Migration d'un FTD d'un FMC vers un autre FMC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Configurer

- Configurations

Vérifier

Dépannage

Informations connexes

Introduction

Ce document décrit comment migrer un périphérique Cisco Firepower Threat Defense (FTD) entre les centres de gestion Firepower.

Conditions préalables

Avant de commencer le processus de migration, assurez-vous que les conditions suivantes sont réunies :

- Accès aux FMC source et de destination.
- Informations d'identification administratives pour FMC et FTD.
- Sauvegardez la configuration FMC actuelle.
- Assurez-vous que les périphériques FTD exécutent une version logicielle compatible avec le FMC de destination.
- Assurez-vous que le FMC de destination a la même version que le FMC source.

Exigences

- Les deux FMC doivent exécuter des versions logicielles compatibles.
- Connectivité réseau entre le périphérique FTD et les deux FMC.
- Stockage et ressources adéquats sur le FMC de destination pour accueillir le périphérique FTD.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

Cisco Firepower Threat Defense Virtual (FTDv) Version 7.2.5

Firepower Management Center Virtual (FMCv) Version 7.2.5

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

La migration d'un périphérique FTD d'un FMC à un autre implique plusieurs étapes, notamment la désinscription du périphérique du FMC source, la préparation du FMC de destination et la réinscription du périphérique. Ce processus garantit que toutes les stratégies et configurations sont correctement transférées et appliquées.

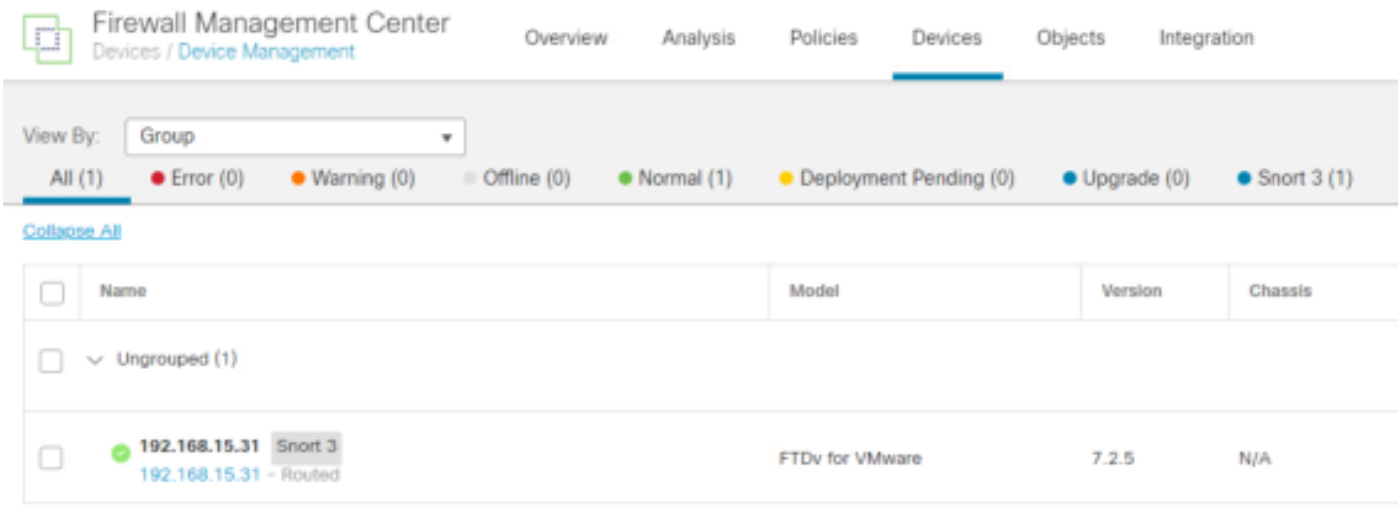
Configurer

Configurations

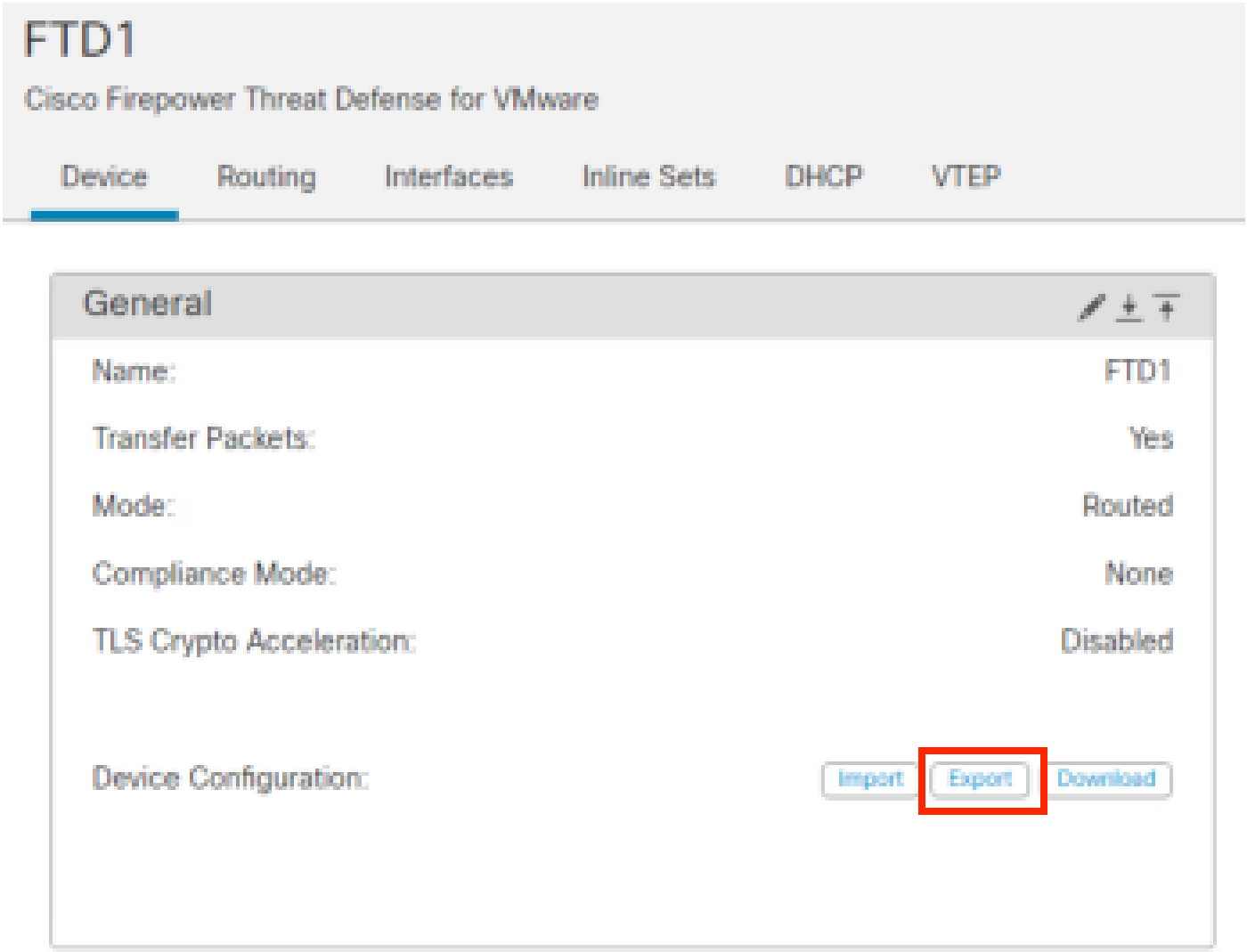
1. Connectez-vous au FMC source.



