あるFMCから別のFMCへのFTDの移行

内容

はじめに

このドキュメントでは、Firepower Management Center(FMC)間でCisco Firepower Threat Defense(FTD)デバイスを移行する方法について説明します。

前提条件

移行プロセスを開始する前に、次の前提条件を満たしていることを確認してください。

- 送信元と宛先の両方のFMCにアクセスできます。
- FMCとFTDの両方の管理者クレデンシャル
- 現在のFMC設定をバックアップします。
- 宛先FMCと互換性のあるソフトウェアバージョンを実行しているFTDデバイスを確認します。
- 宛先FMCと送信元FMCのバージョンが同じであることを確認します。

要件

- 両方のFMCで互換性のあるソフトウェアバージョンが実行されている必要があります。
- FTDデバイスと両方のFMC間のネットワーク接続。
- FTDデバイスに対応するために、宛先FMC上に十分なストレージとリソースがあること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

Cisco Firepower Threat Defense(FTDv)仮想バージョン7.2.5

Firepower Management Center(FMCv)仮想バージョン7.2.5

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

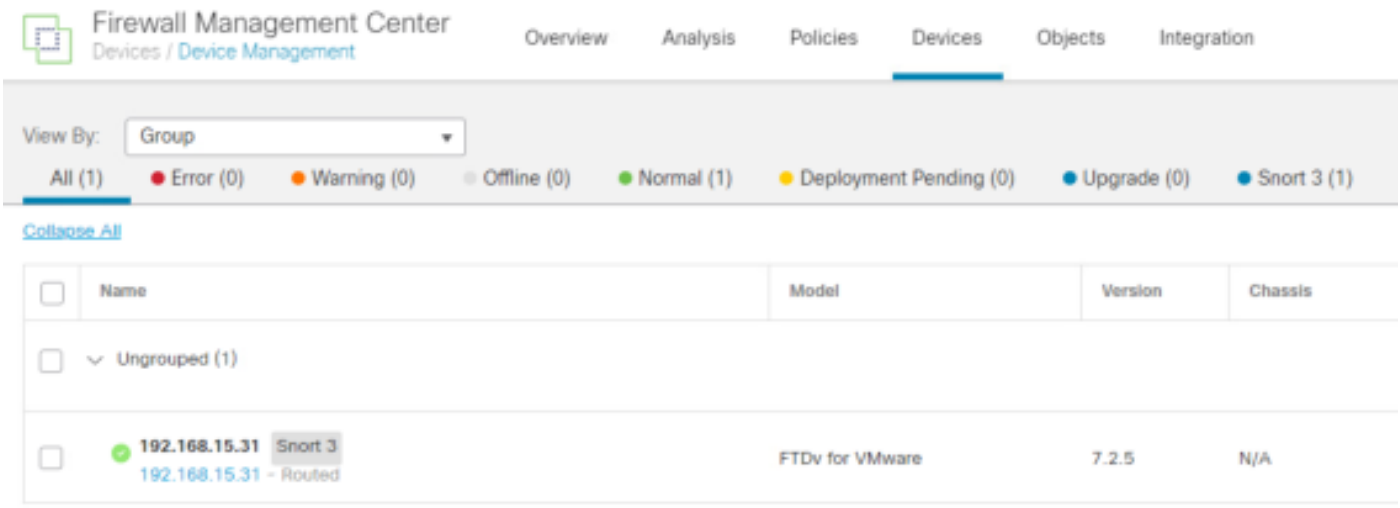
あるFMCから別のFMCにFTDデバイスを移行するには、ソースFMCからのデバイスの登録解除、宛先FMCの準備、デバイスの再登録など、いくつかの手順を実行する必要があります。このプロセスにより、すべてのポリシーと設定が正しく転送および適用されます。

