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

Table des matières

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.

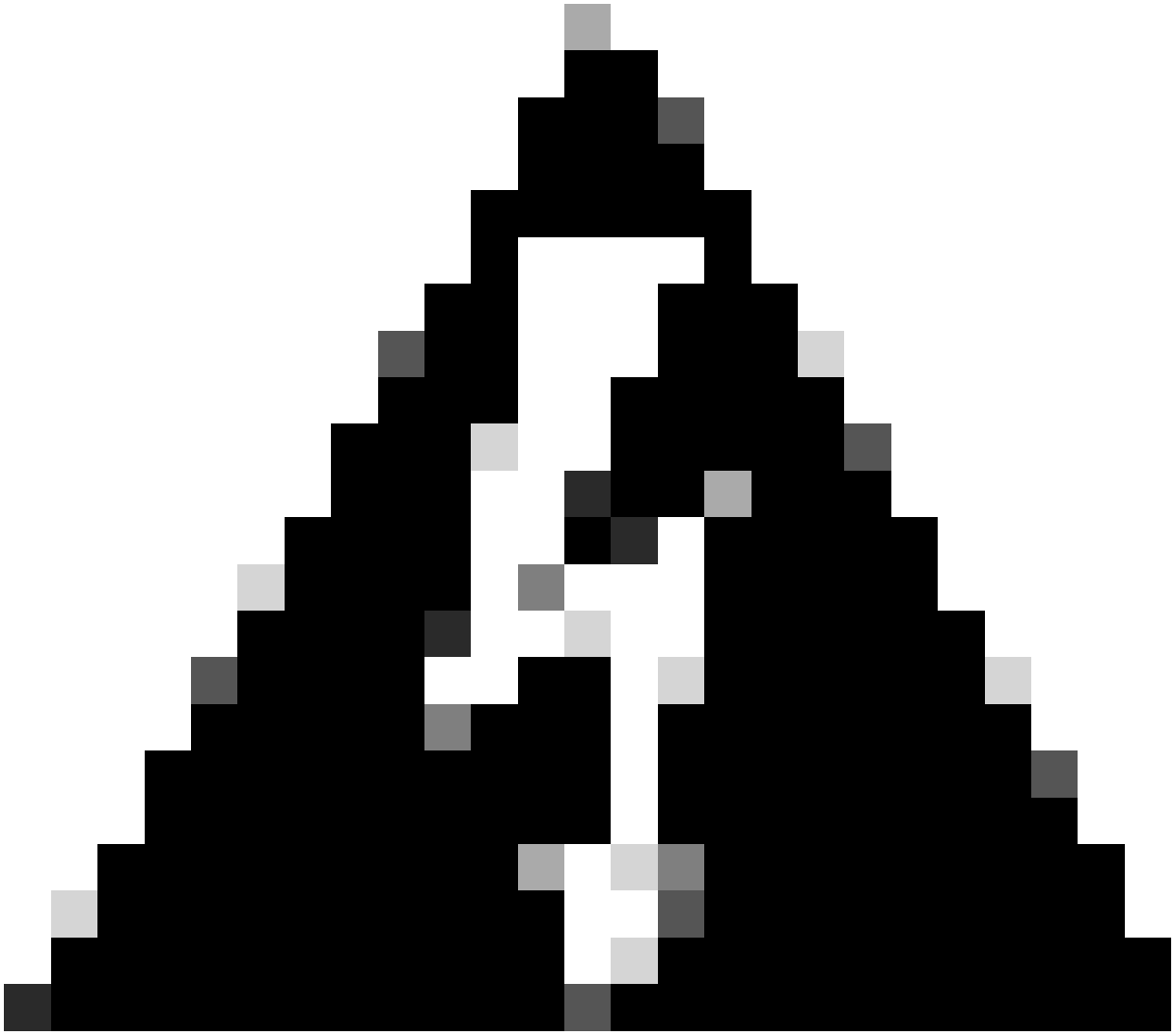
Informations générales

- 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.

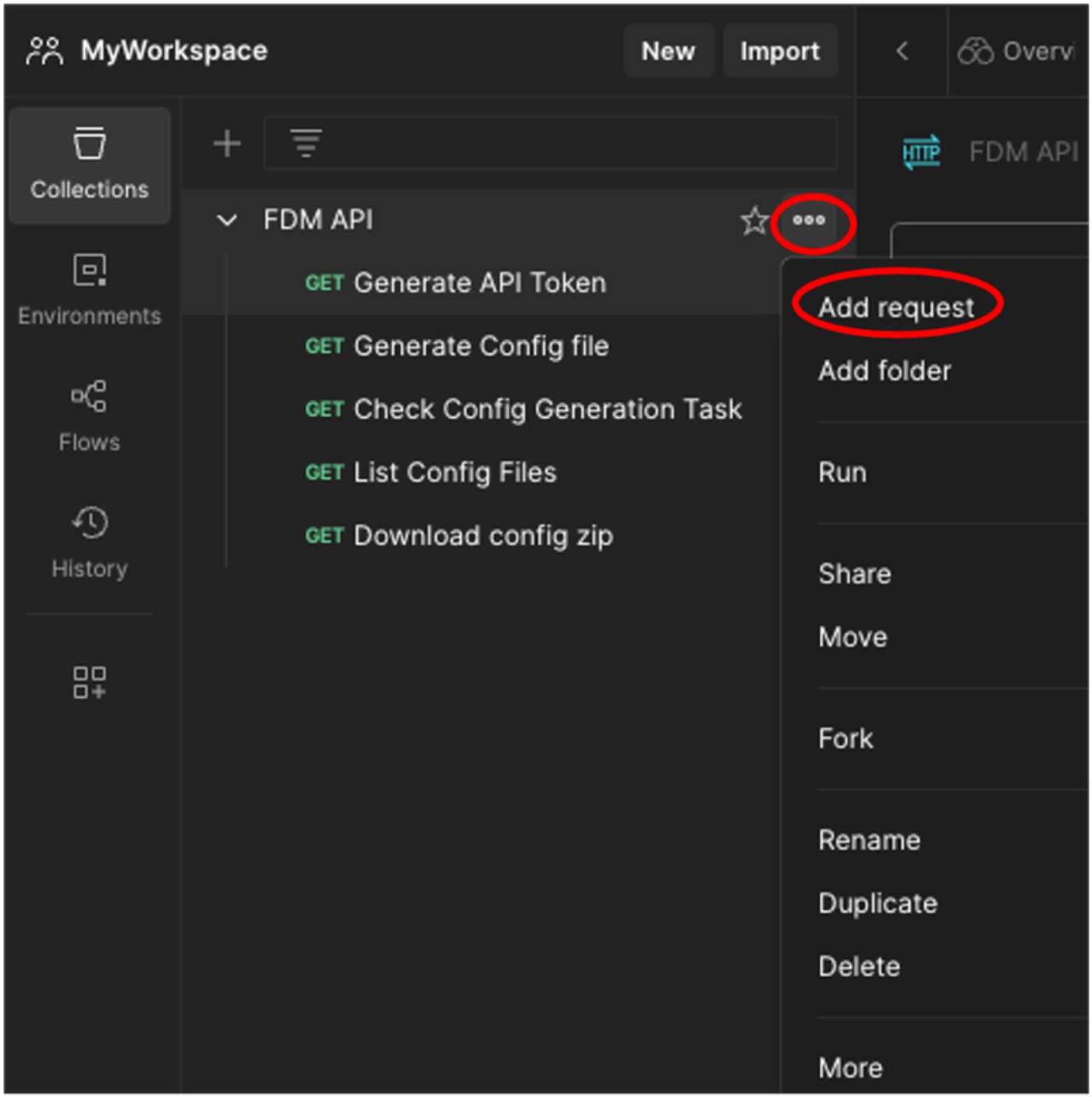


Avertissement : Le choix de ce mode permet de migrer uniquement la politique de contrôle d'accès (ACP), la politique de traduction d'adresses de réseau (NAT) et les objets. En ce qui concerne les objets, ceux-ci doivent être utilisés dans une règle ACP ou NAT, pour être migrés, sinon ils sont ignorés.

Configuration

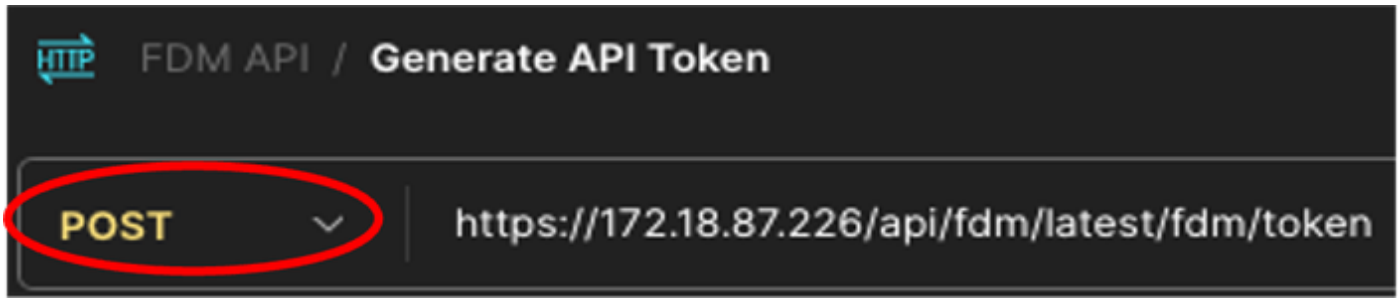
Demandes API - Postman

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.