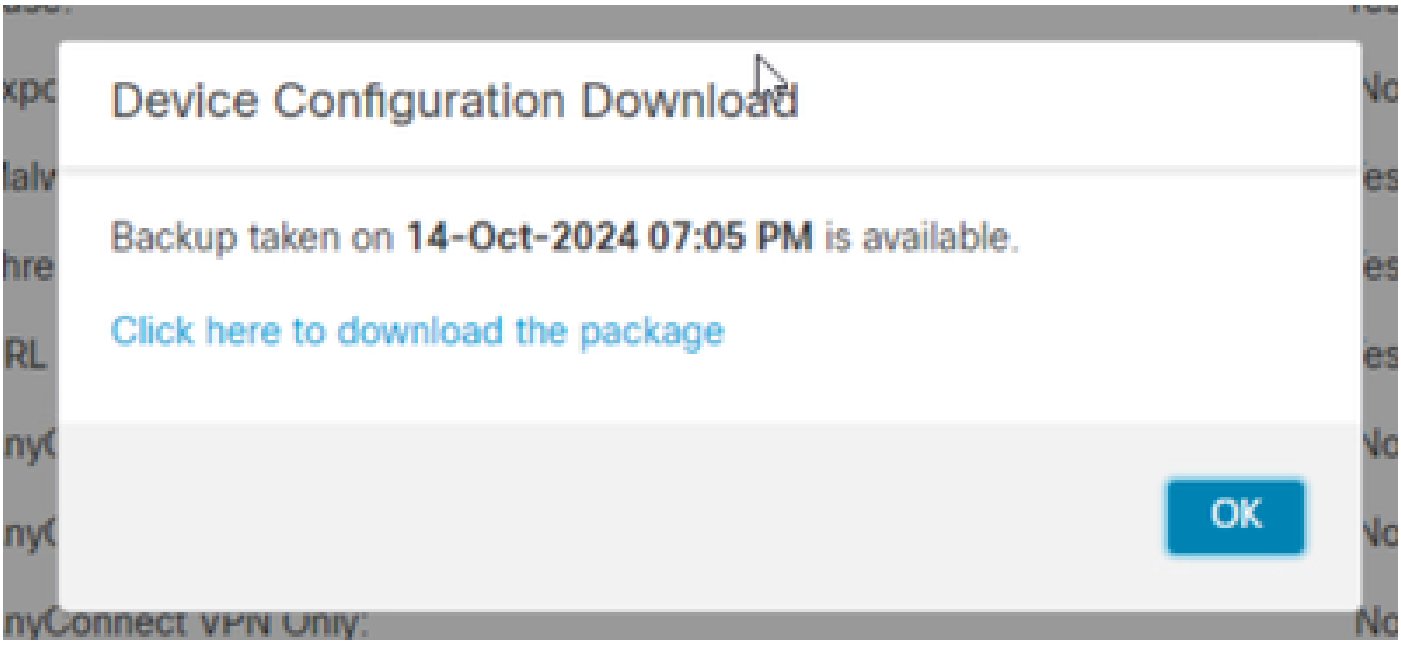
2. Accédez à Périphériques > Gestion des périphériques et sélectionnez le périphérique à migrer.

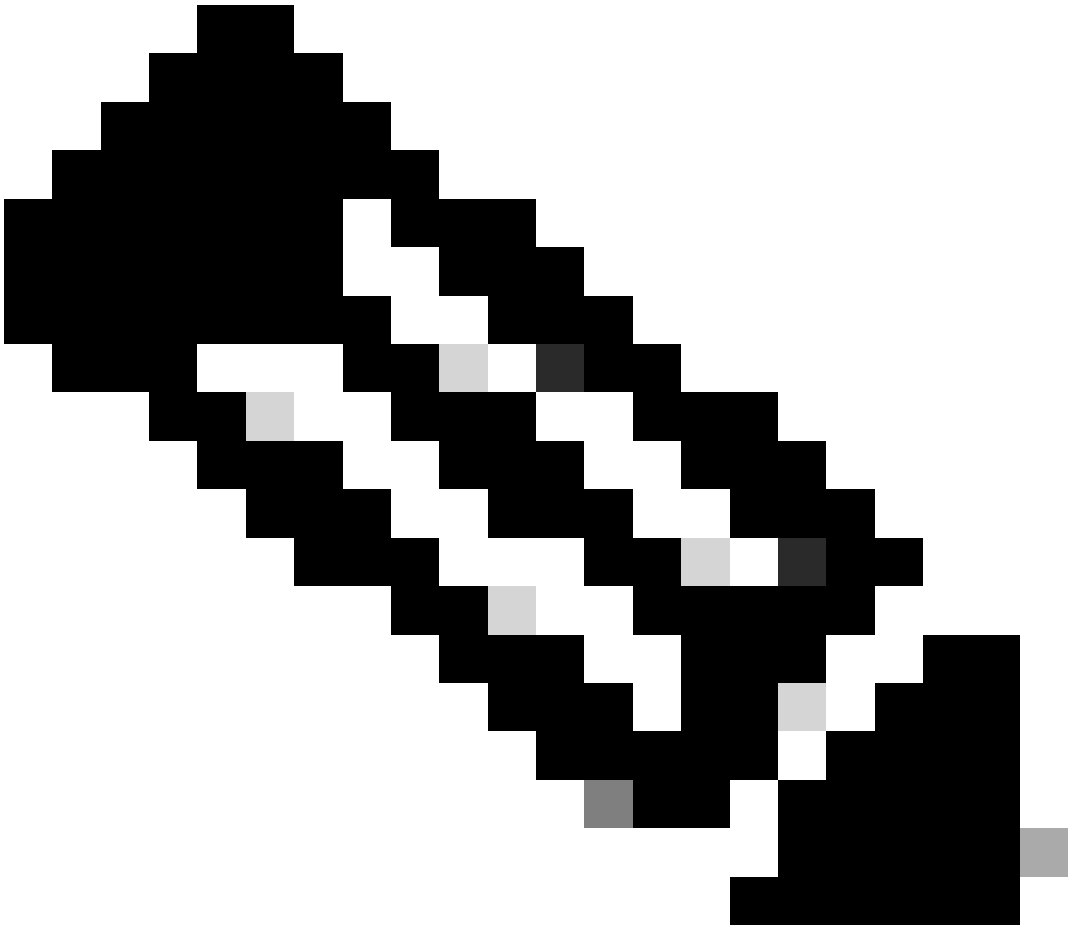


3. Dans la section périphérique, accédez à périphérique et cliquez sur exporter pour exporter vos paramètres de périphérique.



