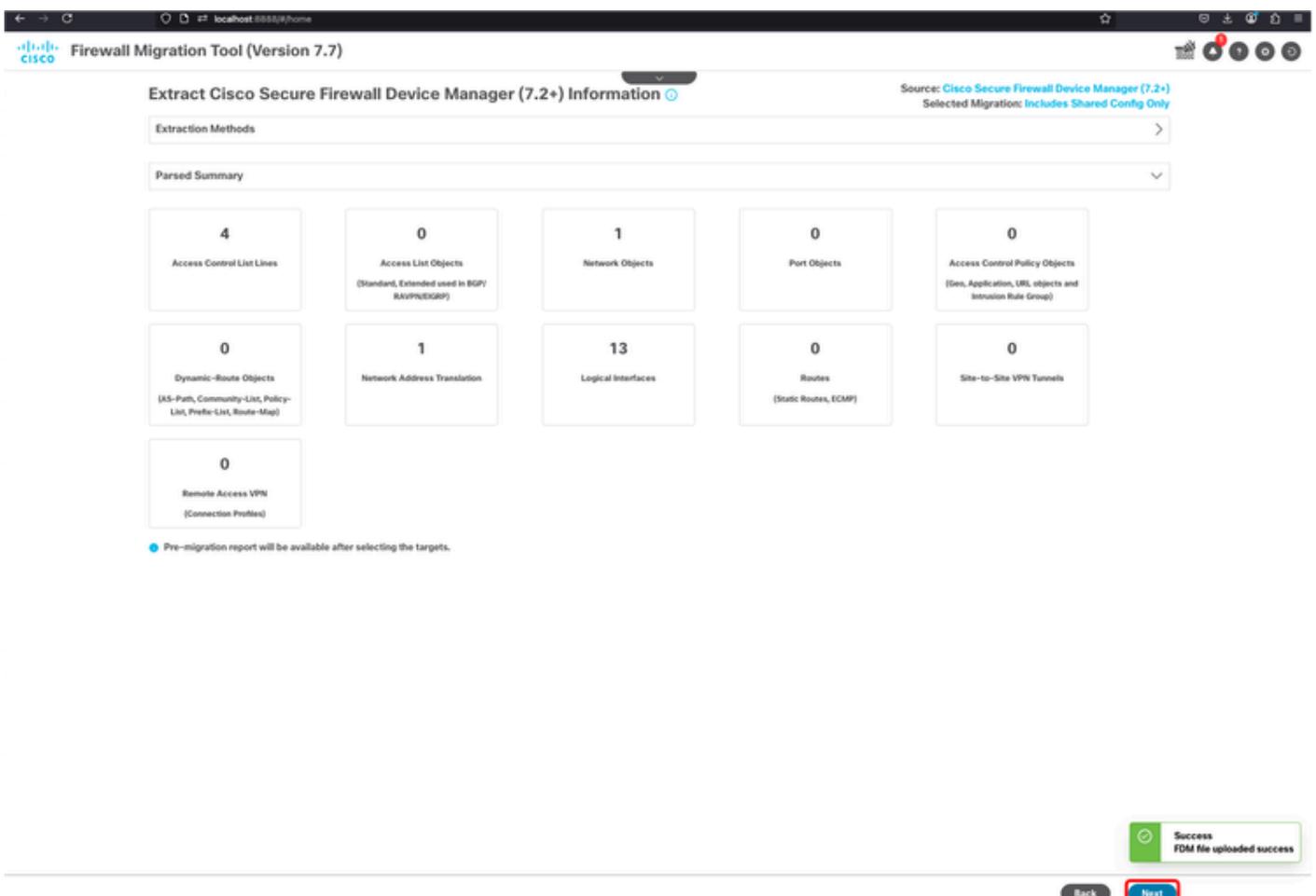
FMT - Télécharger le fichier Config.zip

24. Sélectionnez le fichier de configuration zip exporté dans le dossier que vous avez précédemment enregistré et cliquez sur Ouvrir.