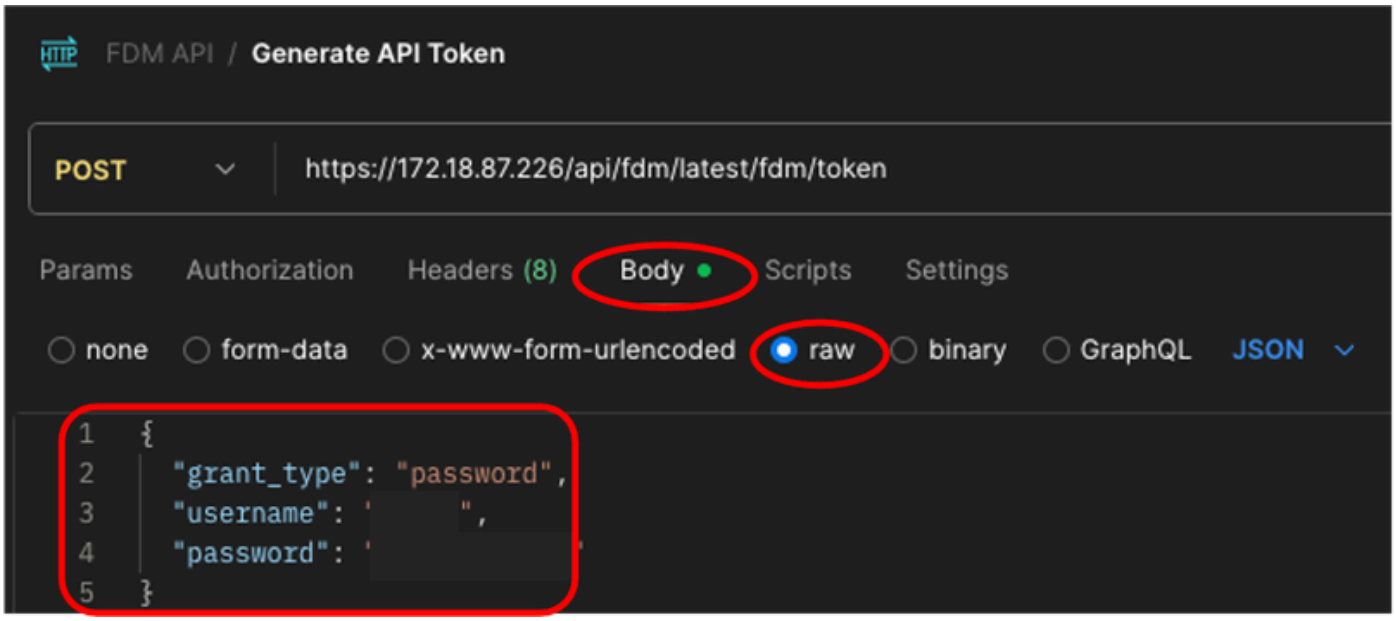
{

"grant_type" : "mot de passe",

"nom d'utilisateur" : »nom d'utilisateur",

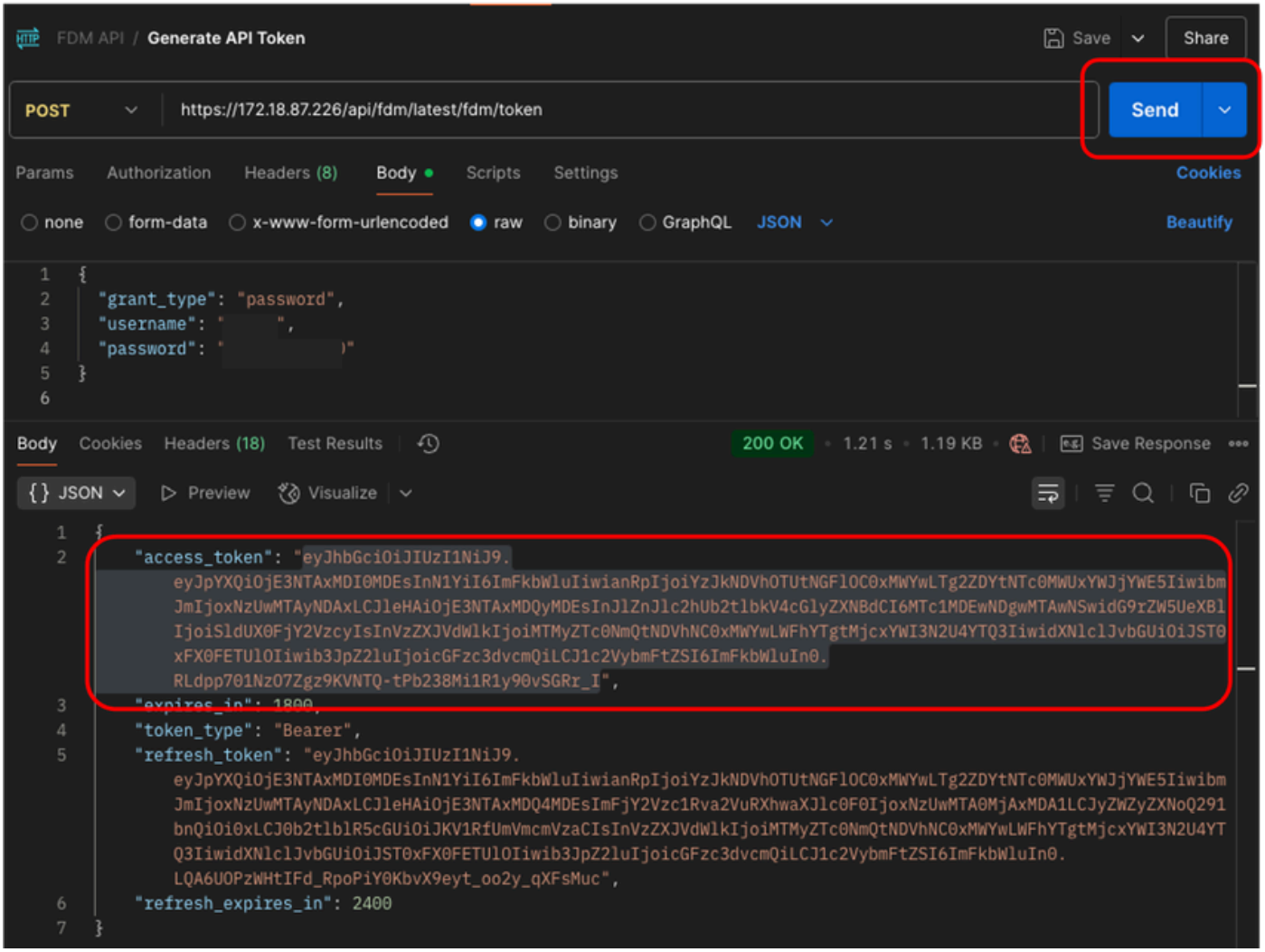
"mot de passe" : »mot de passe"

}



Postman - Corps de la demande de jeton

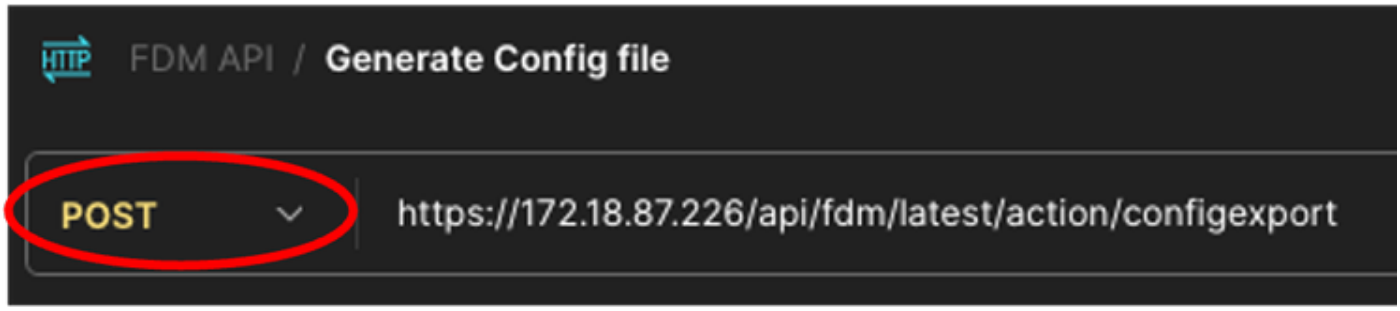
5. Enfin, cliquez sur Send pour obtenir votre jeton d'accès. Si tout va bien, vous recevez une réponse 200 OK. Faites une copie de l'ensemble du jeton (entre guillemets doubles), car il sera utilisé dans les étapes ultérieures.



Facteur - Jeton généré avec succès

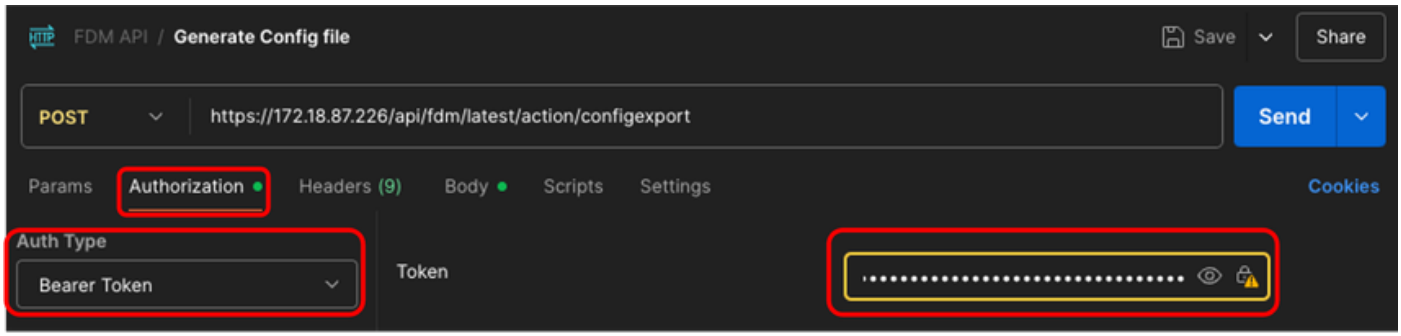
6. Répétez l'étape 2, pour créer une nouvelle demande, POST va être utilisé à nouveau.

7. Appelez cette nouvelle demande : Générez le fichier de configuration. 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/action/configexport



Postman - Générer une demande de fichier de configuration

8. Dans l'onglet Authorization, sélectionnez Bearer Token as Auth Type dans le menu déroulant, et dans la zone de texte en regard de Token, collez le jeton copié à l'étape 5.