設定

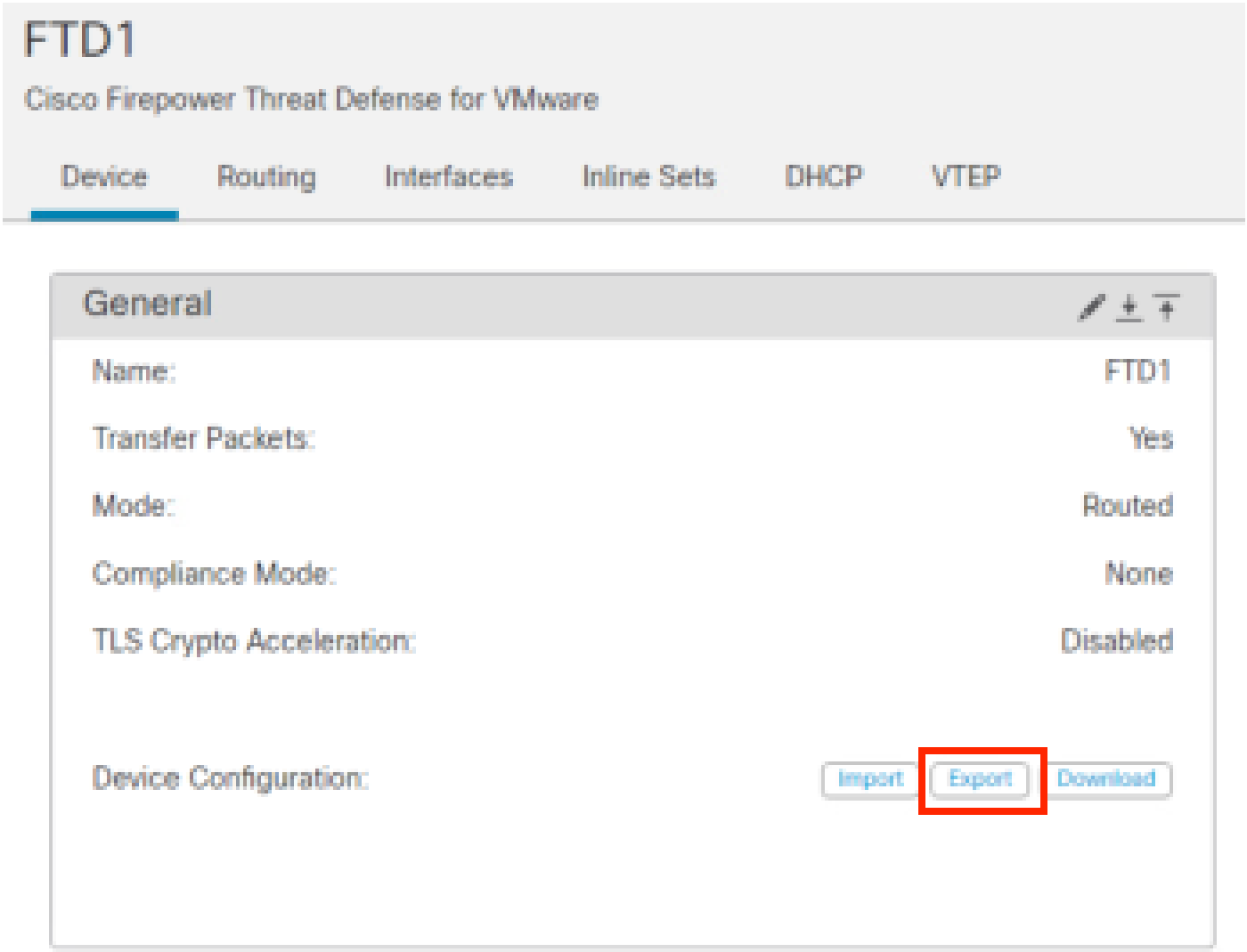
コンフィギュレーション

1. ソースFMCにログインします。

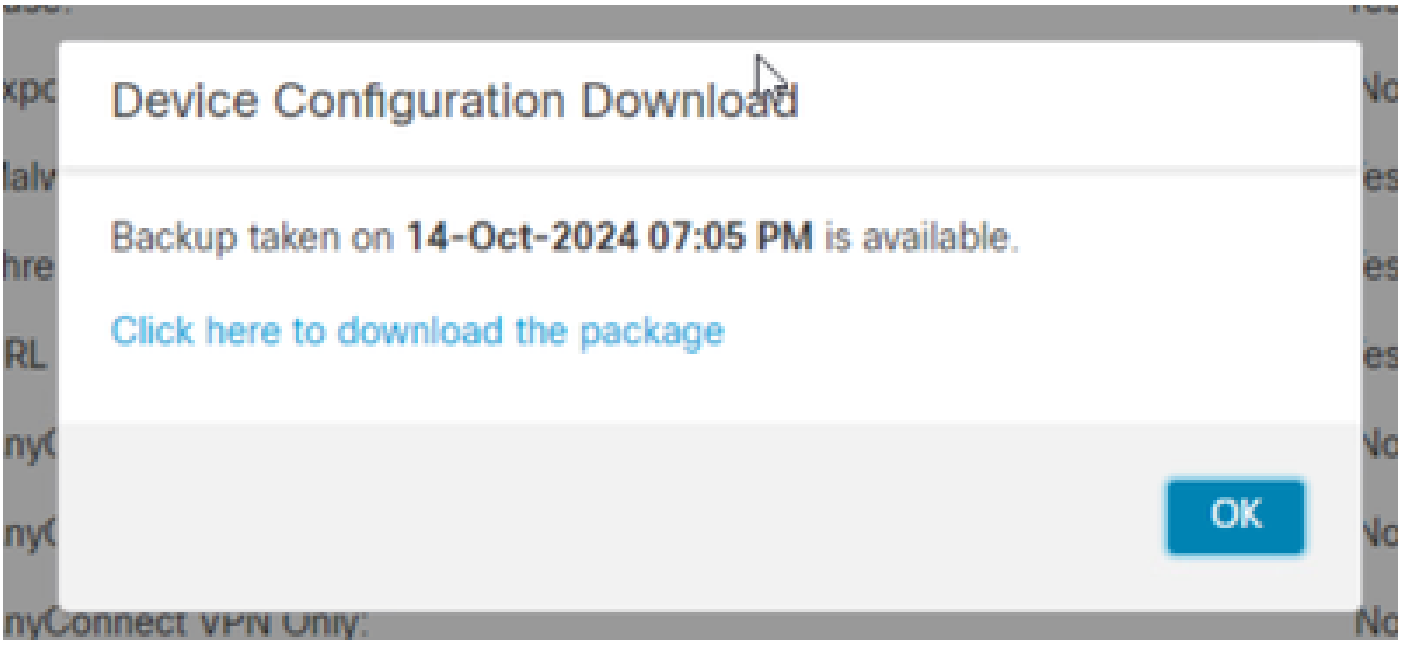
2. Devices > Device Managementの順に移動し、移行するデバイスを選択します。