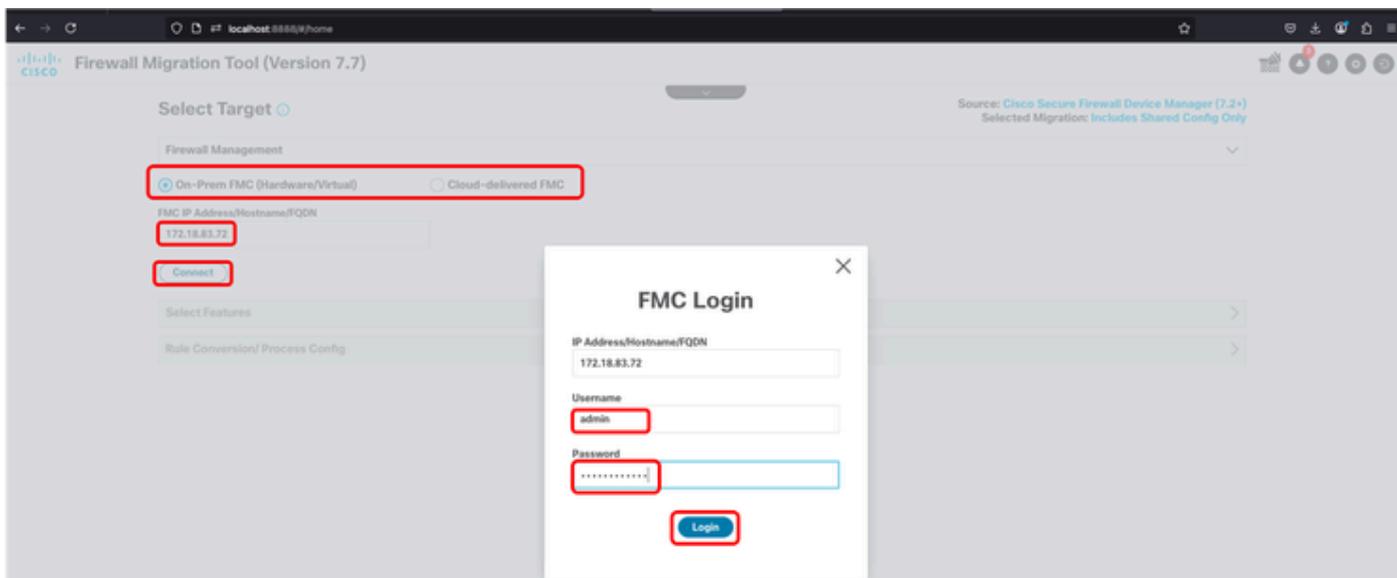
FMT - Sélection du fichier Config.zip

25. Si tout se passe comme prévu, le résumé analysé s'affiche. En outre, dans le coin inférieur droit, une fenêtre contextuelle s'affiche pour vous informer que le fichier FDM a été téléchargé avec succès. Cliquez sur Next (Suivant).