4. Une fois la configuration exportée, vous devez la télécharger.

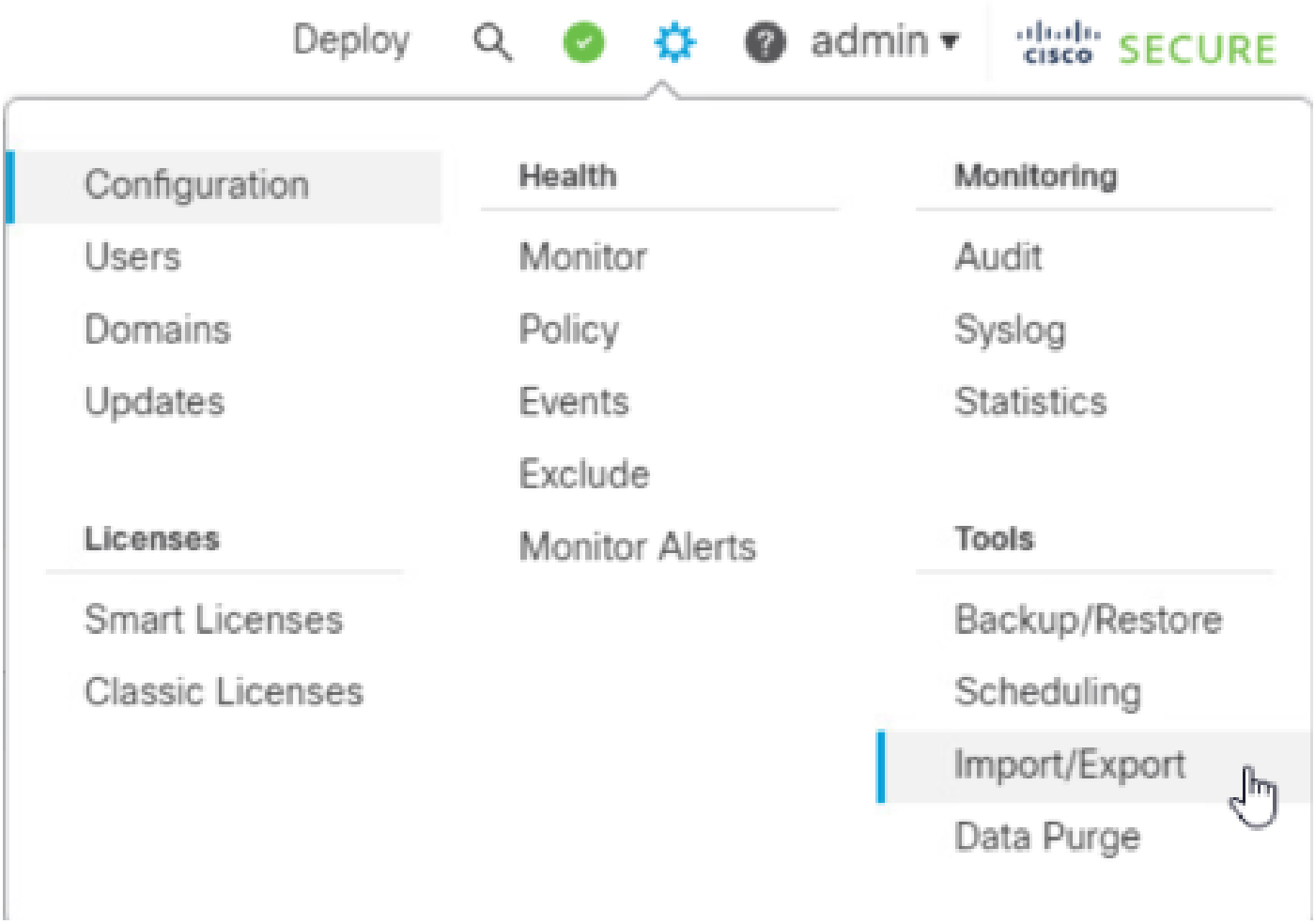


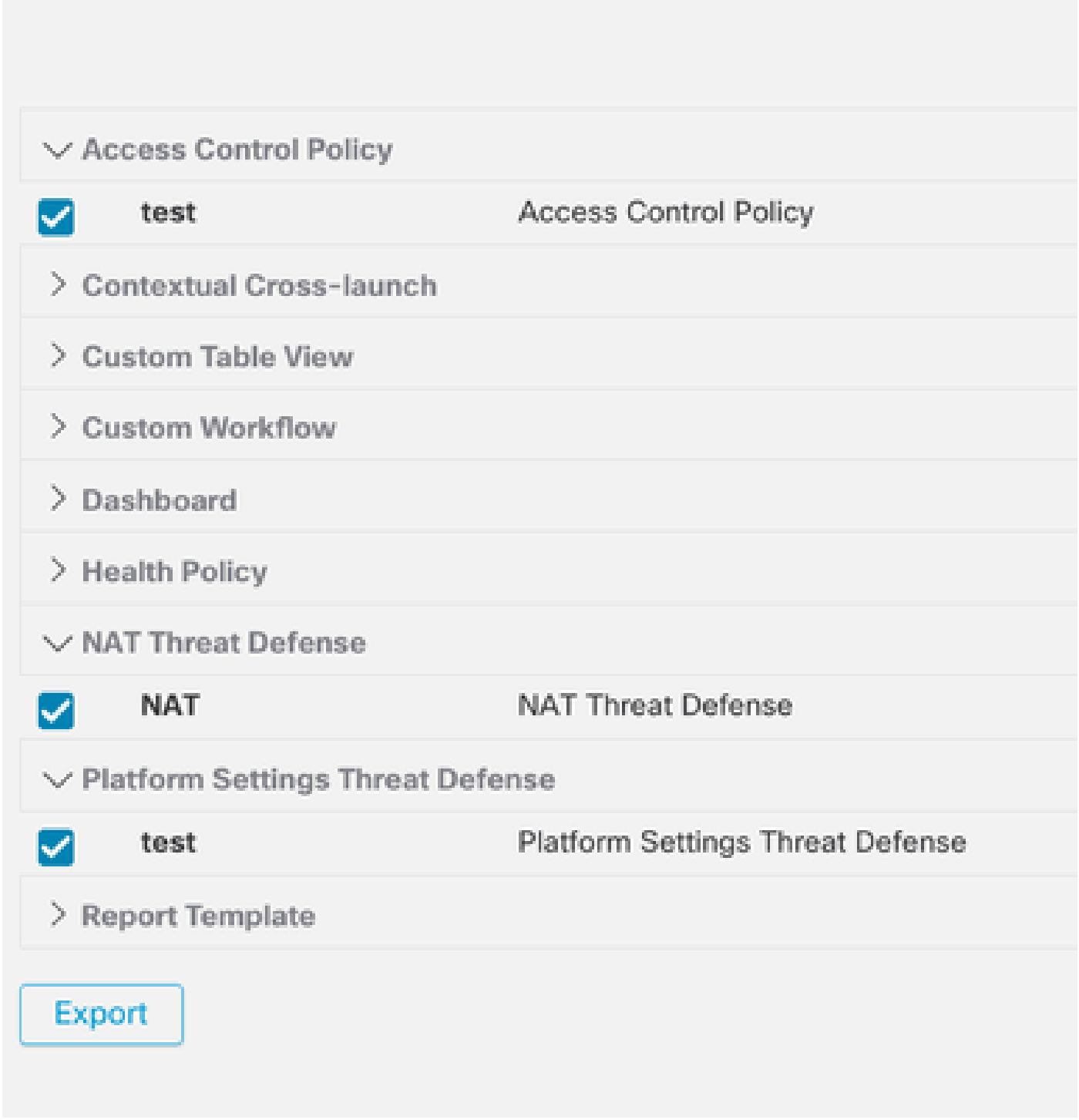


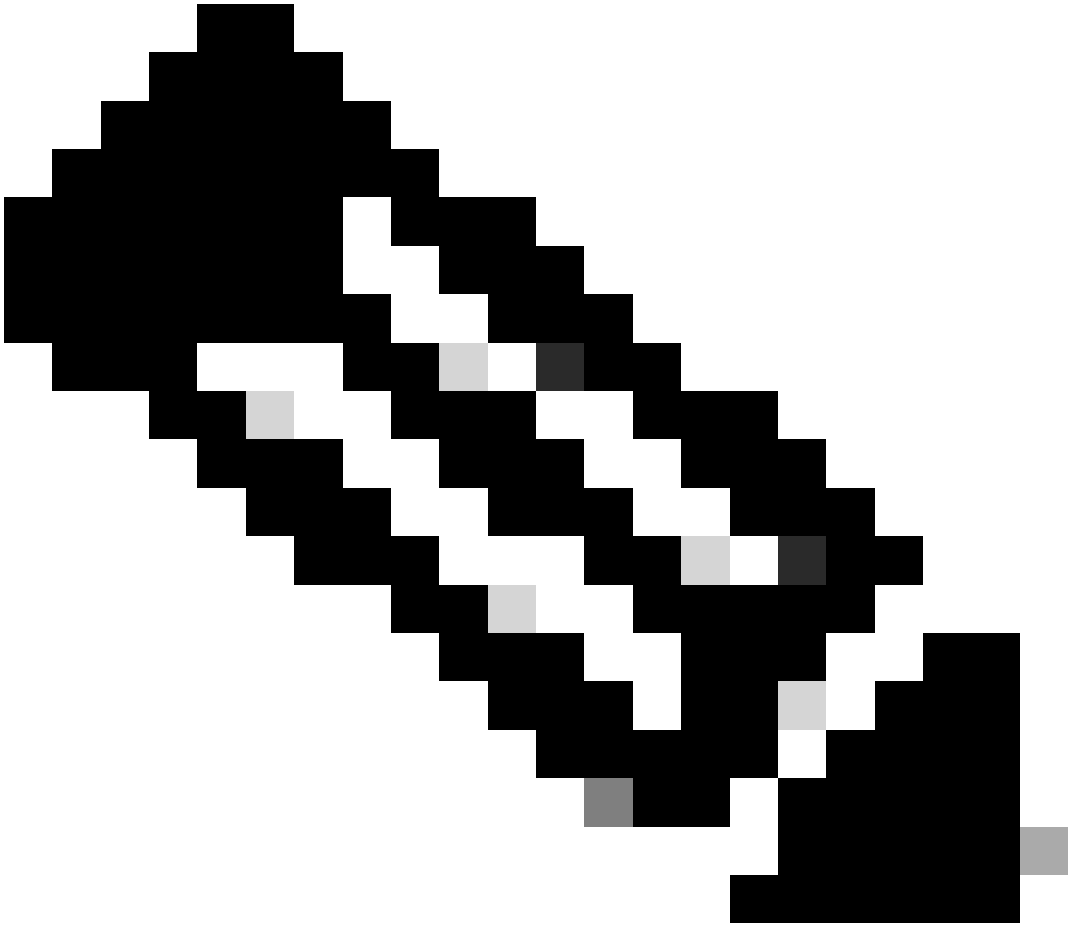
Remarque : le fichier téléchargé doit contenir l'extension .SFO et des informations de