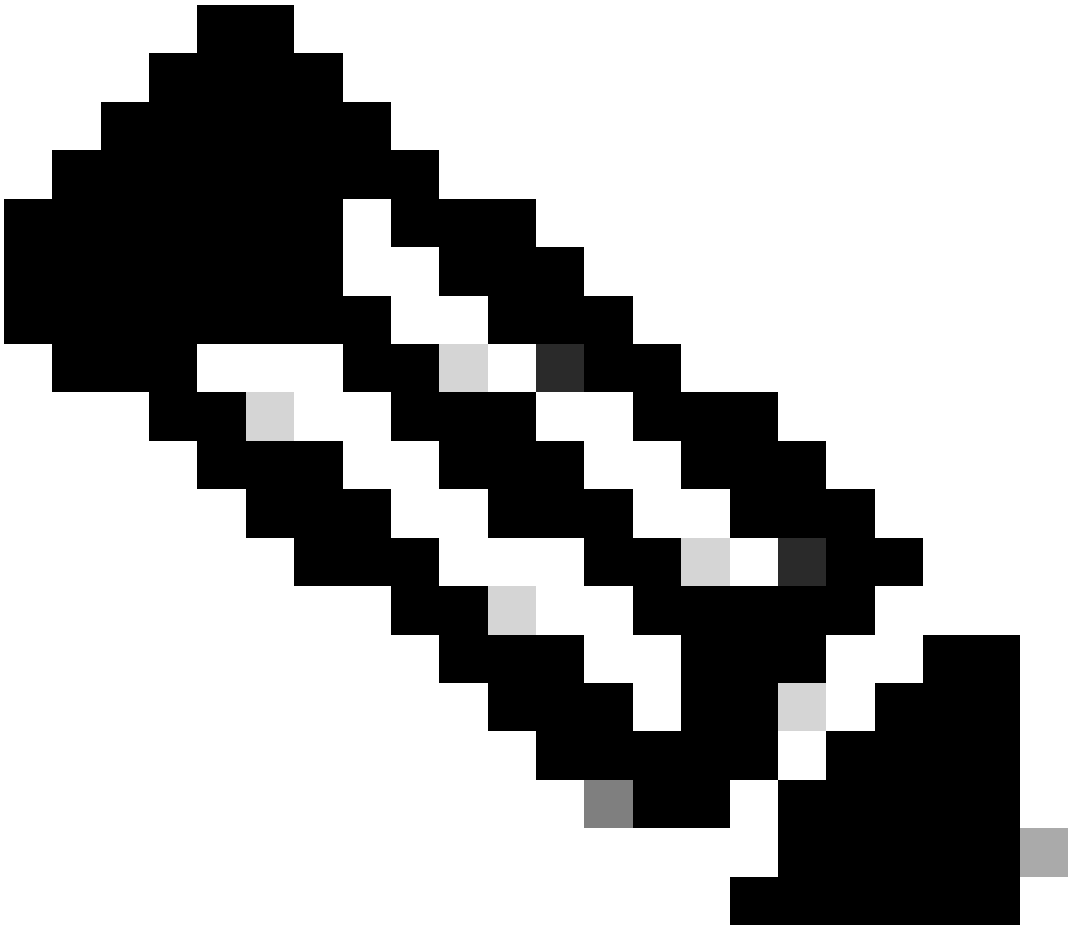


3. デバイスセクションで、デバイスに移動し、エクスポートをクリックしてデバイス設定をエクスポートします。



4. 設定をエクスポートしたら、ダウンロードする必要があります。

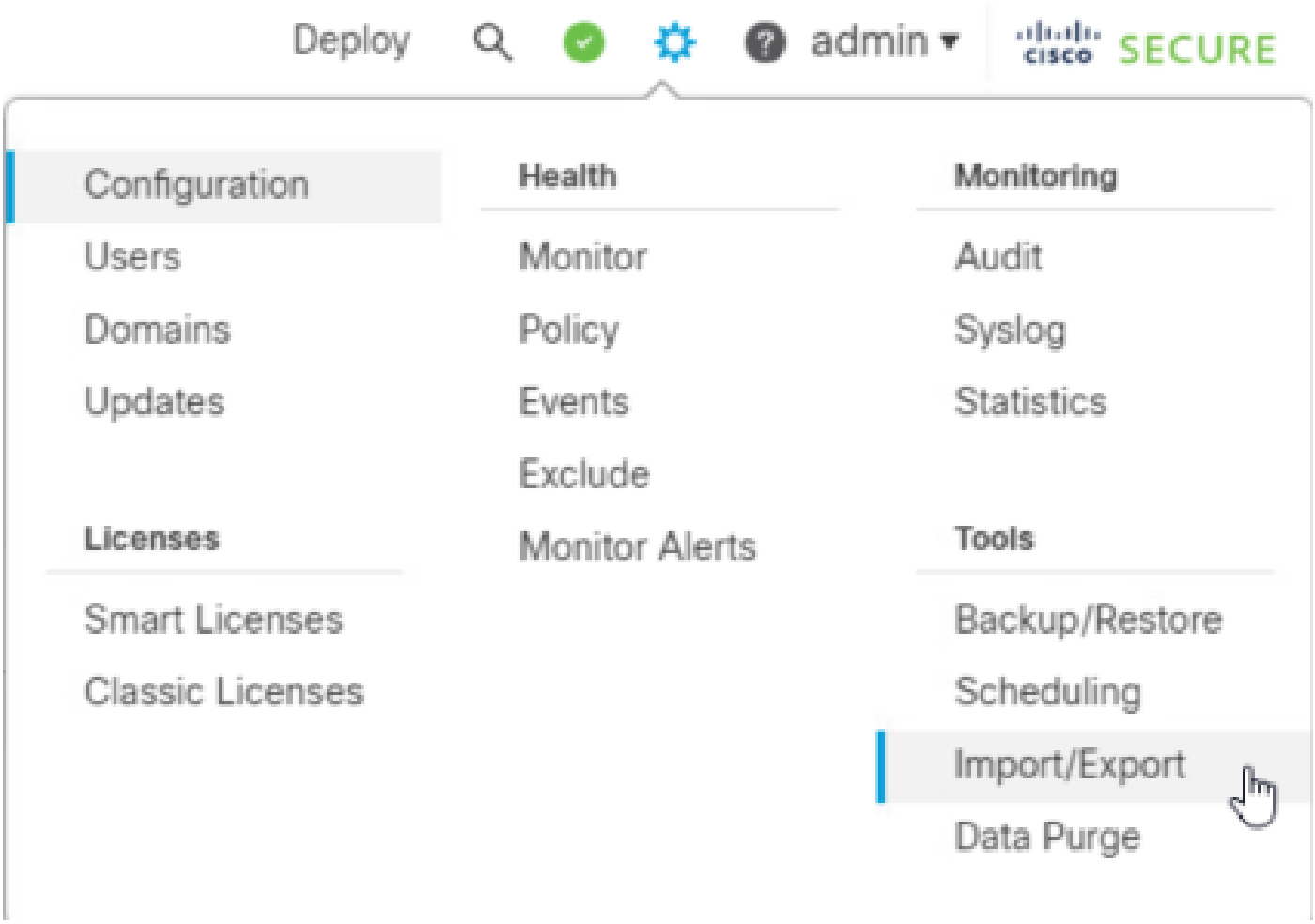


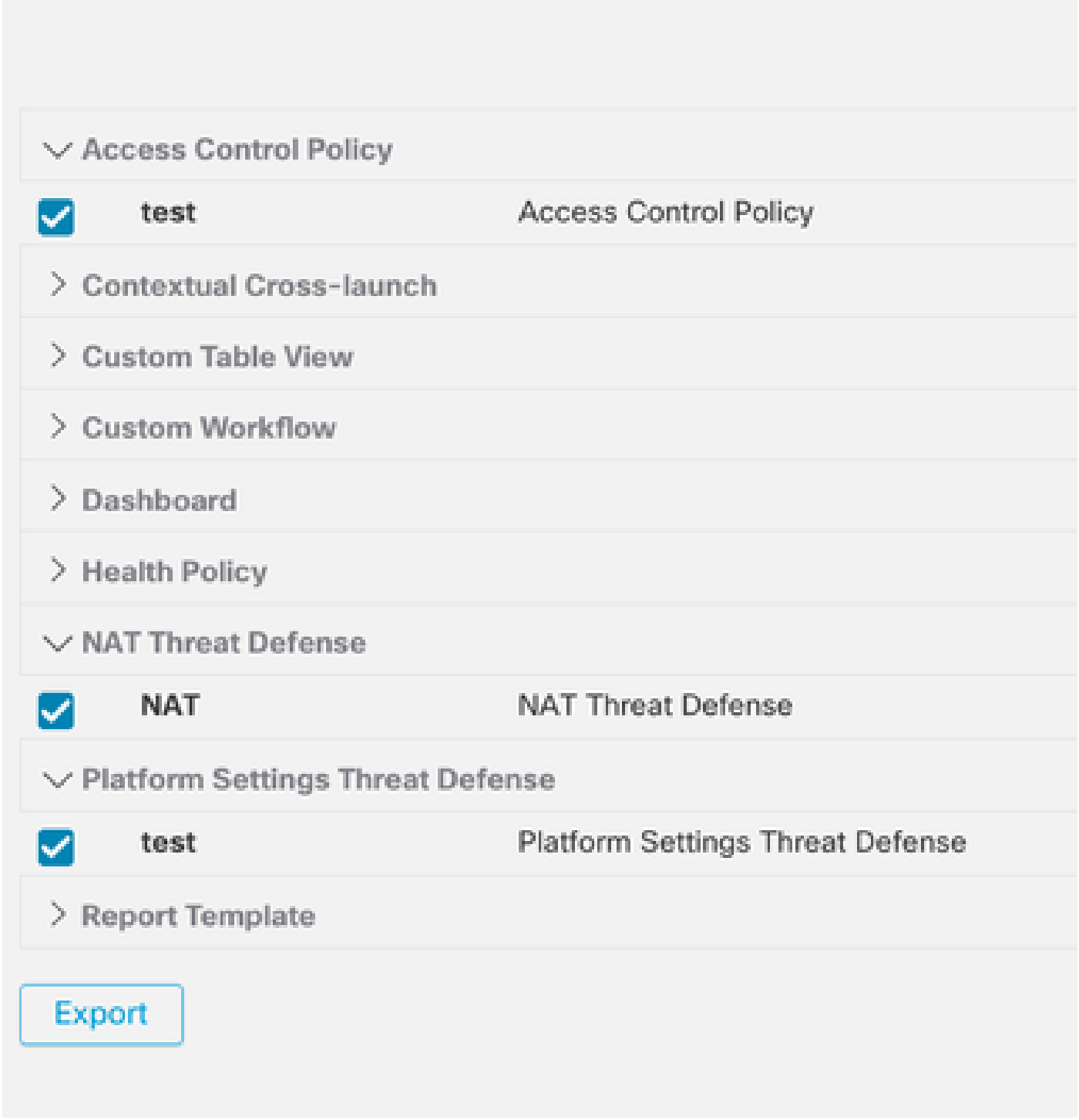


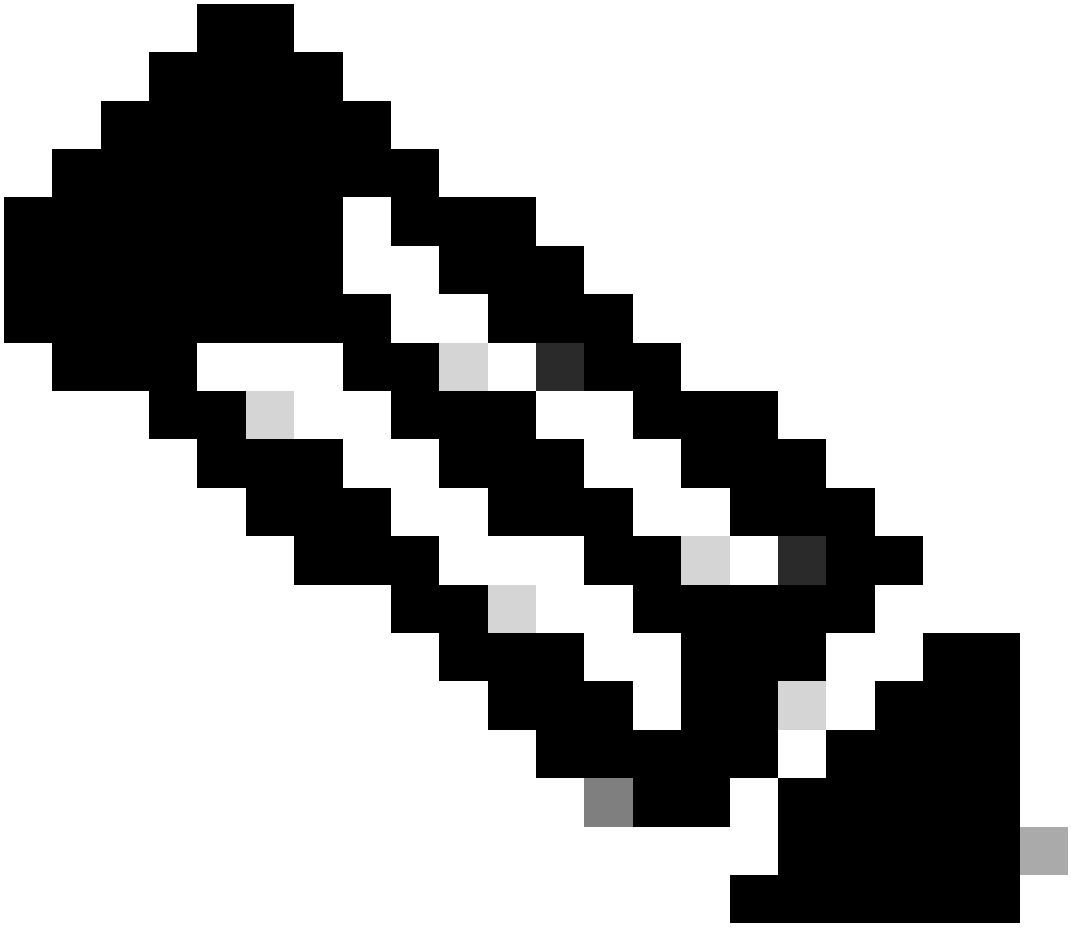
注：ダウンロードするファイルには、拡張子.SFOが付いており、IPアドレス、セキュリ