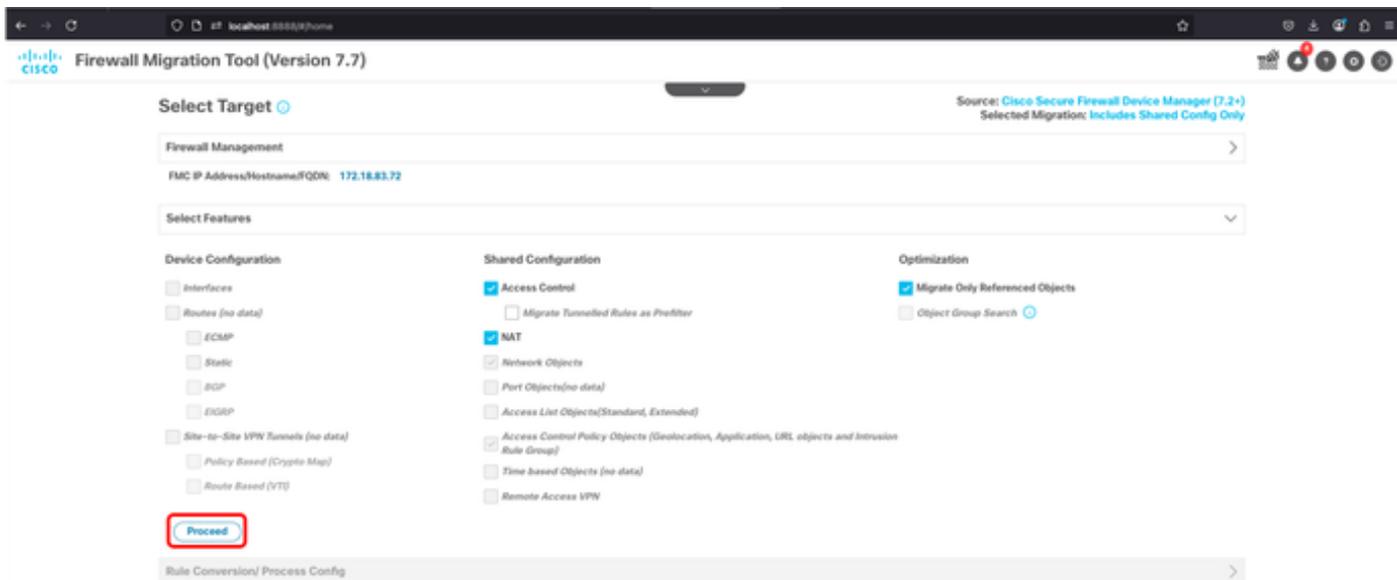
FMT - Résumé d'analyse

26. Cochez l'option qui convient le mieux à votre environnement (On-Prem FMC ou Cd-FMC). Dans ce scénario, un contrôleur FMC sur site est utilisé. Tapez l'adresse IP FMC et cliquez sur Connect. Une nouvelle fenêtre contextuelle apparaît et demande des informations d'identification FMC, après avoir saisi ces informations, cliquez sur Login.