configuration de périphérique telles que les adresses IP, les zones de sécurité, les routes statiques et d'autres paramètres de périphérique.

5. Vous devez exporter les stratégies associées au périphérique, accéder à Système > Outils > Importer/Exporter, sélectionner les stratégies que vous souhaitez exporter et cliquer sur exporter.



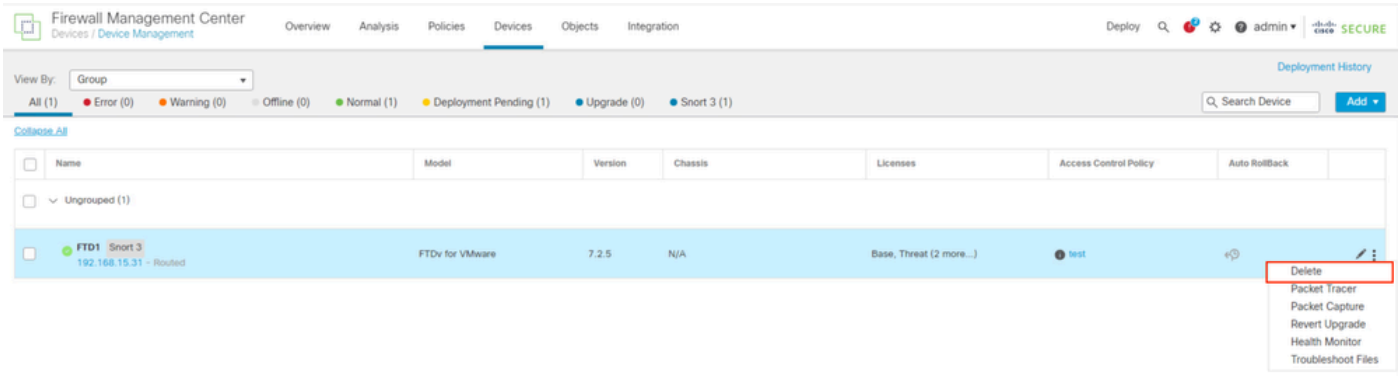

Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



Remarque : vérifiez que le fichier .SFO a bien été téléchargé. Le téléchargement est effectué automatiquement après avoir cliqué sur export. Ce fichier contient les politiques de contrôle d'accès, les paramètres de plate-forme, les politiques NAT et d'autres politiques qui sont indispensables pour la migration car elles ne sont pas exportées avec la configuration du périphérique et doivent être téléchargées manuellement vers le FMC de destination.

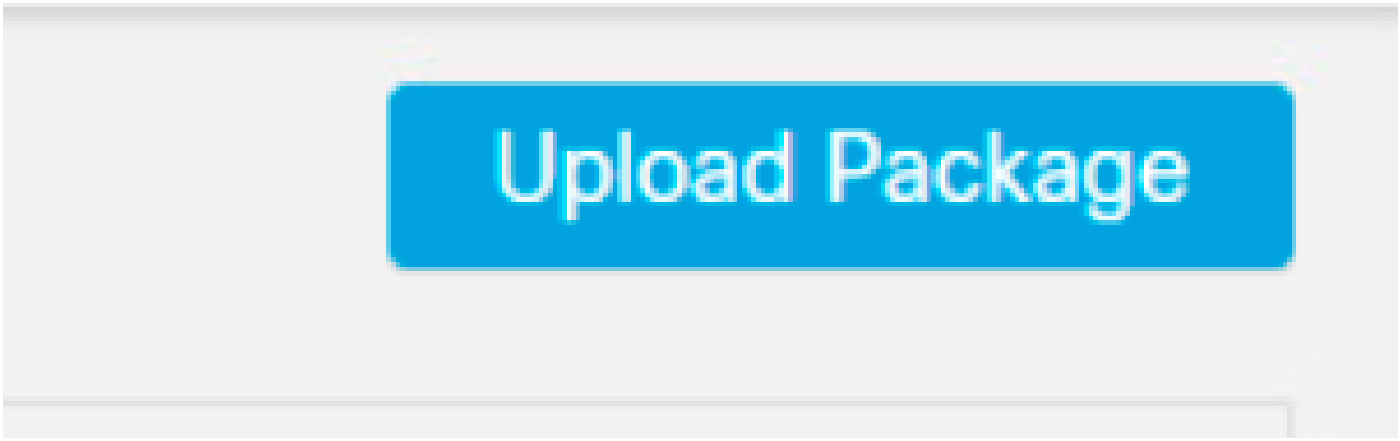
---

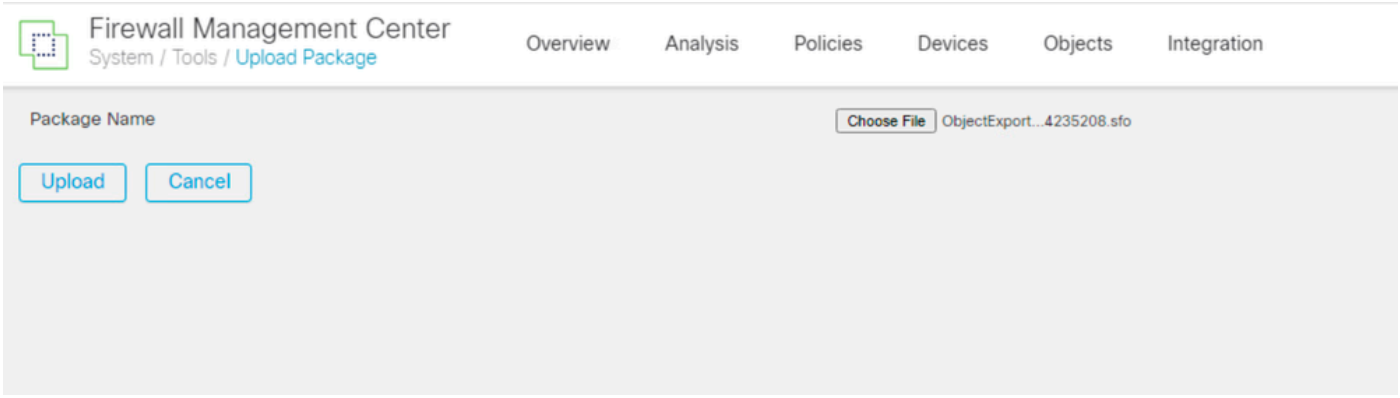
6. Annulez l'enregistrement du périphérique FTD du FMC, accédez à Périphériques > Gestion des périphériques, cliquez sur les trois points verticaux sur le côté droit et sélectionnez supprimer.