Postman - Demande de génération de fichier de configuration - Autorisation

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

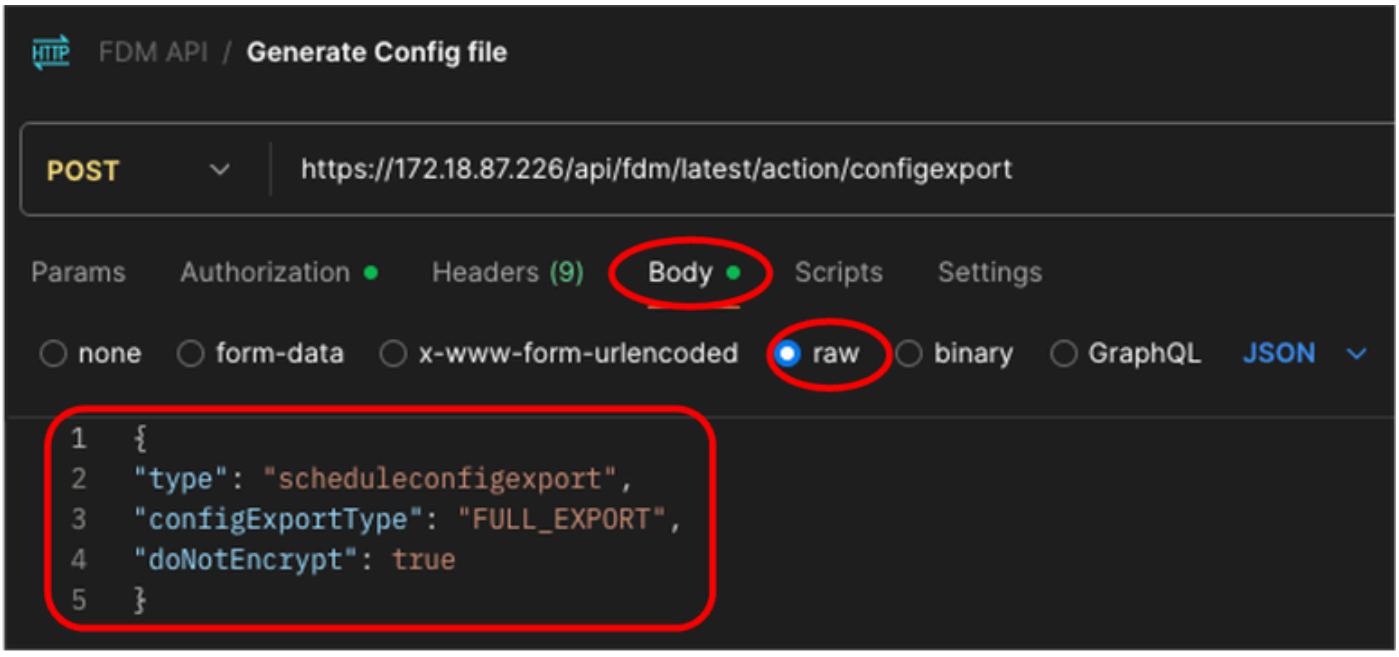
{

"type" : "schedule onfigexport",

"configExportType" : "EXPORT_COMPLET",

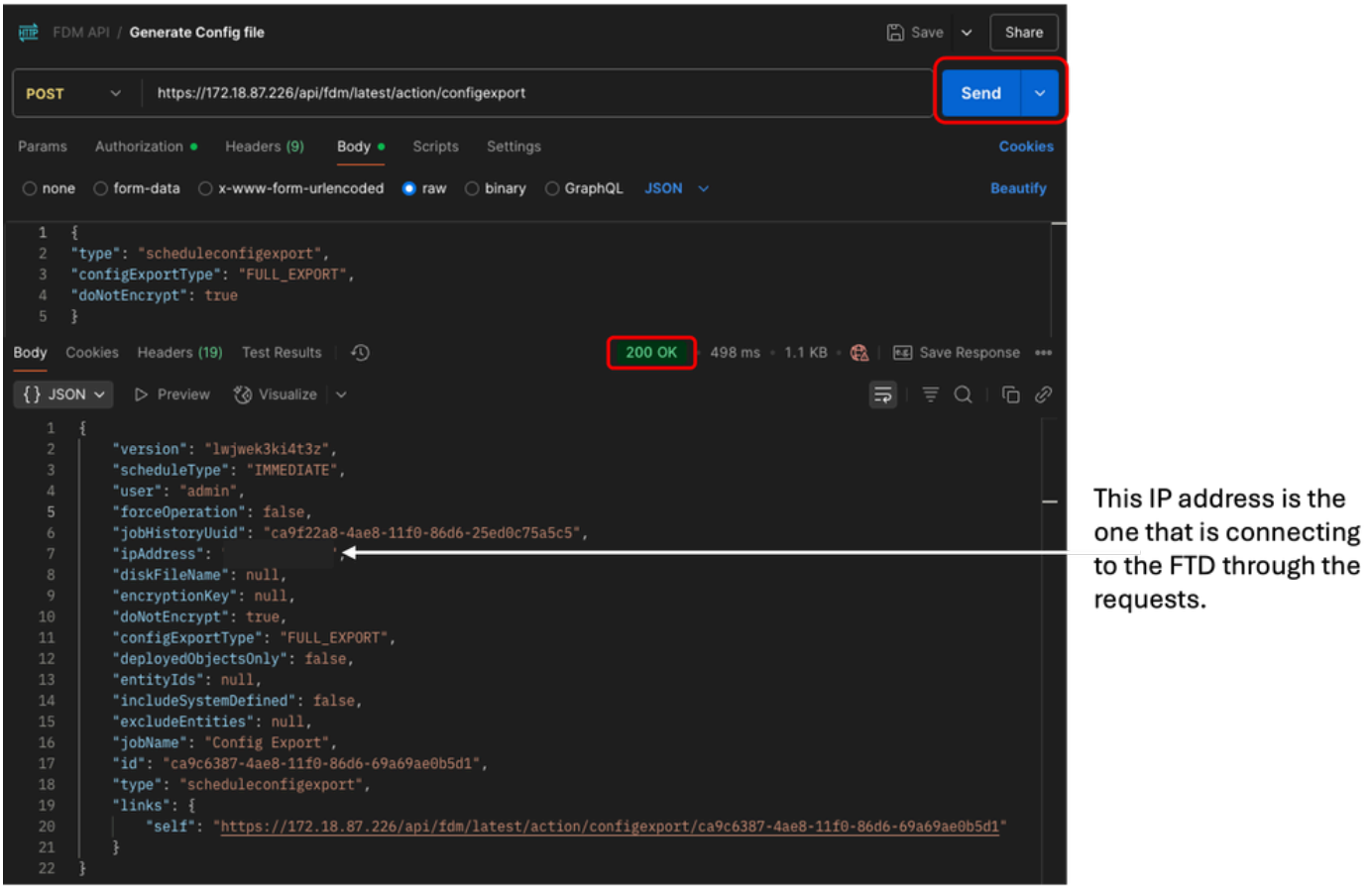
"doNotEncrypt" : vrai

}



Postman - Générer une demande de fichier de configuration - Corps

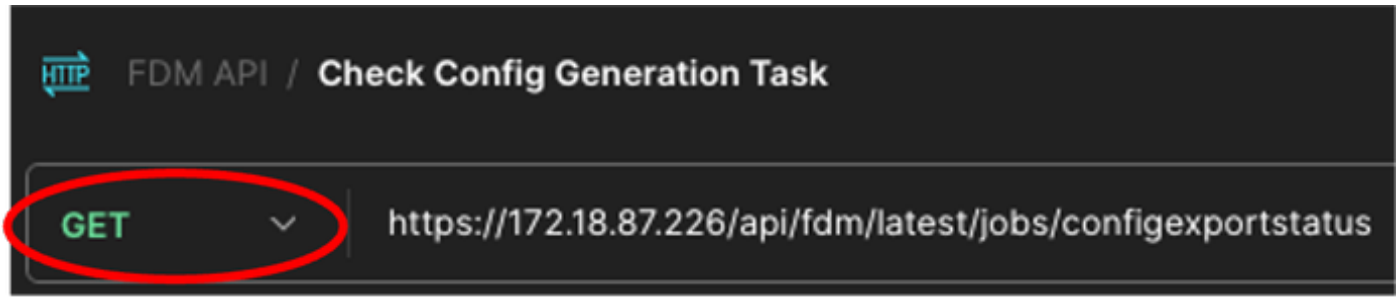
10. Enfin, cliquez sur Envoyer. Si tout va bien, vous recevez une réponse 200 OK.



Postman - Demande de génération de fichier de configuration - Sortie

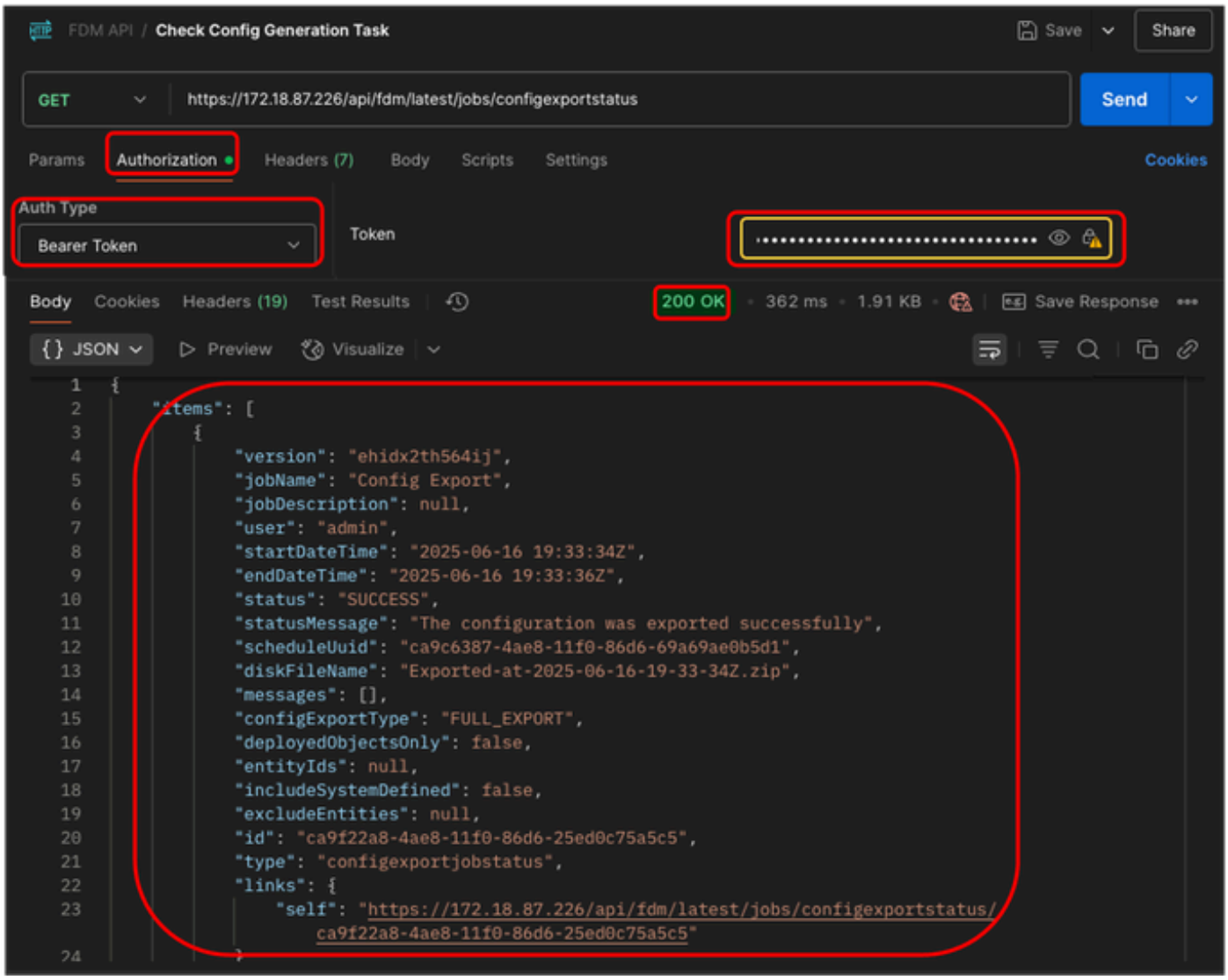
11. Répétez l'étape 2 pour créer une nouvelle demande. GET va être utilisé cette fois.

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/last/jobs/configexportstatus



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

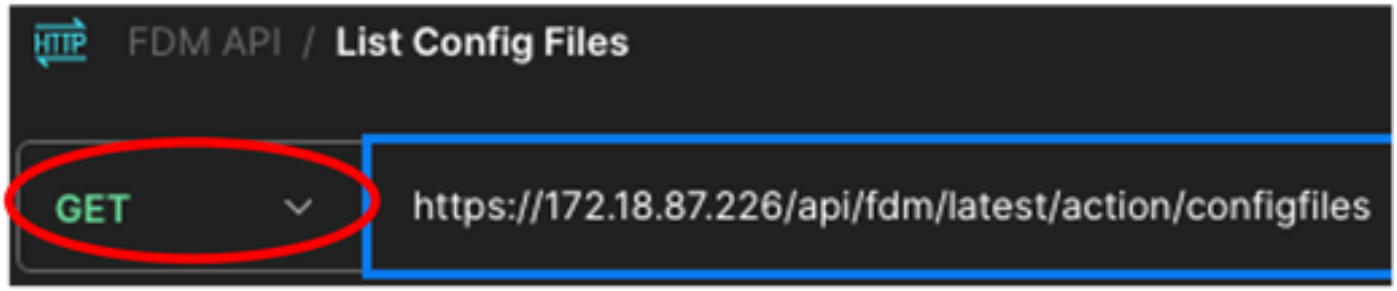
13. Dans l'onglet Autorisation, sélectionnez Bearer Token as Auth Type dans le menu déroulant, et dans la zone de texte à côté de Token, collez le jeton copié à l'étape 5. Enfin, cliquez sur Send. Si tout va bien, vous recevez une réponse 200 OK et dans le champ JSON, l'état de la tâche et d'autres détails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