FMT - Connexion à la cible FMC

27. L'écran suivant affiche le FMC cible et les fonctionnalités qui vont être migrées. Cliquez sur Continuer.



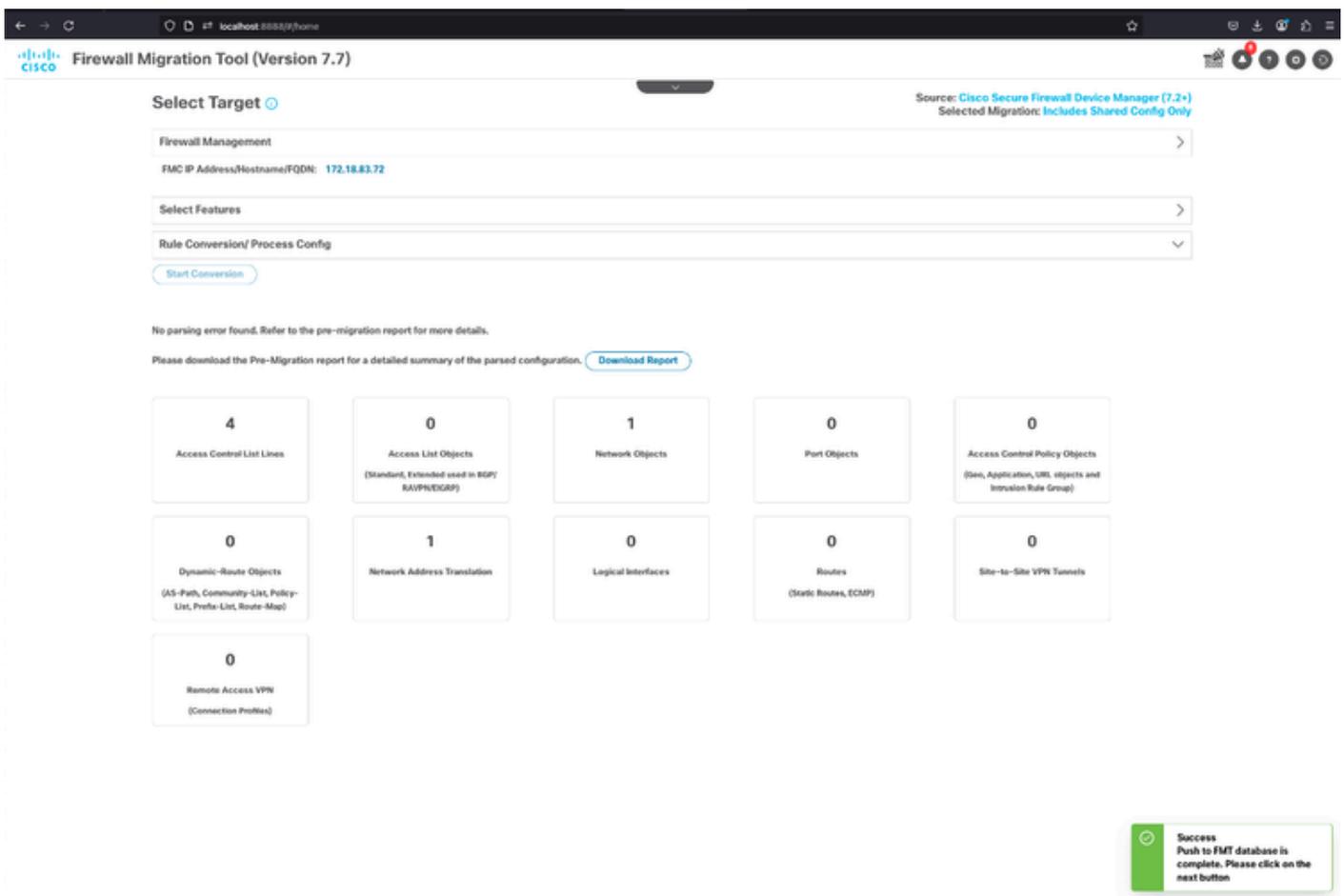
FMT - Cible FMC - Sélection de fonctionnalités

28. Une fois la cible FMC confirmée, cliquez sur le bouton Démarrer la conversion.



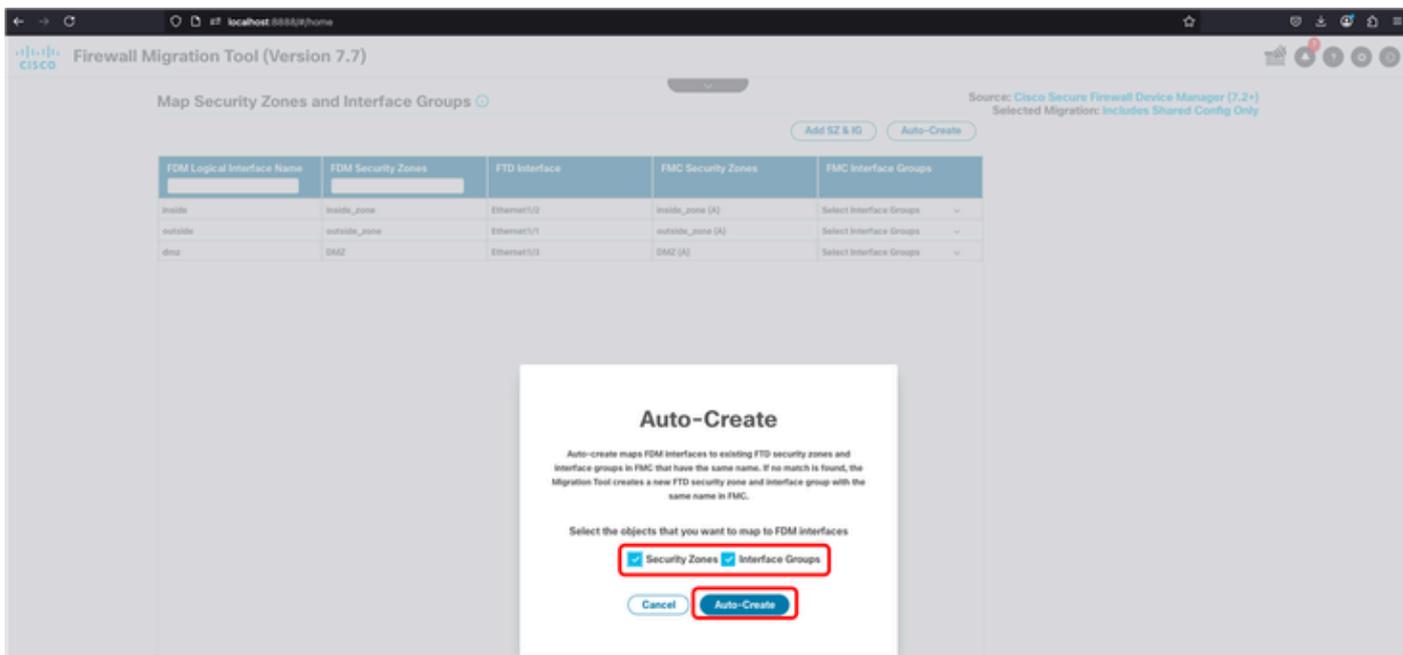
FMT - Démarrage de la conversion de configuration