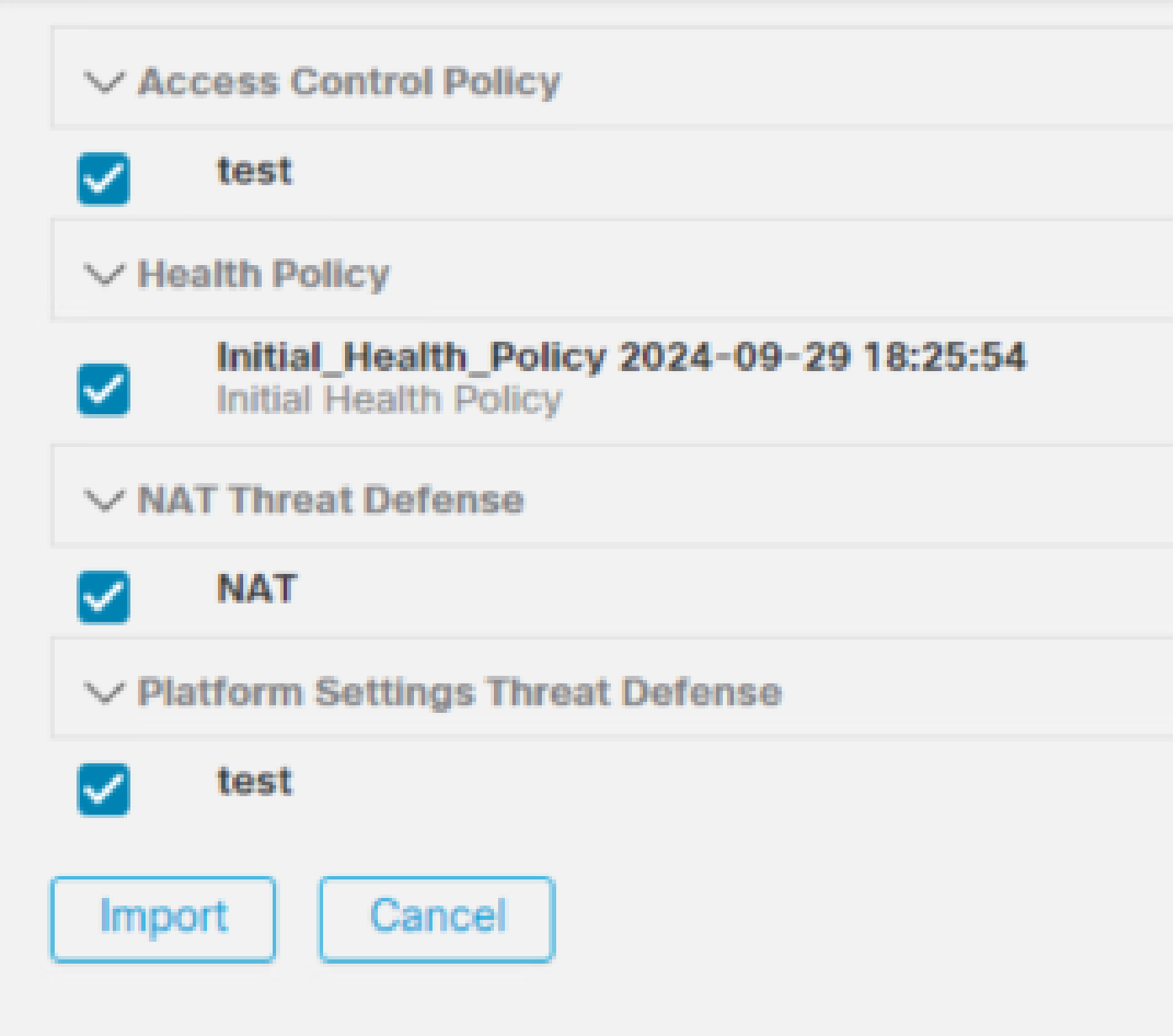
7. Préparez le FMC de destination :

- Connectez-vous au FMC de destination.
- Assurez-vous que le FMC est prêt à accepter le nouveau périphérique en important les stratégies FMC source que vous avez téléchargées à l'étape 5. Accédez à System > Tools > Import/Export et cliquez sur upload package. Téléchargez le fichier à importer et cliquez sur Télécharger.