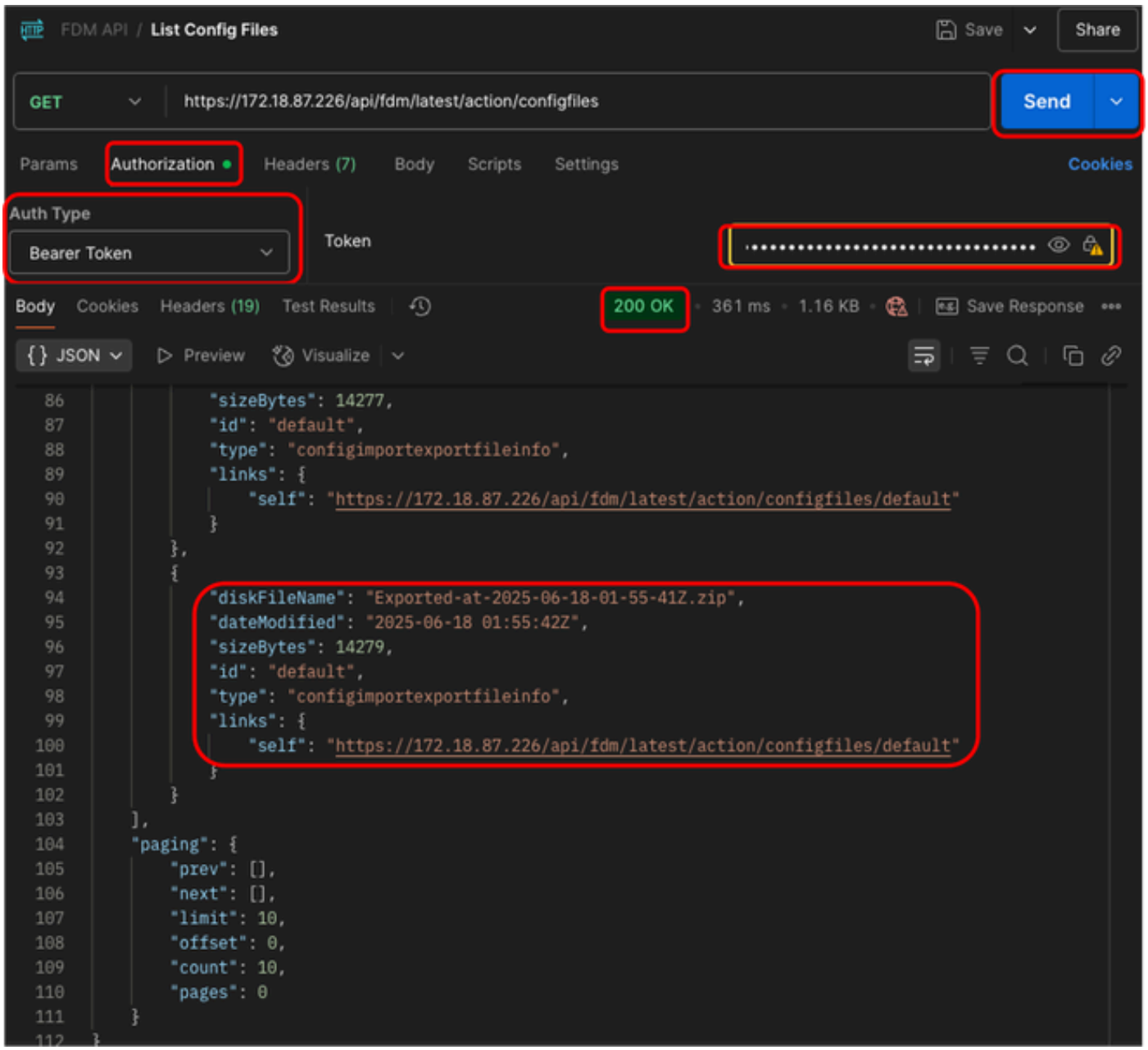
15. Appelez cette nouvelle demande : Répertoriez les fichiers de configuration. Il va être créé en tant que requête GET, également au moment où vous exécutez celle-ci, GET doit être sélectionné dans le menu déroulant. Dans la zone de texte à côté de GET, introduisez la ligne suivante https://<FDM IP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



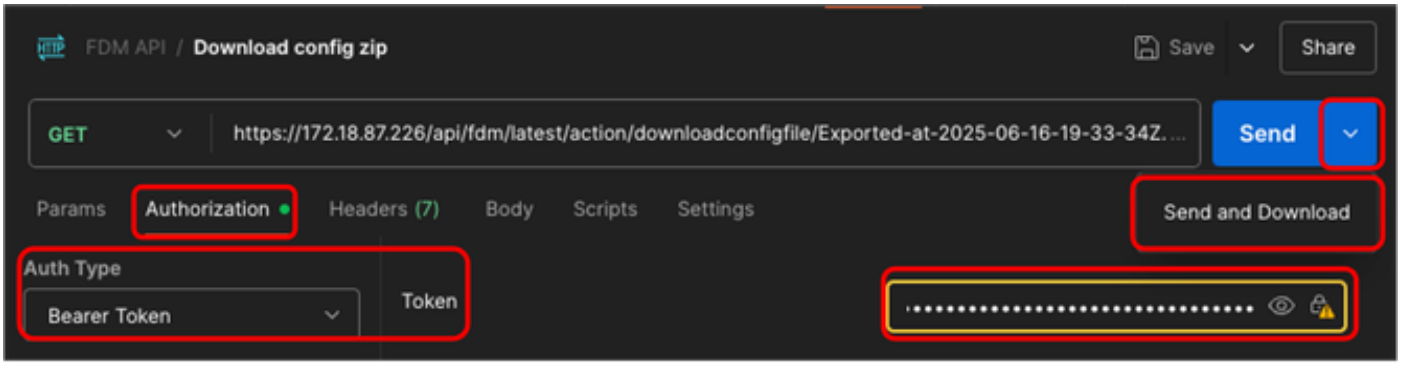
Postman - List Exported Config Files Request - Autorisation et sortie

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 >

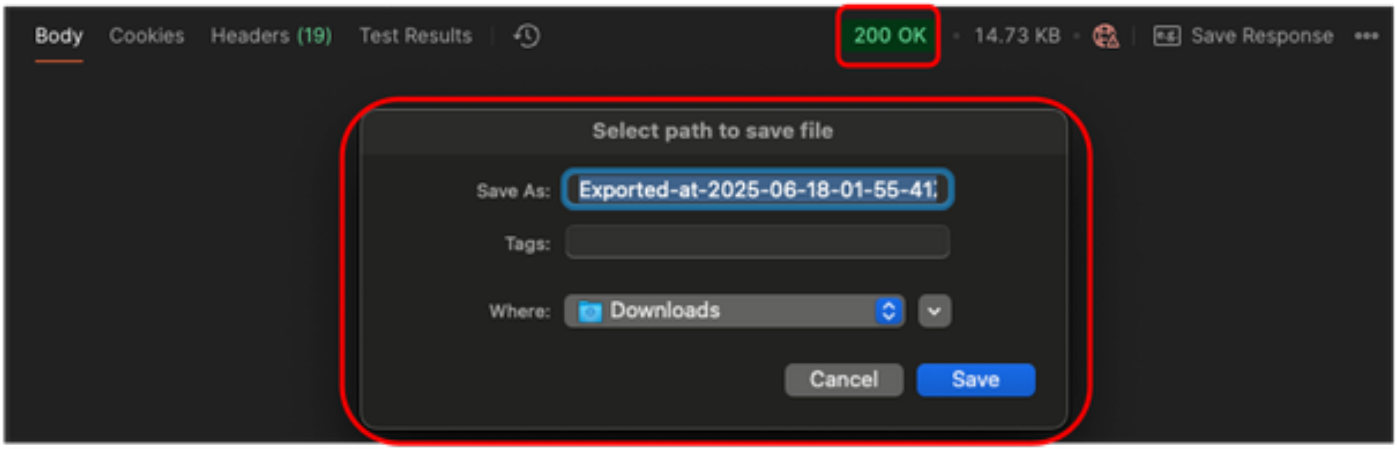
Postman - Télécharger la demande de fichier Config.zip

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

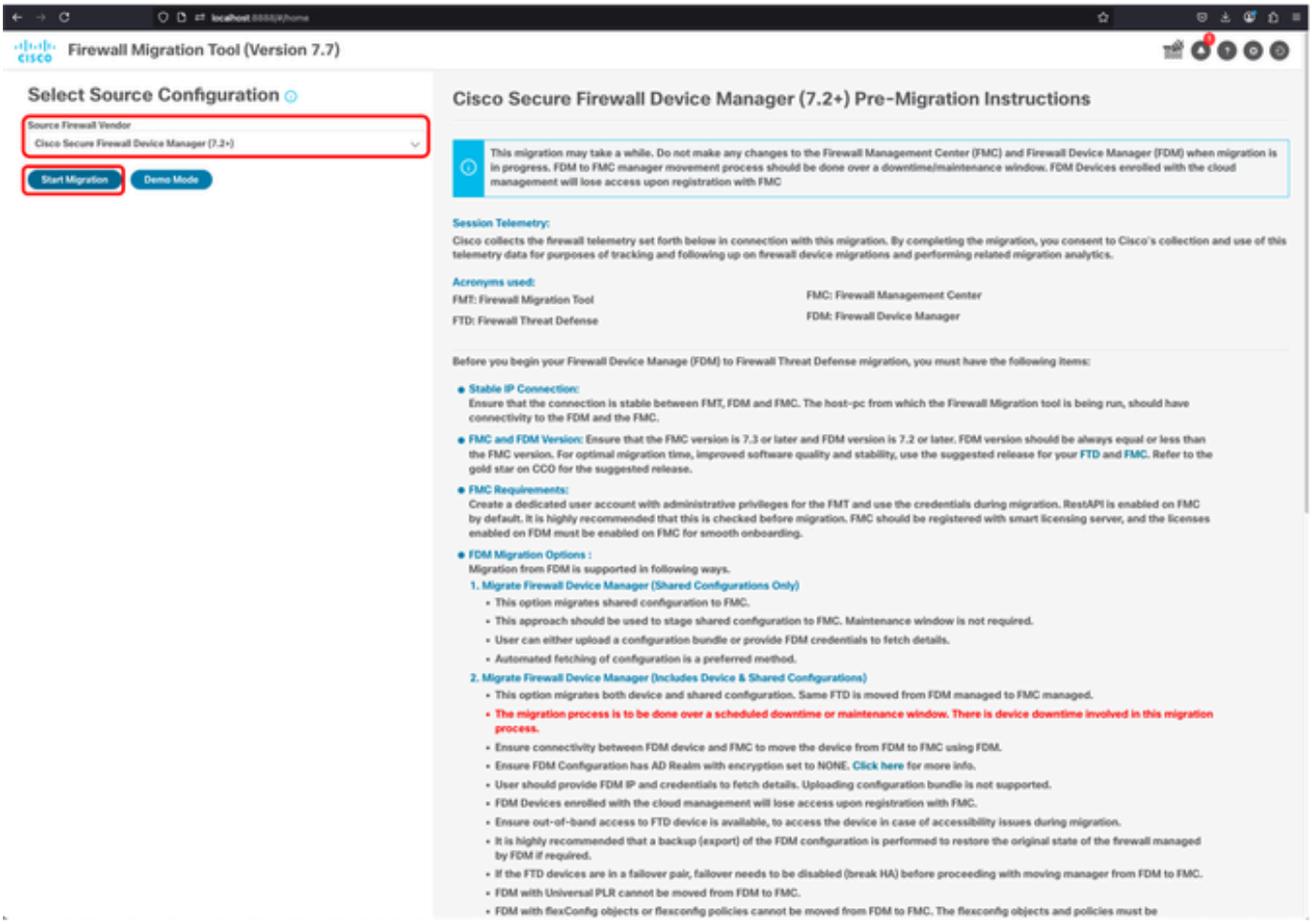
20. Si tout va bien, vous recevez une réponse 200 OK et une fenêtre contextuelle s'affiche pour vous demander le dossier de destination dans lequel le fichier configuration.zip va être enregistré. Ce fichier .zip peut désormais être téléchargé vers l'outil de migration du pare-feu.