29. Si tout se passe comme prévu, une fenêtre contextuelle s'affiche dans le coin inférieur droit pour indiquer que l'envoi à la base de données FMT est terminé. Cliquez sur Next (Suivant).



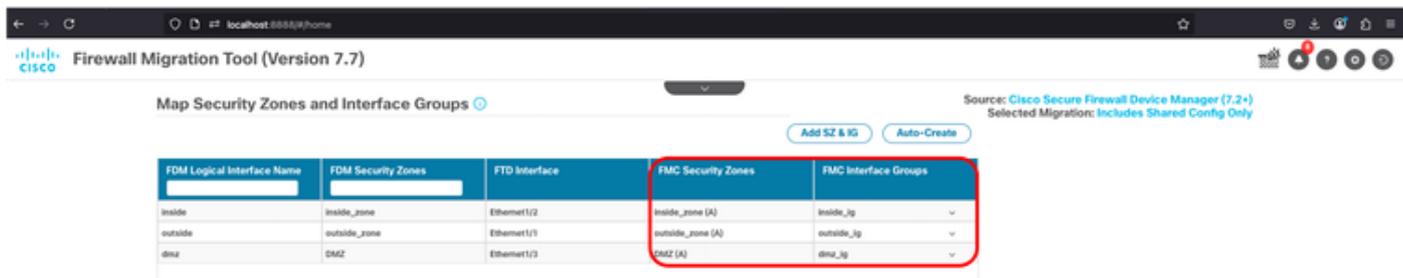
FMT - Diffusion de la base de données terminée

30. Dans l'écran suivant, vous devez créer manuellement ou choisir de créer automatiquement les zones de sécurité et les groupes d'interfaces. Dans ce scénario, la création automatique est utilisée.



FMT - Création automatique de zones de sécurité et de groupes d'interfaces

31. Une fois terminé, le tableau indique dans les 4e et 5e colonnes, respectivement, la zone de sécurité et le groupe d'interfaces.



FMT - Création des zones de sécurité et des groupes d'interfaces réussie

32. Dans l'écran suivant, vous pouvez optimiser la liste de contrôle d'accès ou simplement valider ACP, Objets et NAT. Une fois terminé, cliquez sur le bouton Valider.