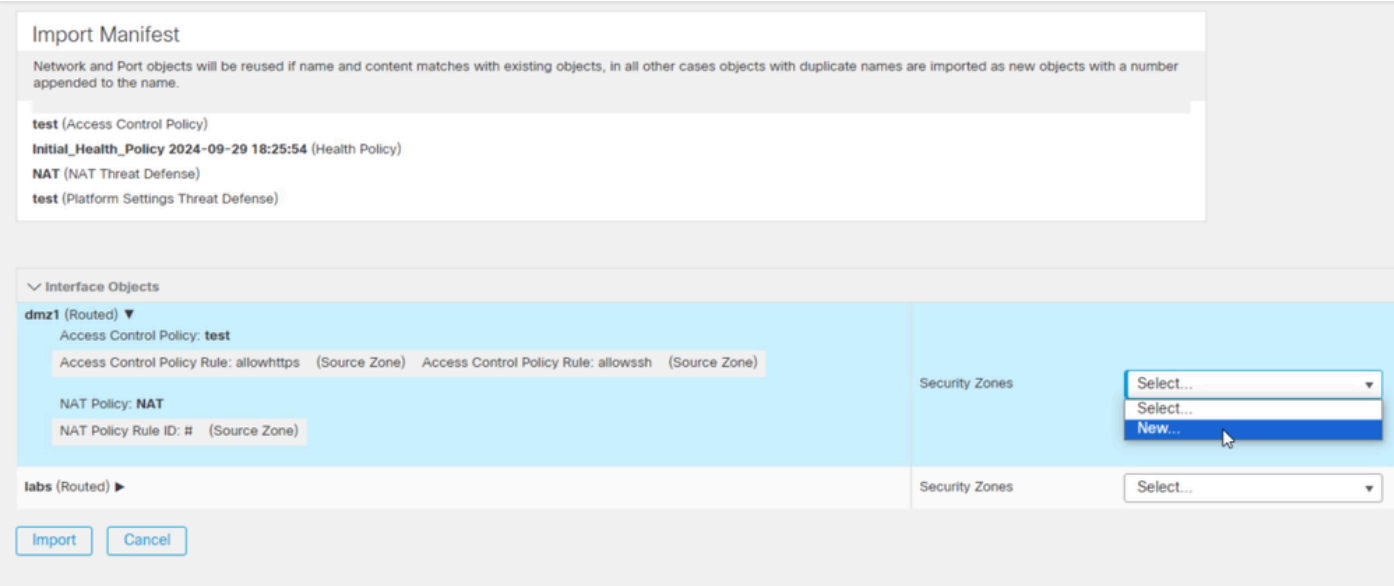




8. Sélectionnez les stratégies à importer dans le FMC de destination.

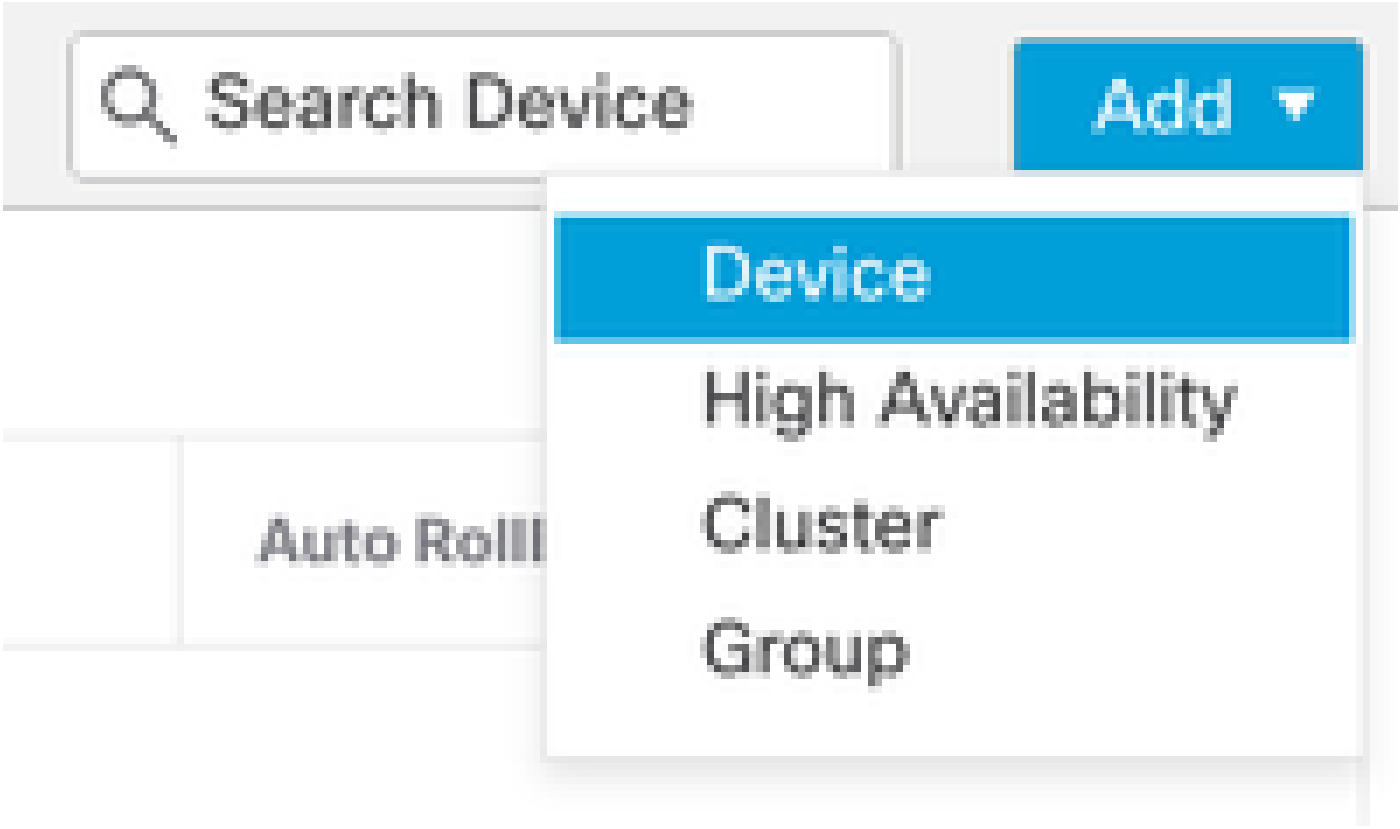


9. Dans le manifeste d'importation, sélectionnez une zone de sécurité ou créez-en une nouvelle à affecter à l'objet interface et cliquez sur importer.



10. Enregistrez le FTD sur le FMC de destination :

- Sur le FMC de destination, accédez à Device > Management tab et sélectionnez Add > Device.
- Suivez la procédure d'inscription en répondant aux invites.



Add Device

CDO Managed Device

Host:†

Display Name:

Registration Key:*

Group:

None

Access Control Policy:*

Smart Licensing

Note: All virtual Firewall Threat Defense devices require a performance tier license.
Make sure your Smart Licensing account contains the available licenses you need.
It's important to choose the tier that matches the license you have in your account.
Click here for information about the Firewall Threat Defense performance-tiered licensing.
Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Select a recommended Tier

Malware

Threat

URL Filtering

Advanced

Unique NAT ID:†

Transfer Packets

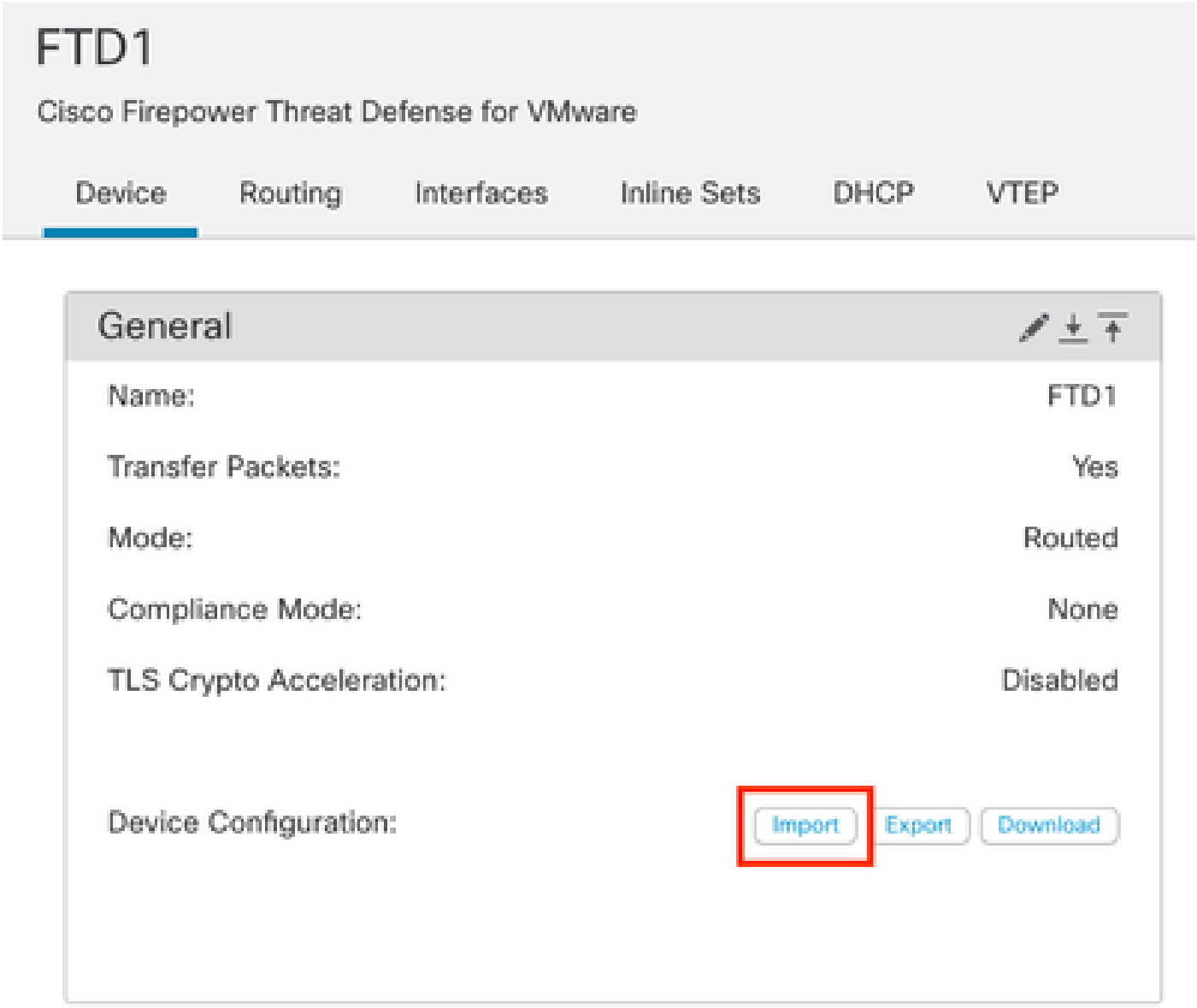
† Either host or NAT ID is required.