ティゾーン、スタティックルート、およびその他のデバイス設定などのデバイス設定情報が含まれている必要があります。

5. デバイスに関連付けられたポリシーをエクスポートする必要があります。System > Tools > Import/Exportの順に選択し、exportするポリシーを選択して、exportをクリックします。



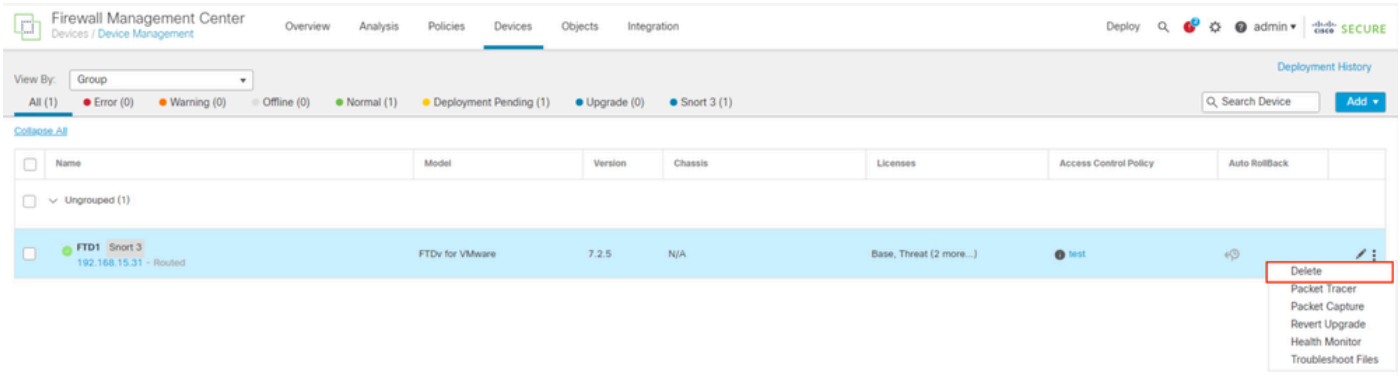

Access Control Policy
test
Access Control Policy
Contextual Cross-launch
Custom Table View
Custom Workflow
Dashboard
Health Policy
NAT Threat Defense
NAT
NAT Threat Defense
Platform Settings Threat Defense
test
Platform Settings Threat Defense
Report Template
Export



注:.SFOファイルが正常にダウンロードされたことを確認します。エクスポートをクリックすると、ダウンロードが自動的に実行されます。このファイルには、アクセスコントロールポリシー、プラットフォーム設定、NATポリシー、およびその他のポリシーが含まれています。これらはデバイス設定とともにエクスポートされず、宛先FMCに手動でアップロードする必要があるため、移行に不可欠なポリシーです。