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

| # | Name | SOURCE | | | DESTINATION | | | ACCESS CONTROL POLICY ... | | | ACE Count | Objects |
|--------------------------|----------------------|--------------|---------|------|--------------|---------|------|---------------------------|------|-------|-----------|---------|
| | | Zone | Network | Port | Zone | Network | Port | Applications | URLs | State | | |
| <input type="checkbox"/> | Inside_Outside_Bu... | inside_zone | ANY | ANY | outside_m... | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | AD-Srvr_01 | DMZ | AD-Srvr | ANY | inside_zone | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | DMZ-Inside_01 | DMZ | ANY | ANY | inside_zone | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | Outside_DMZ_01 | outside_m... | ANY | ANY | DMZ | ANY | ANY | ANY | ANY | deny | 1 | None |

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

Optimize ACL Validate

FMT - Optimiser ACL - Valider la migration

33. La validation ne prend que quelques minutes.

Firewall Migration Tool (Version 7.7)

Optimize, Review and Validate Shared Configuration

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

| # | Name | SOURCE | | | DESTINATION | | | ACCESS CONTROL POLICY ... | | | ACE Count | Objects |
|--------------------------|----------------------|--------------|---------|------|--------------|---------|------|---------------------------|------|-------|-----------|---------|
| | | Zone | Network | Port | Zone | Network | Port | Applications | URLs | State | | |
| <input type="checkbox"/> | Inside_Outside_Bu... | inside_zone | ANY | ANY | outside_m... | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | AD-Srvr_01 | DMZ | AD-Srvr | ANY | inside_zone | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | DMZ-Inside_01 | DMZ | ANY | ANY | inside_zone | ANY | ANY | ANY | ANY | deny | 1 | None |
| <input type="checkbox"/> | Outside_DMZ_01 | outside_m... | ANY | ANY | DMZ | ANY | ANY | ANY | ANY | deny | 1 | None |

Validation in progress. It will take a while

FMT - Validation en cours

34. Une fois terminé, FMT vous indique que la configuration a été validée et l'étape suivante consiste à cliquer sur le bouton 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 - Validation réussie - Diffuser la configuration vers FMC

35. Enfin, cliquez sur le bouton Continuer.

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 - Poursuivre la configuration push

36. Si tout se passe comme prévu, la notification Migration réussie s'affiche. FMT vous demande de vous connecter à FMC et de déployer la stratégie migrée vers FTD.

Complete Migration

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

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)

| | | | | |
|---|--|--|---|---|
| 4 Access Control List Lines | Not selected for migration Access List Objects <small>(Standard, Extended used in NGFW, NXAF, NDGDP)</small> | 1 Network Objects | Not selected for migration Port Objects | 0 Access Control Policy Objects <small>(Deny, Application, URL, objects and Intrusion Rule Group)</small> |
| Not selected for migration Dynamic-Route Objects <small>(IS-Path, Community-List, Policy-List, Profile List, Route-Map)</small> | 1 Network Address Translation | Not selected for migration Logical Interfaces | Not selected for migration Routers <small>(Static Routes, ECMP)</small> | Not selected for migration Site-to-Site VPN Tunnels |
| Not selected for migration Remote Access VPN <small>(Concurrent Profiles)</small> | | | | |

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 - Notification de migration réussie

Vérification FMC

37. Après la connexion à FMC, les politiques ACP et NAT sont affichées comme FTD-Mig. Vous pouvez maintenant poursuivre le déploiement vers le nouveau FTD.

| | Access Control Policy | Last Modified | Status |
|--------------------------|------------------------|---|--|
| <input type="checkbox"/> | ACP | 2025-06-18 00:51:41 Modified by "Firepower System" | Targeting 1 device <i>Out-of-date on all targeted devices</i> |
| <input type="checkbox"/> | FTD-Mig-ACP-1750297713 | 2025-06-18 21:48:35 Modified by "admin" | Targeting 0 devices |
| <input type="checkbox"/> | SNMP | 2025-06-18 00:51:41 Modified by "Firepower System" | Targeting 1 device <i>Out-of-date on all targeted devices</i> |

FMC - ACP migré

| | NAT Policy | Device Type | Status |
|--------------------------|--------------------|----------------|-----------------------|
| <input type="checkbox"/> | FTD-Mig-1750297649 | Threat Defense | Targeting 0 device(s) |

FMC - Politique NAT migrée

Informations connexes

- [FMT - Guide de migration FDM vers FMC](#)
- [Notes de version FMT](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.