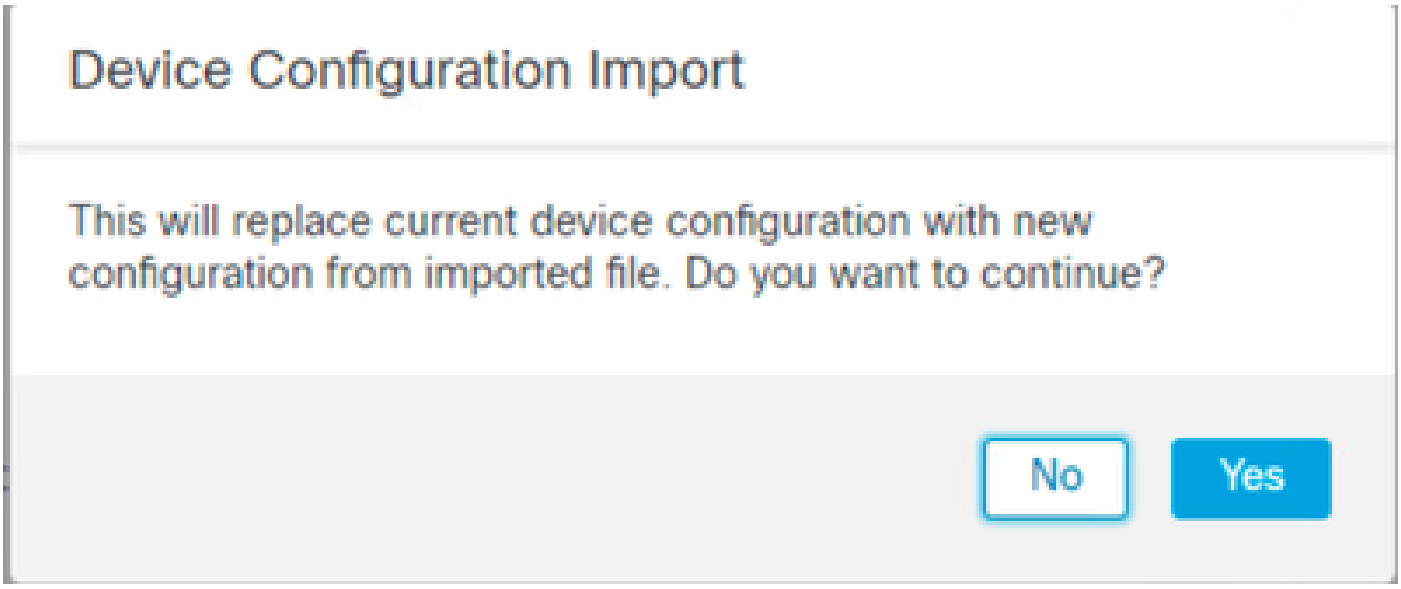
Cancel

Register

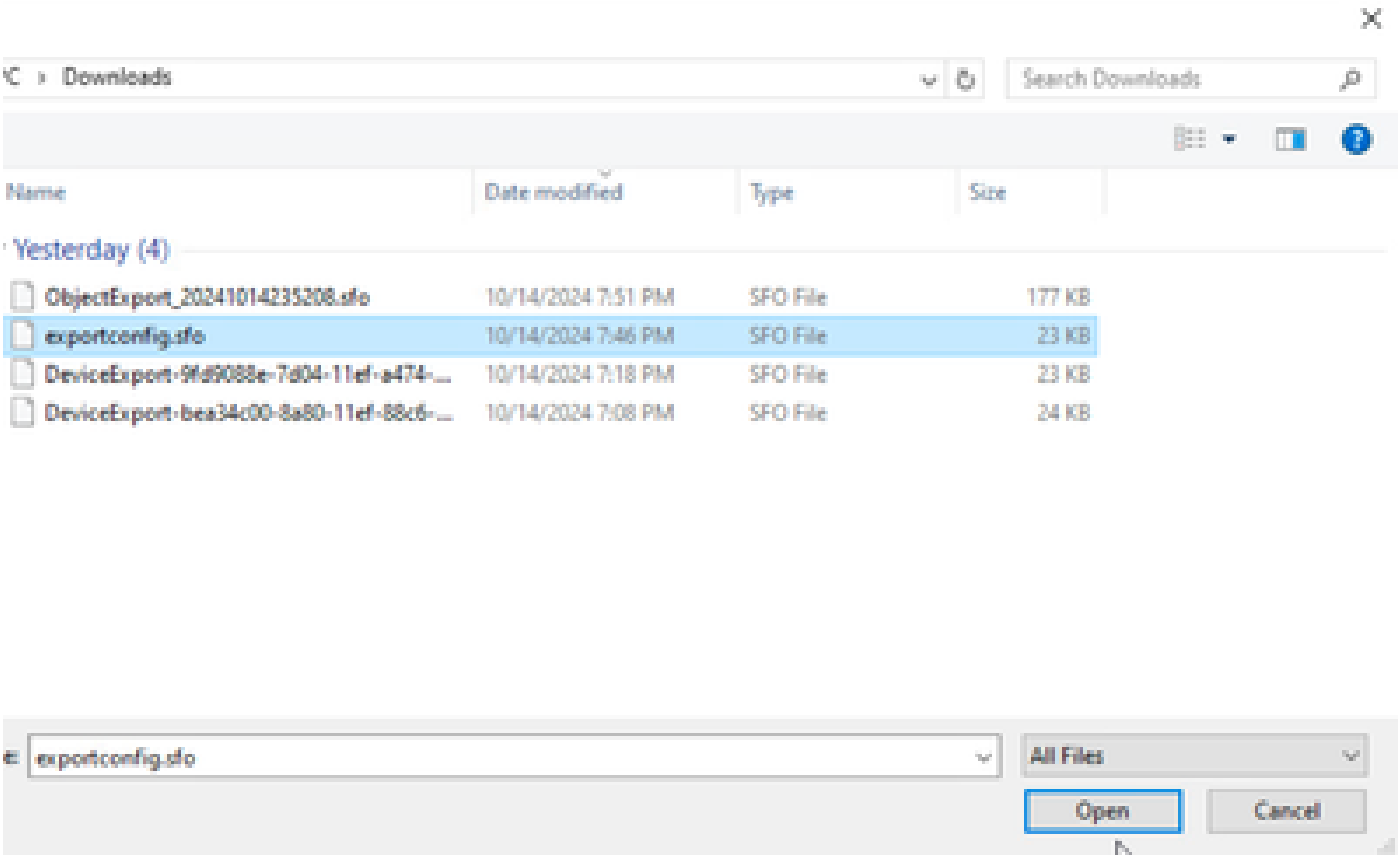
Pour plus d'informations, consultez le Guide de configuration de Firepower Management Center, [Ajouter des périphériques à Firepower Management Center]