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

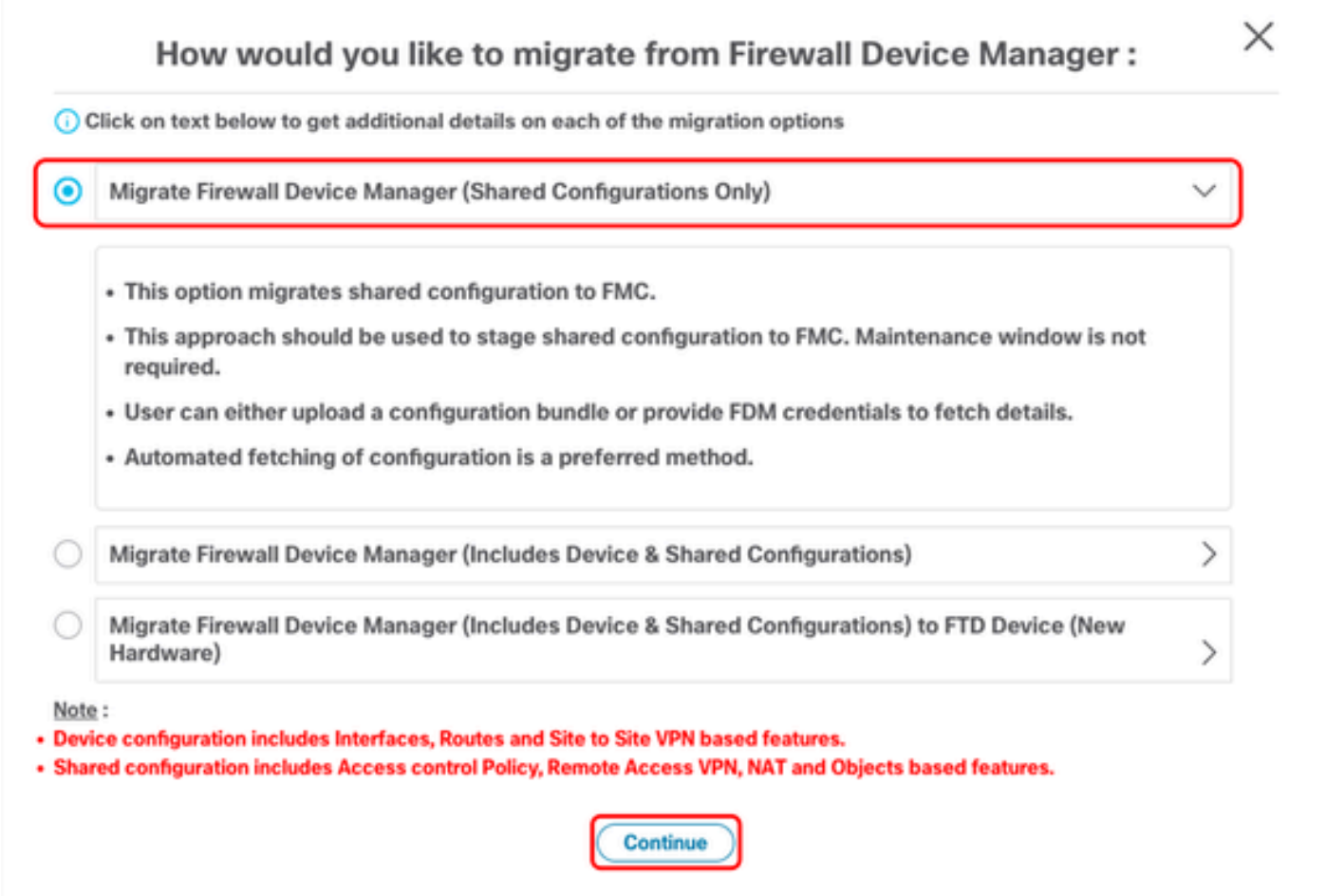
Outil de migration de pare-feu

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.



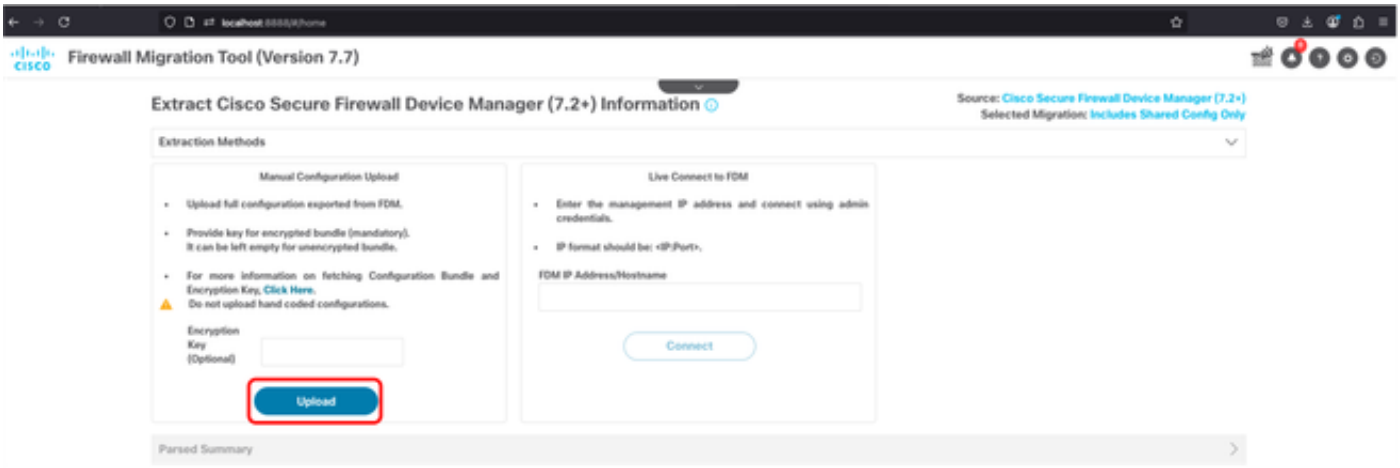
FMT - Sélection FDM

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



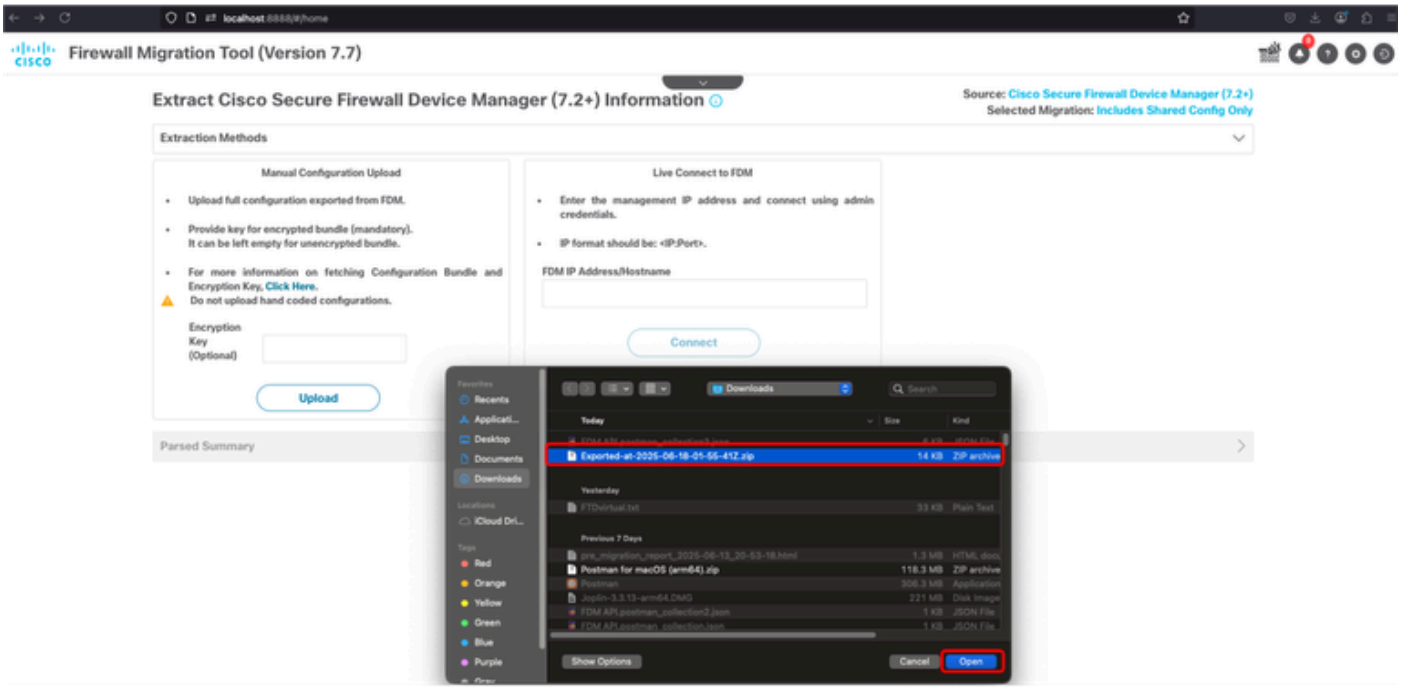
FMT - Configurations partagées de migration FDM uniquement