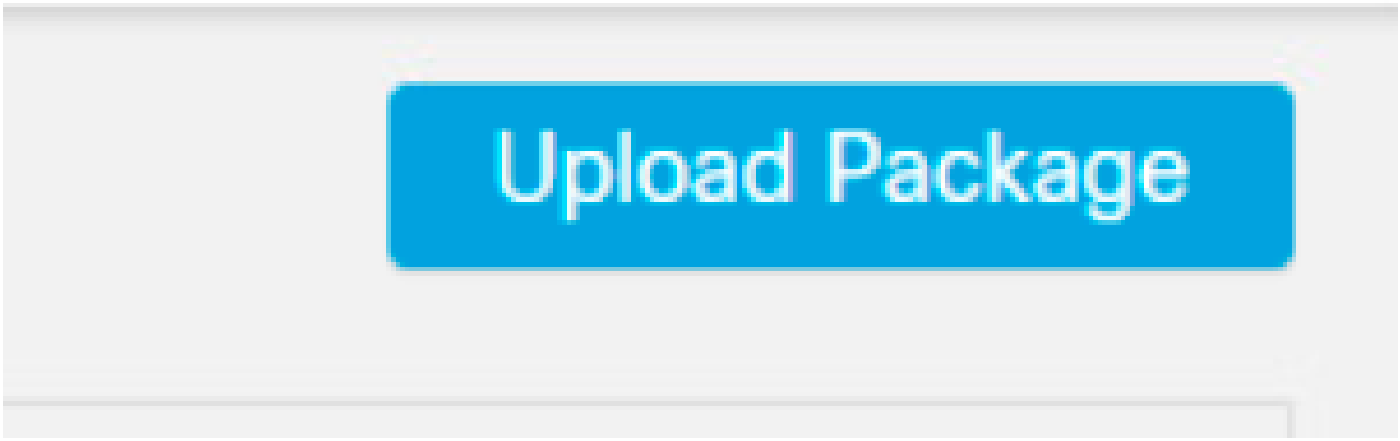
---

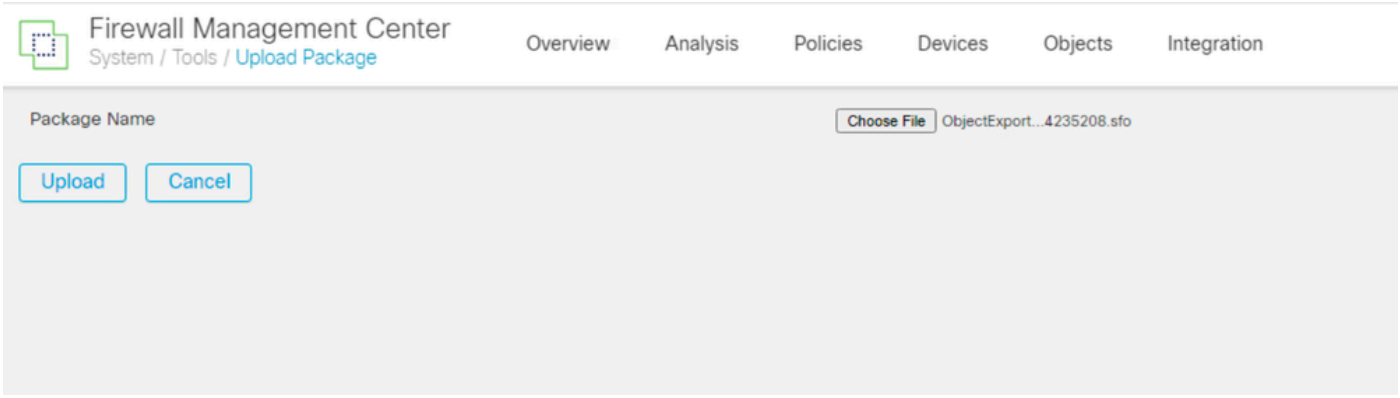
6. FMCからFTDデバイスの登録を解除し、Devices > Device managementに移動し、右側にある3つの垂直ドットをクリックしてdeleteを選択します。