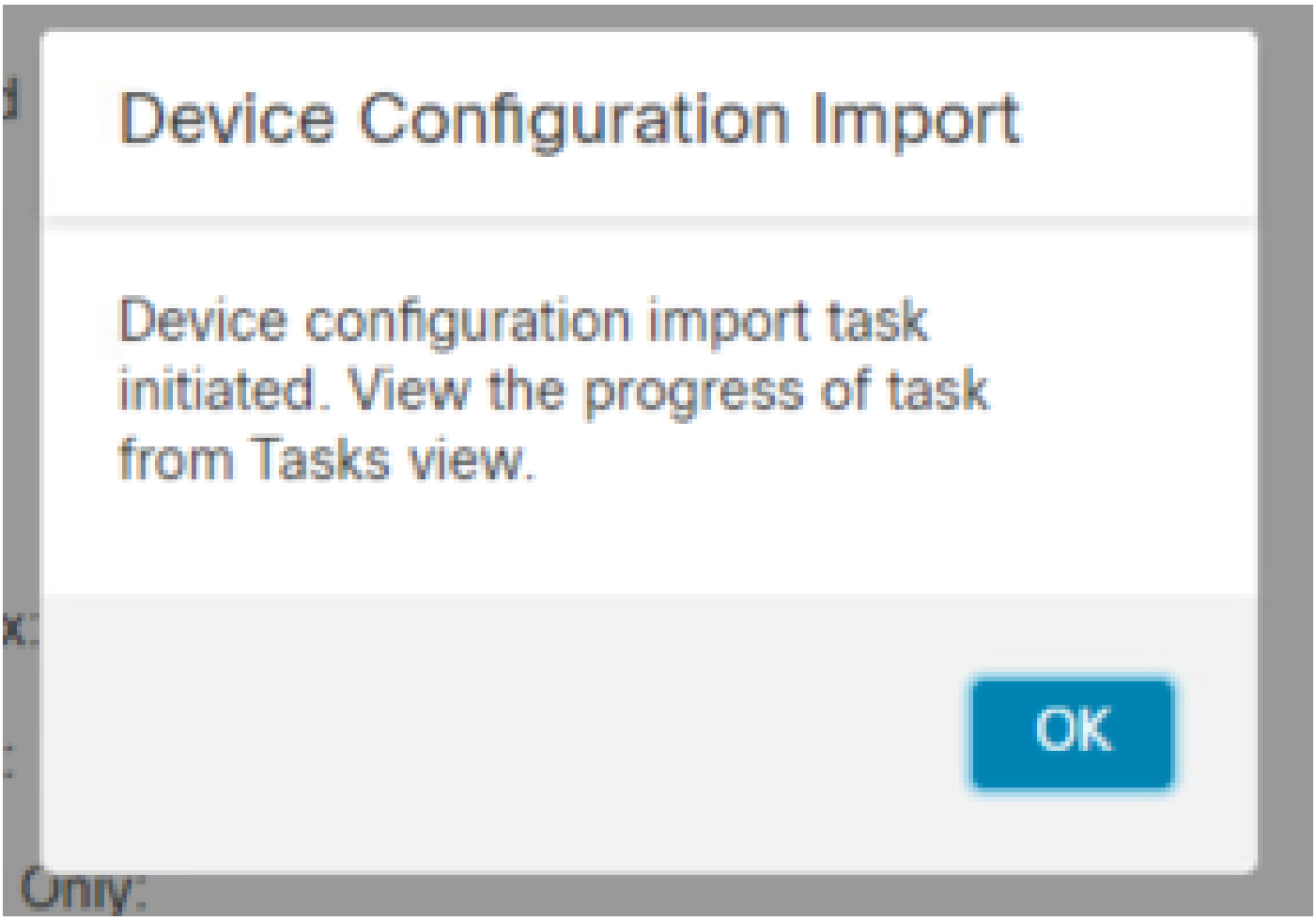
11. Accédez à Device > Device Management > sélectionnez le FTD > Device et cliquez sur import. Un avertissement vous demande de confirmer le remplacement de la configuration du périphérique. Cliquez sur yes.



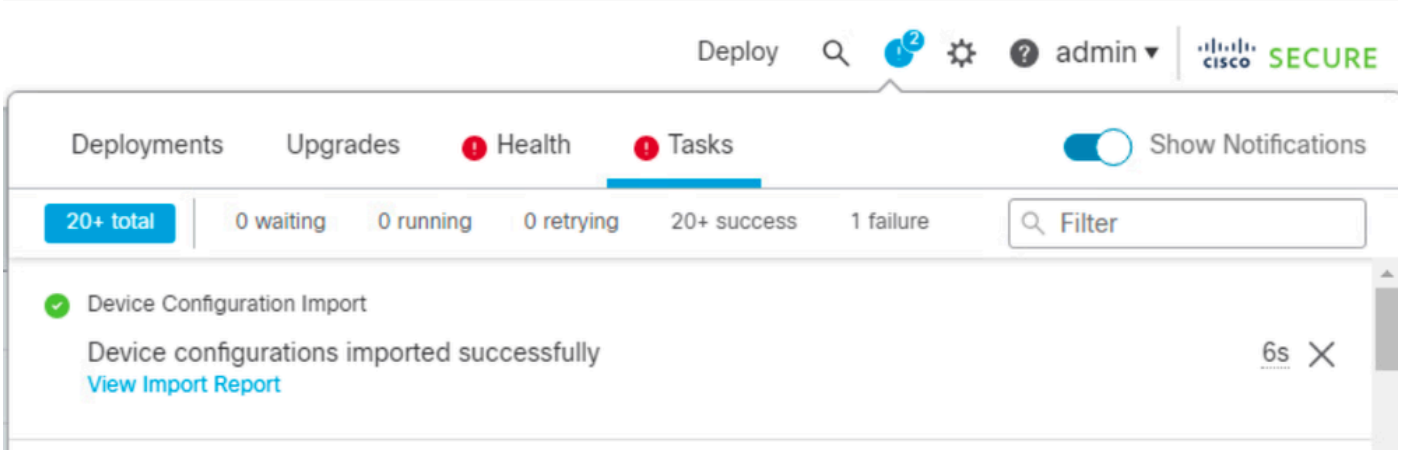


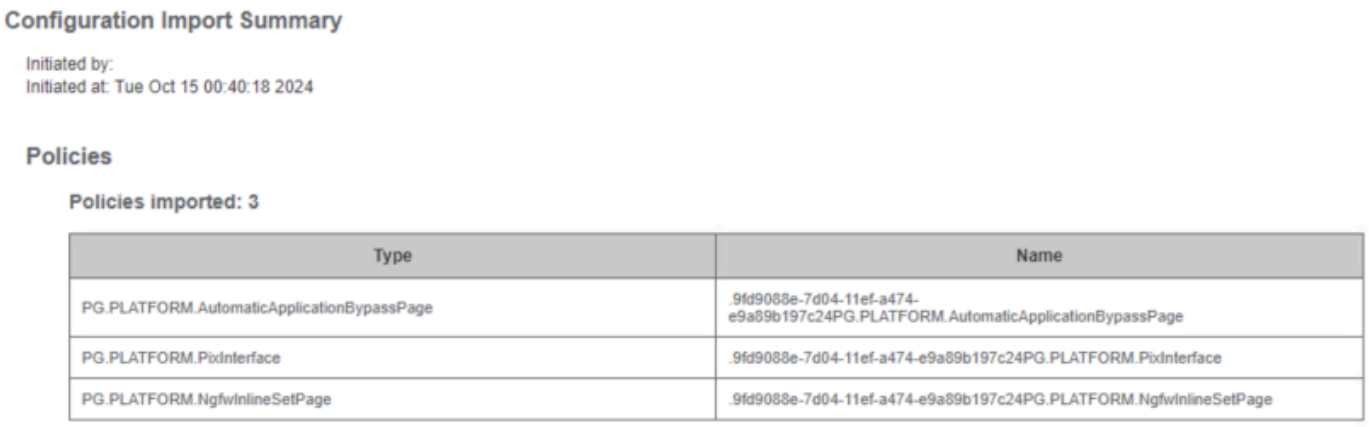
12. Sélectionnez le fichier de configuration d'importation qui doit avoir l'extension .SFO, cliquez sur upload, et un message s'affiche indiquant que l'importation a commencé.





13. Enfin, une alerte s'affiche et un rapport est généré automatiquement à la fin de l'importation, ce qui vous permet de consulter les objets et les règles qui ont été importés.





Configuration Import Summary

Initiated by:
Initiated at: Tue Oct 15 00:40:18 2024

Policies

Policies imported: 3

Type	Name
PG.PLATFORM.AutomaticApplicationBypassPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.AutomaticApplicationBypassPage
PG.PLATFORM.PixInterface	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.PixInterface
PG.PLATFORM.NgfwInlineSetPage	.9fd9088e-7d04-11ef-a474-e9a89b197c24PG.PLATFORM.NgfwInlineSetPage

Vérifier

Une fois la migration terminée, vérifiez que le périphérique FTD est correctement enregistré et fonctionne avec le FMC de destination :

- Vérifiez l'état du périphérique sur le FMC de destination.
- Assurez-vous que toutes les stratégies et configurations sont correctement appliquées.
- Effectuez un test pour confirmer que le périphérique est opérationnel.

Dépannage

Si vous rencontrez des problèmes au cours du processus de migration, tenez compte des étapes de dépannage suivantes :

- Vérifiez la connectivité réseau entre le périphérique FTD et les deux FMC.
- Assurez-vous que la version du logiciel est identique sur les deux FMC.
- Recherchez les messages d'erreur ou les avertissements dans les alertes des deux FMC.

Informations connexes

- Guide d'administration de Cisco Secure Firewall Management Center
- Configuration, vérification et dépannage de l'enregistrement des périphériques Firepower

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.

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.