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



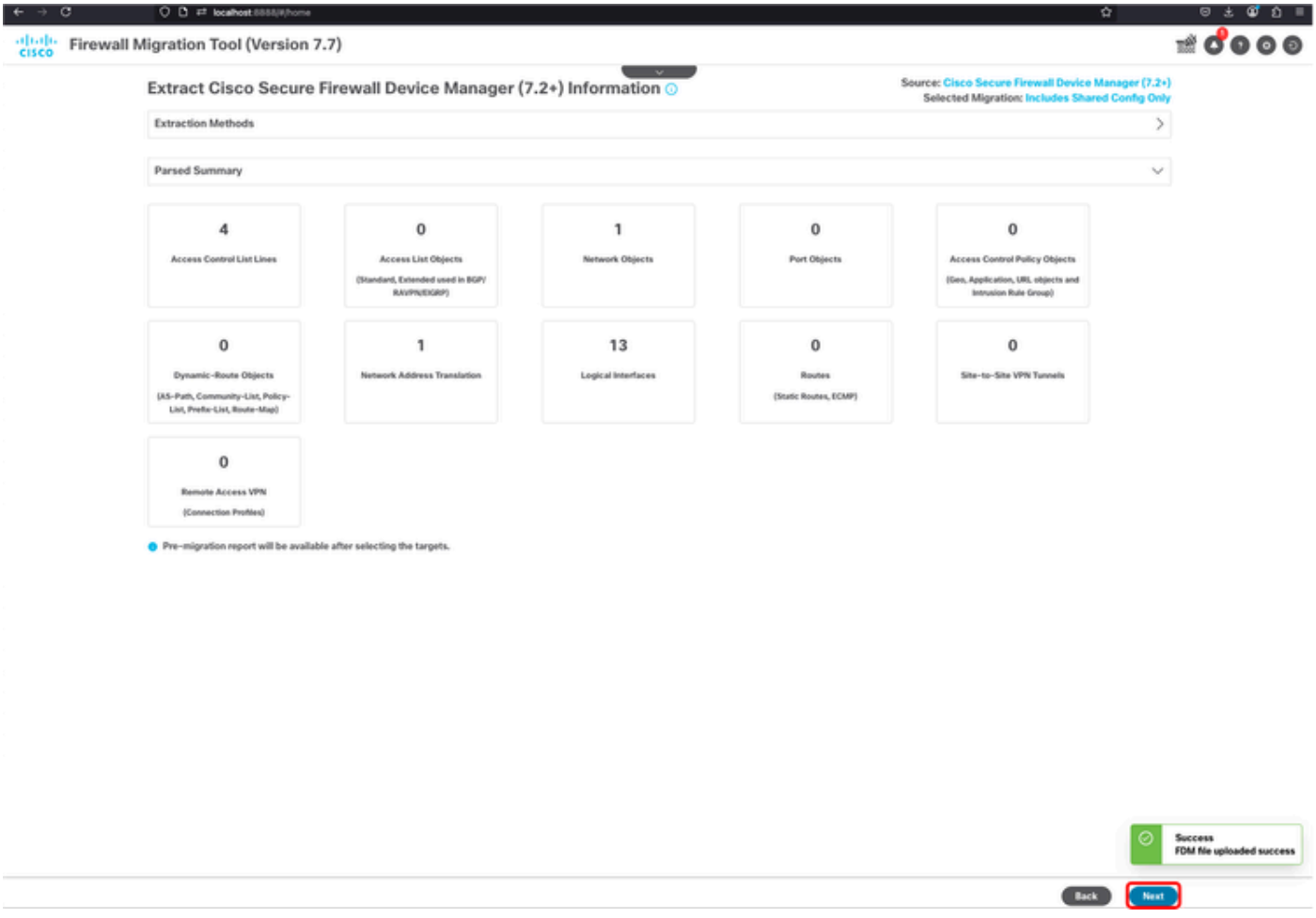
FMT - Télécharger le fichier Config.zip

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



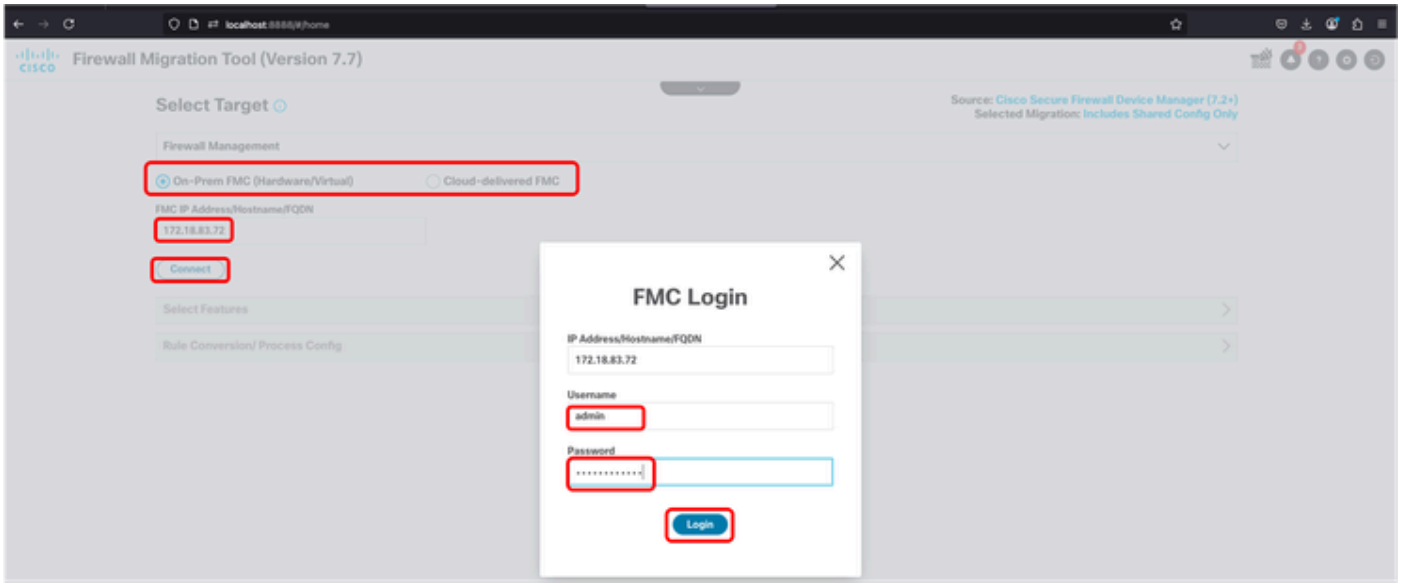
FMT - Sélection du fichier Config.zip

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).



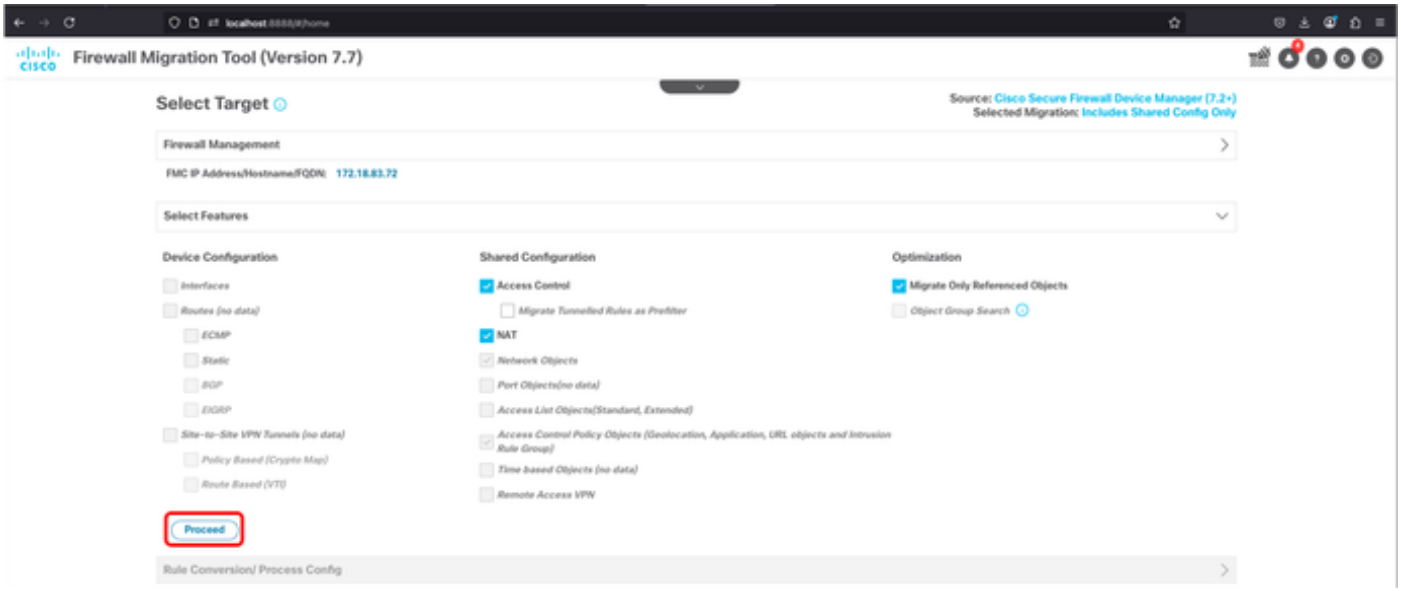
FMT - Résumé d'analyse

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.