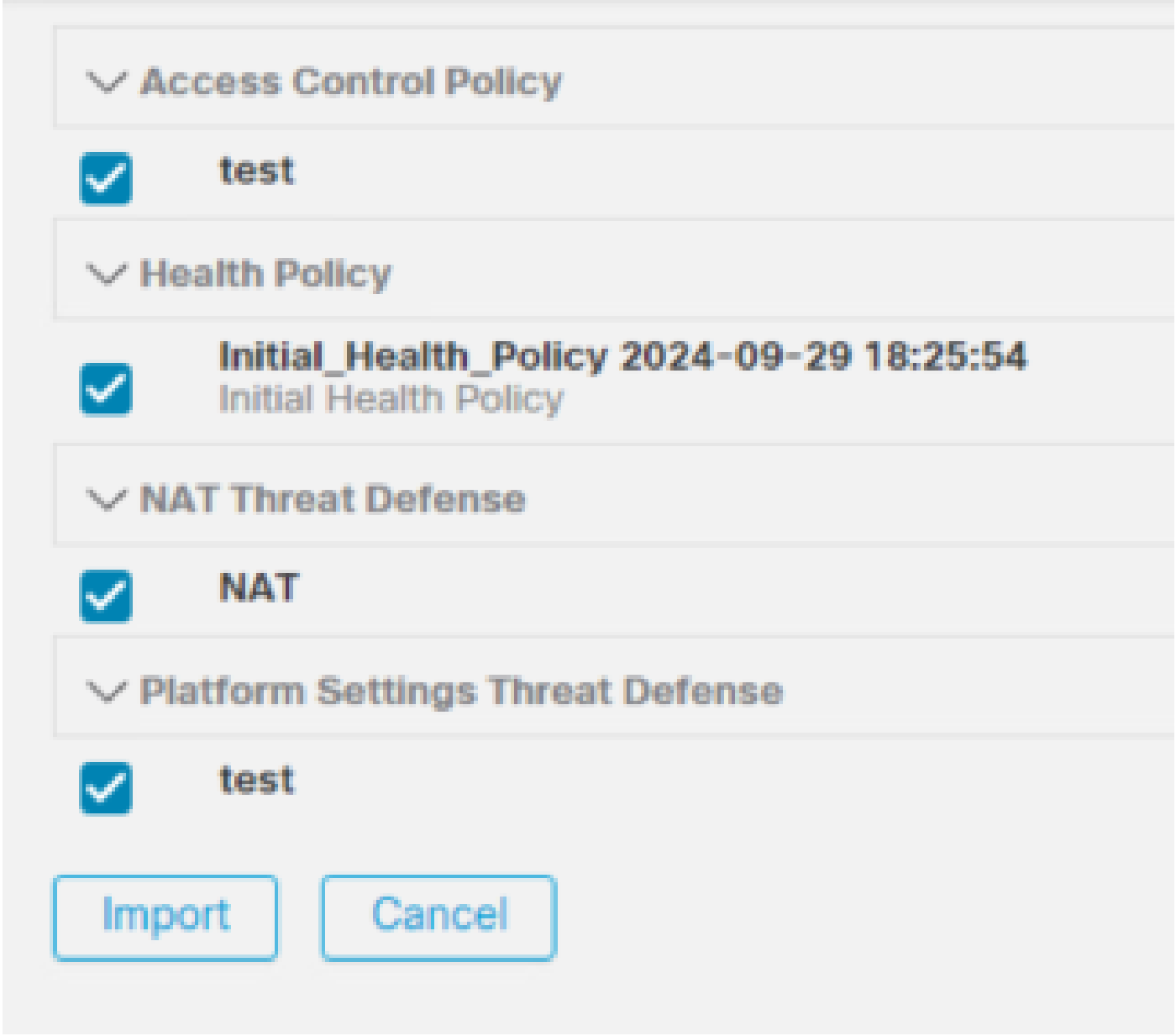
7. 宛先FMCを準備します。

- 宛先FMCにログインします。
- ステップ5でダウンロードしたソースFMCポリシーをインポートして、FMCが新しいデバイスを受け入れる準備ができていることを確認します。System > Tools > Import/Exportの順に移動し、upload packageをクリックします。インポートするファイルをアップロードして、uploadをクリックします。