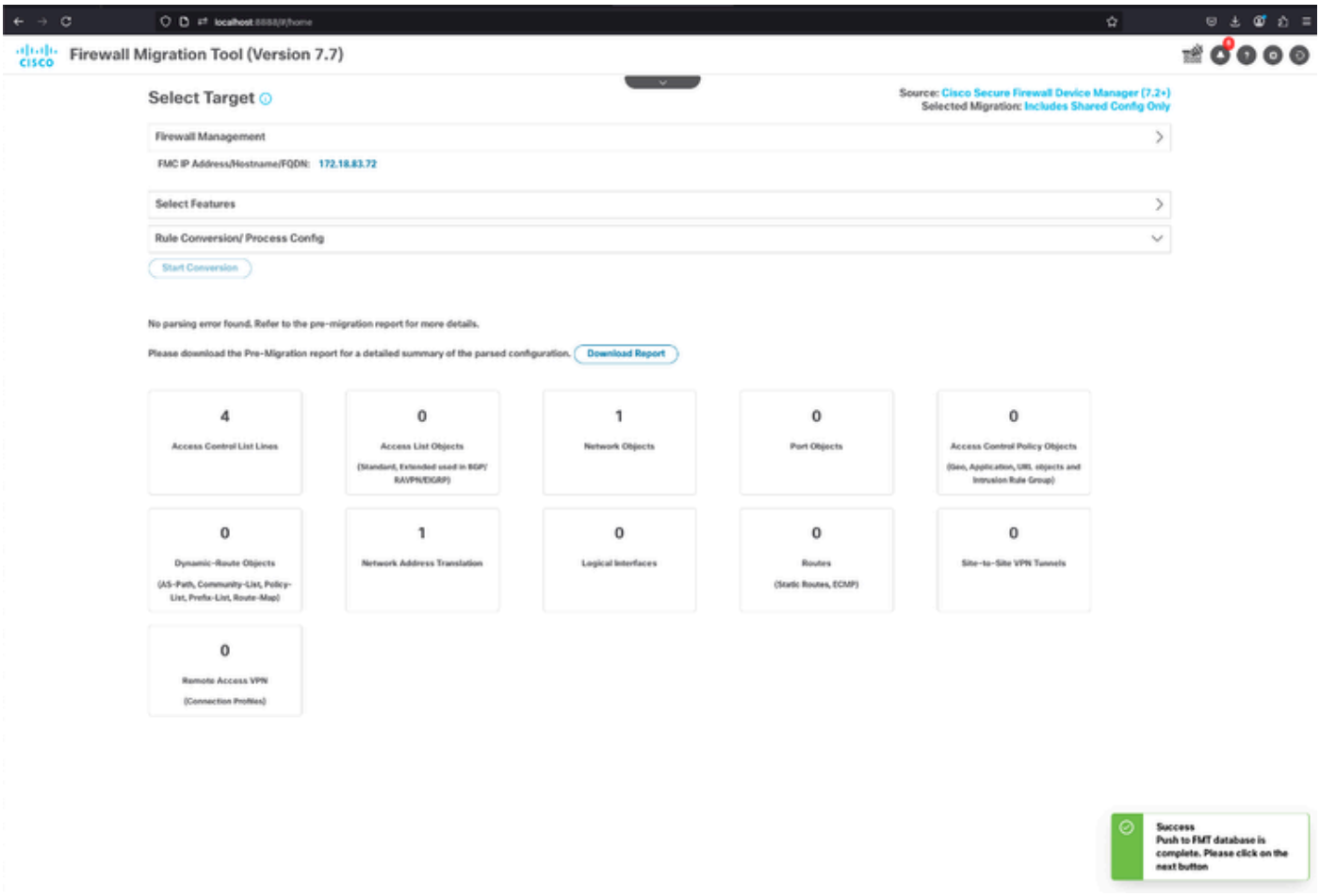


FMT - Cible FMC - Sélection de fonctionnalités

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

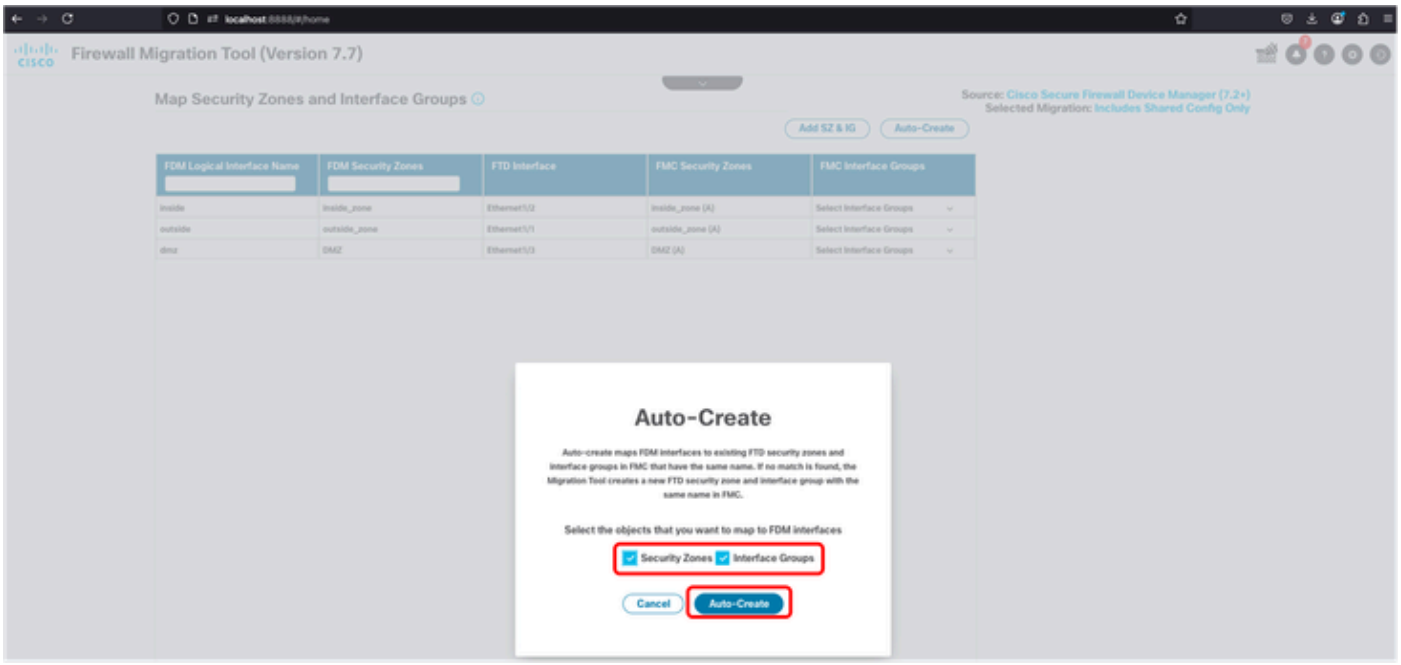
FMT - Démarrage de la conversion de configuration

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).



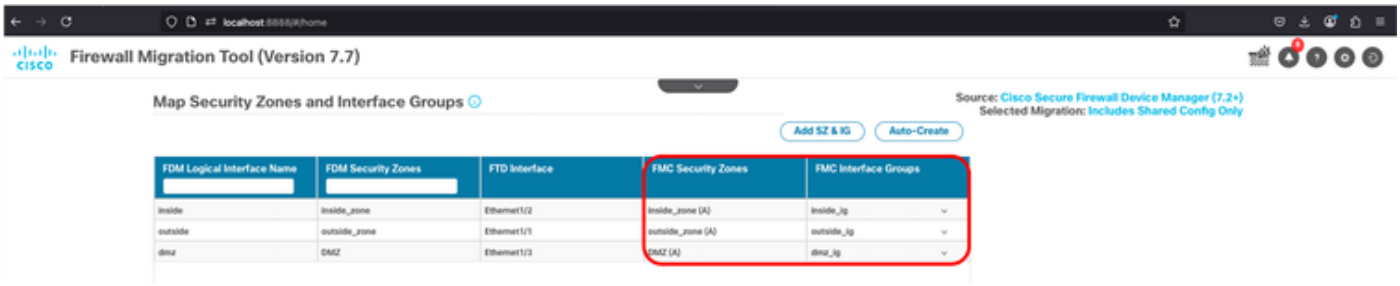
FMT - Diffusion de la base de données terminée

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.



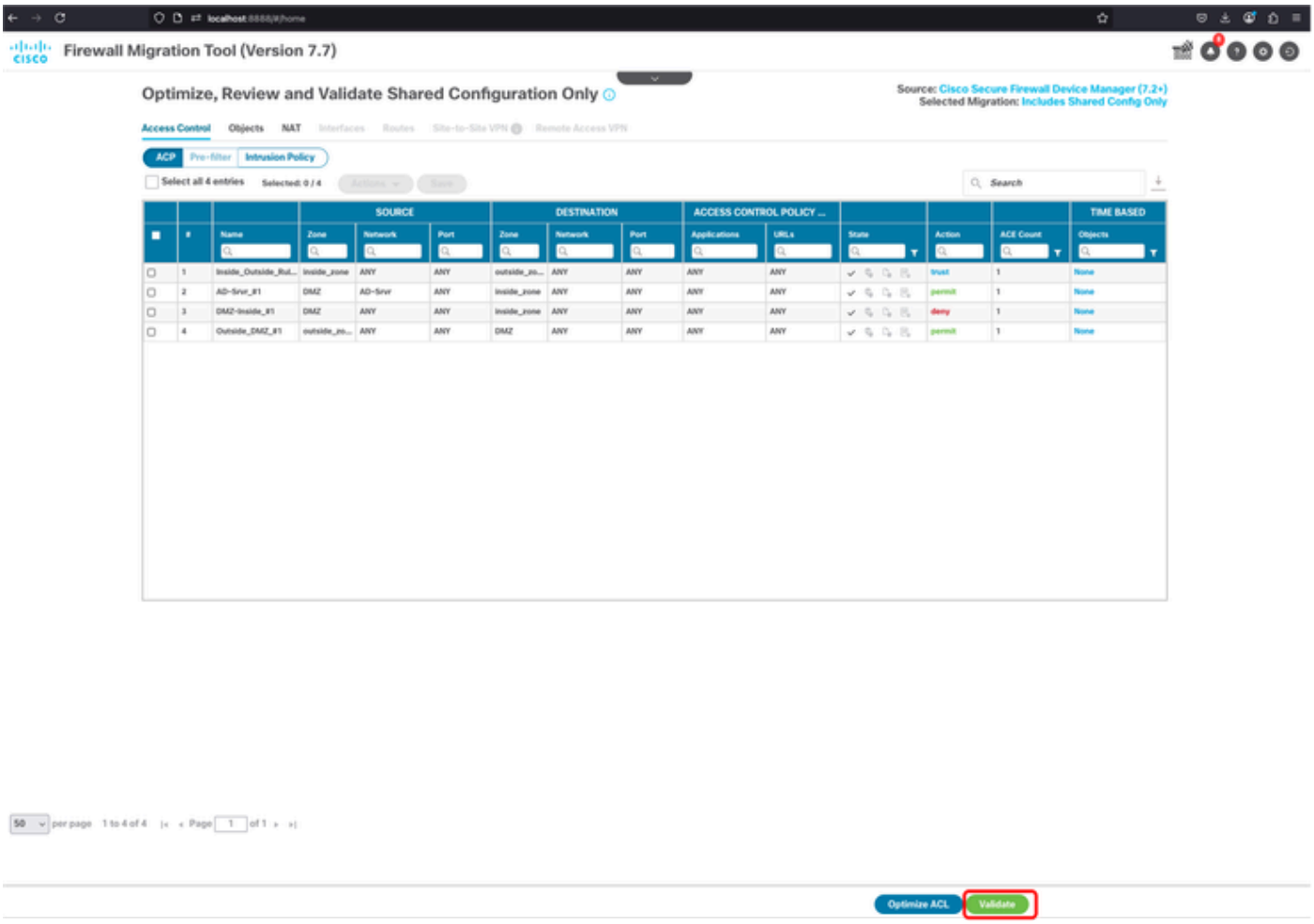
FMT - Création automatique de zones de sécurité et de groupes d'interfaces

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



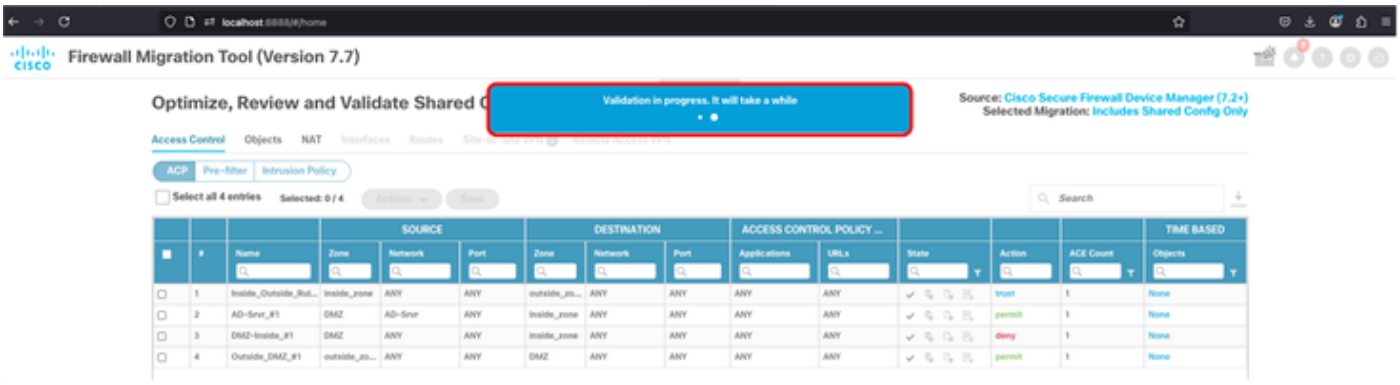
FMT - Création des zones de sécurité et des groupes d'interfaces réussie

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.



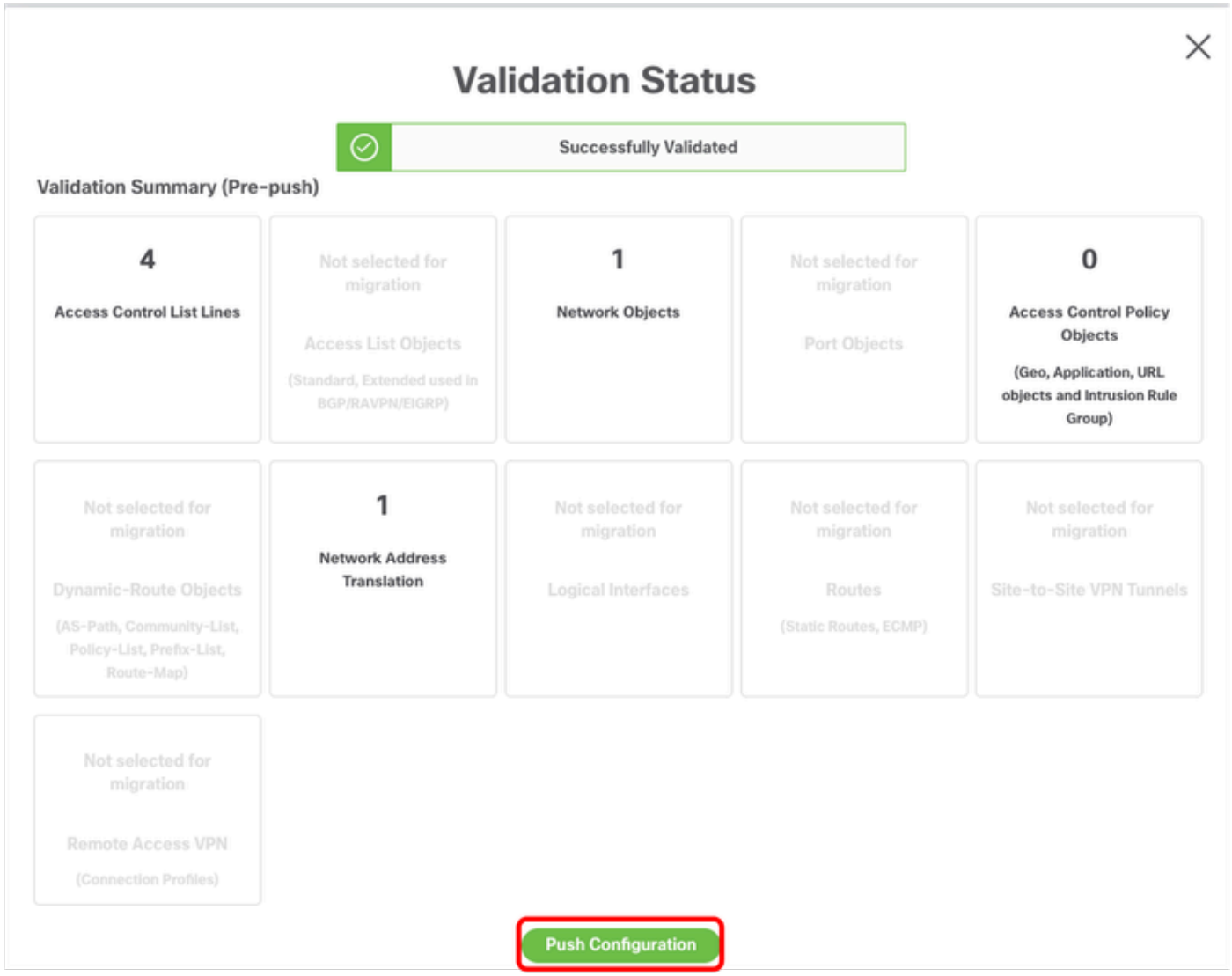
FMT - Optimiser ACL - Valider la migration

33. La validation ne prend que quelques minutes.



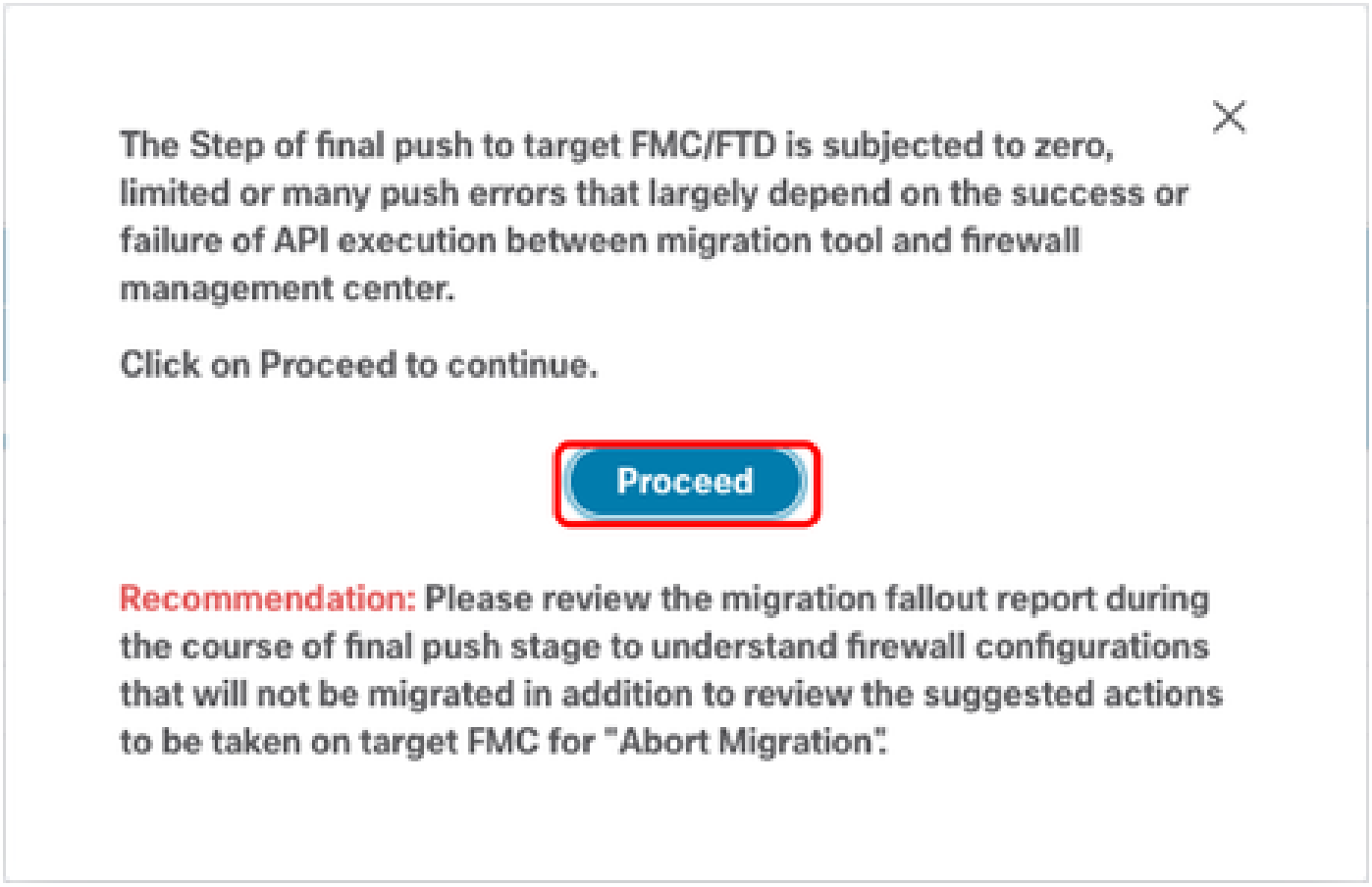
FMT - Validation en cours

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.



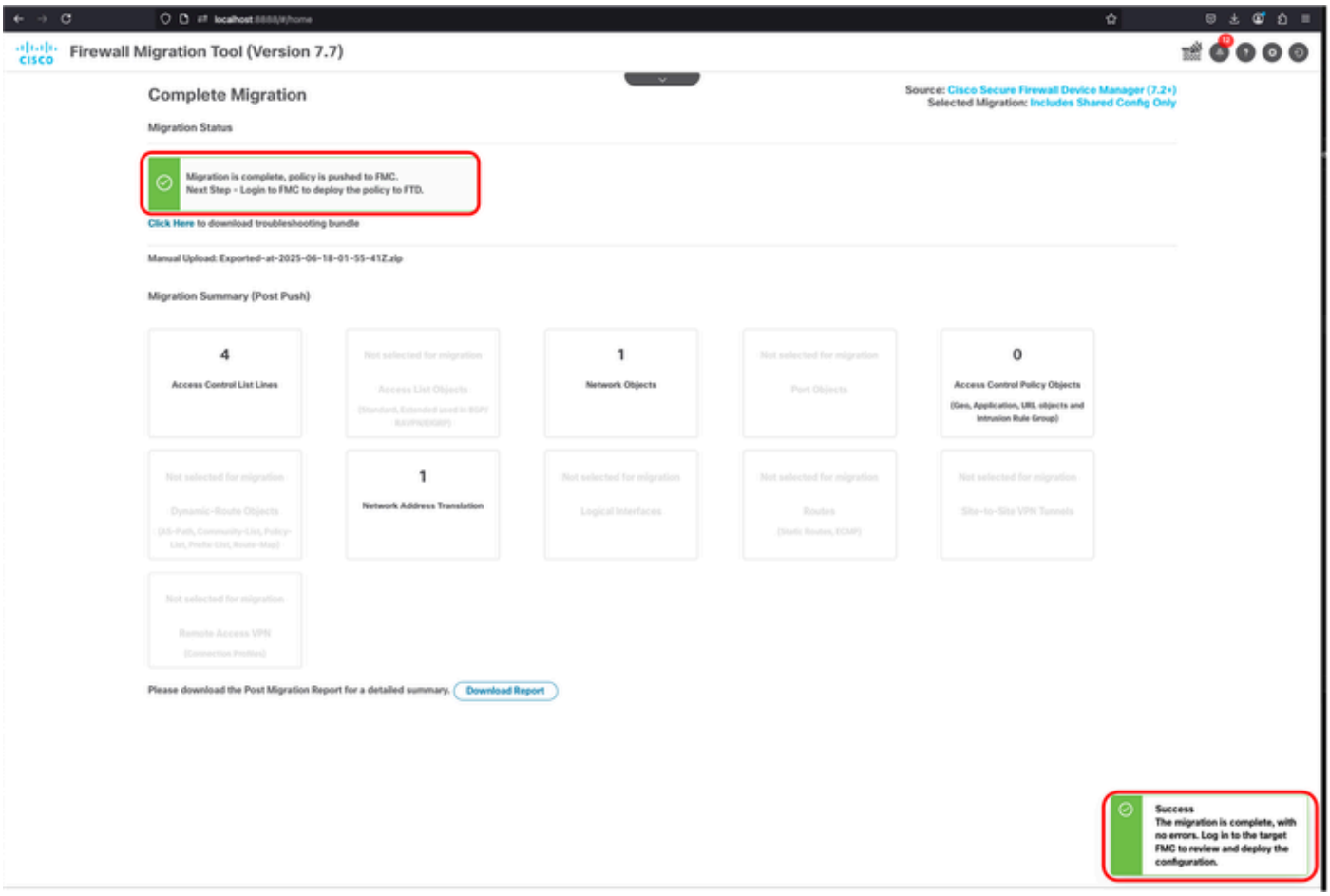
FMT - Validation réussie - Diffuser la configuration vers FMC

35. Enfin, cliquez sur le bouton Continuer.



FMT - Poursuivre la configuration push

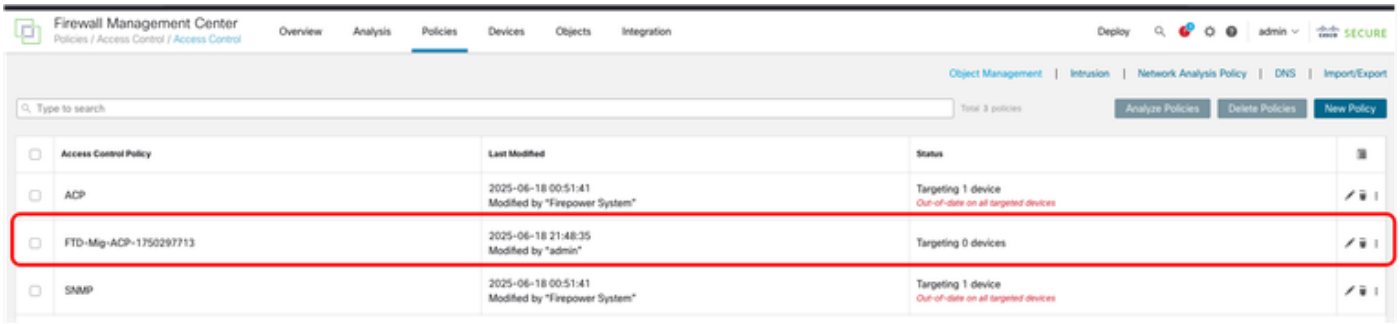
36. Si tout se passe comme prévu, la notification Migration réussie s'affiche. FMT vous demande de vous connecter à FMC et de déployer la stratégie migrée vers FTD.



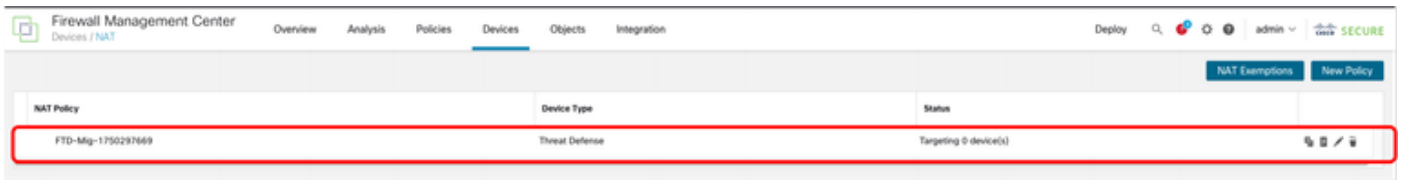
FMT - Notification de migration réussie

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.



FMC - ACP migré



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.