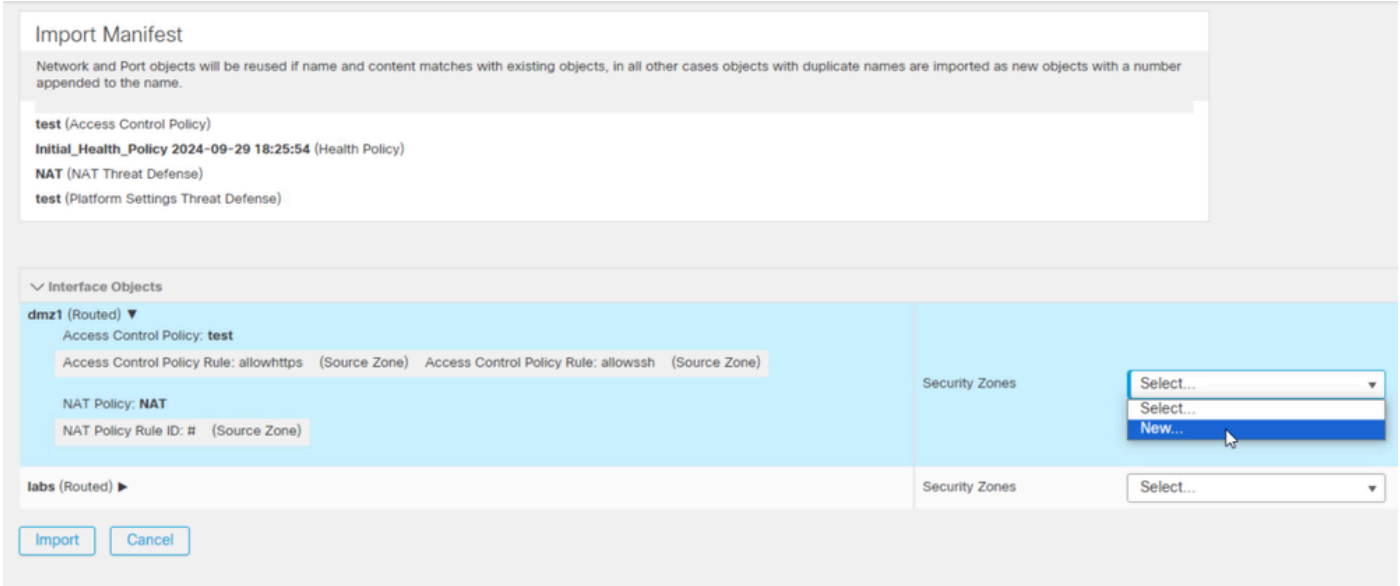




8. インポート先FMCにインポートするポリシーを選択します。

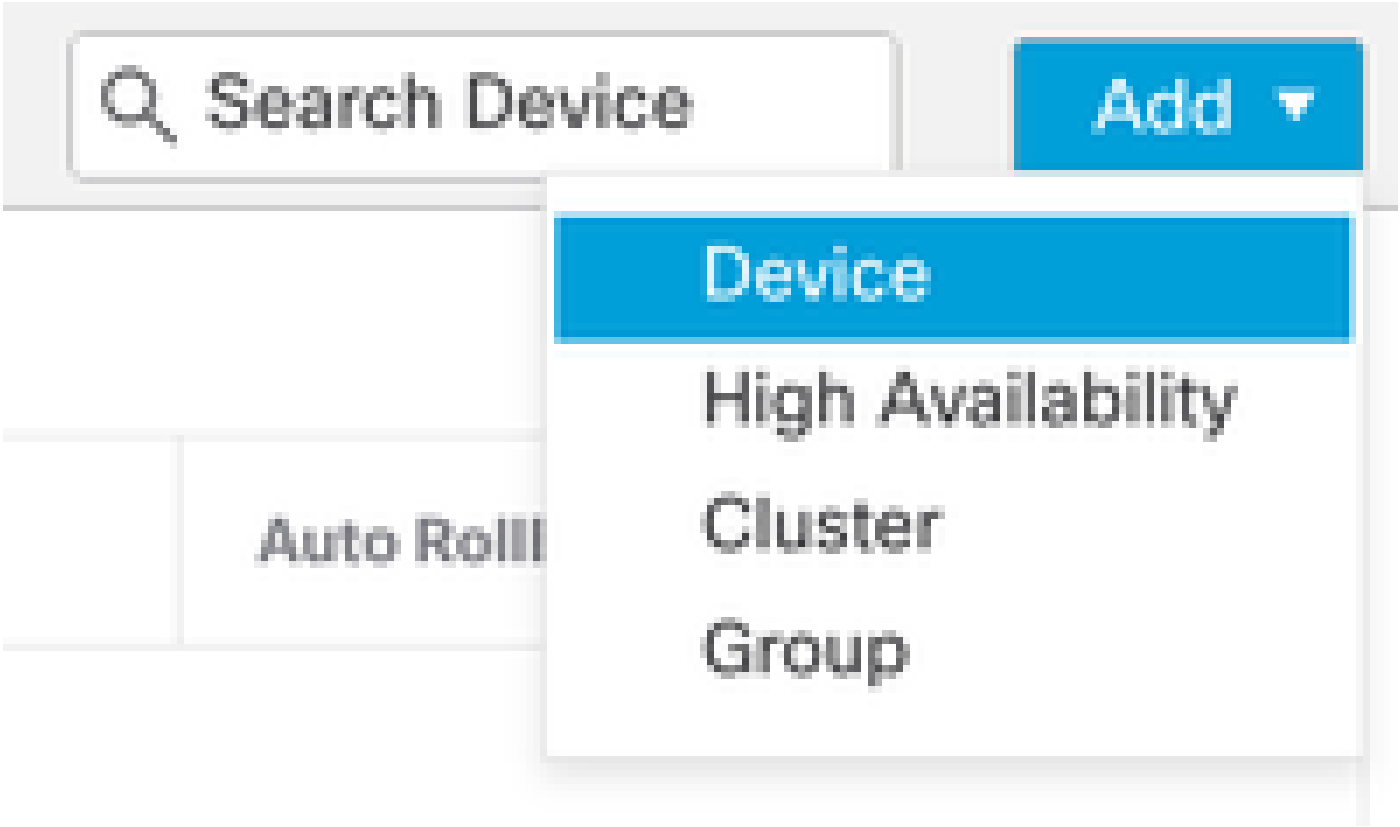


9. インポートマニフェストで、インターフェイスオブジェクトに割り当てるセキュリティゾーンを選択するか、新しいゾーンを作成し、インポートをクリックします。



10. 宛先FMCにFTDを登録します。

- 宛先FMCで、Device > Managementタブに移動し、Add > Deviceを選択します。
- プロンプトに応答して、登録プロセスを完了します。



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

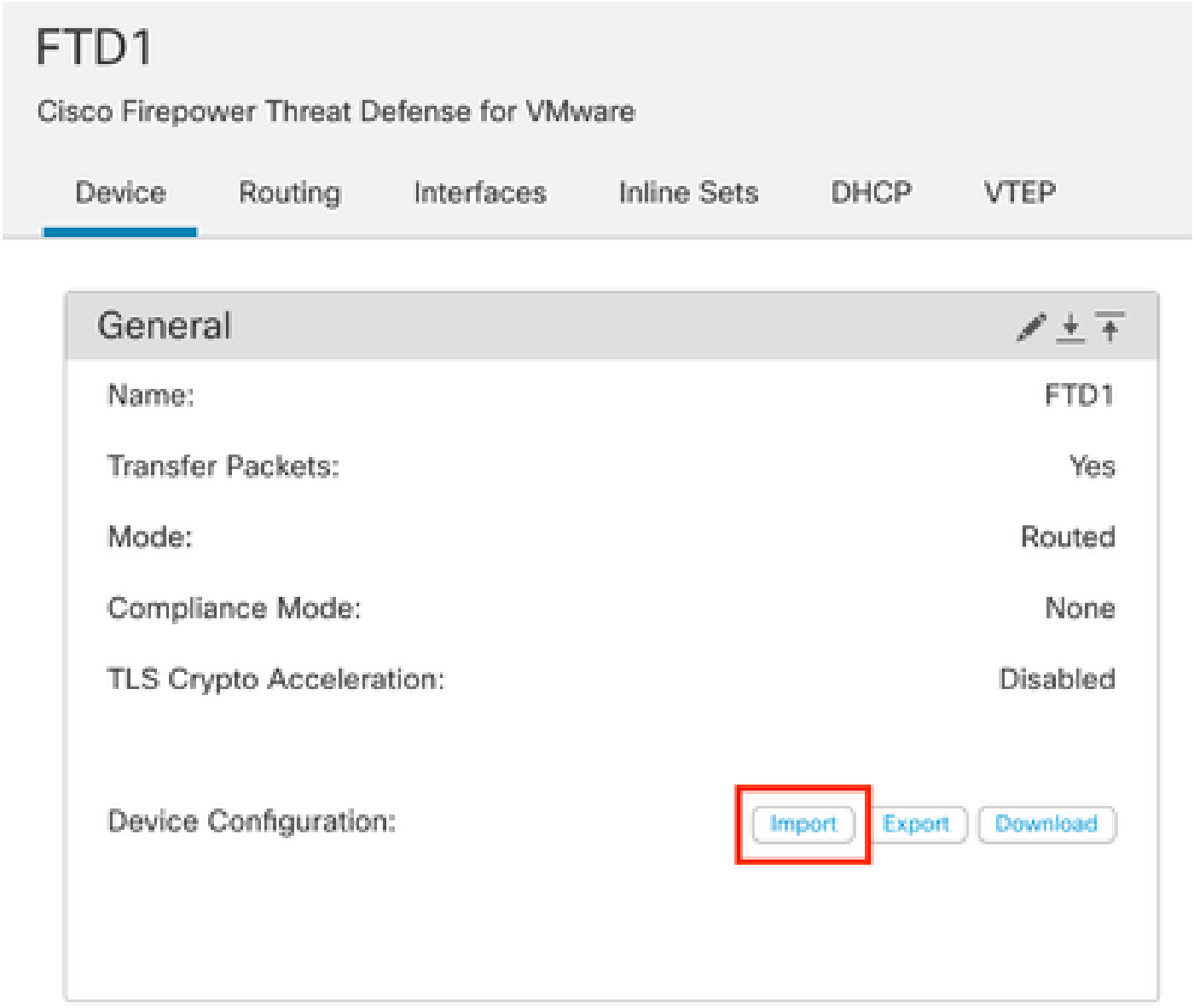
† Either host or NAT ID is required.

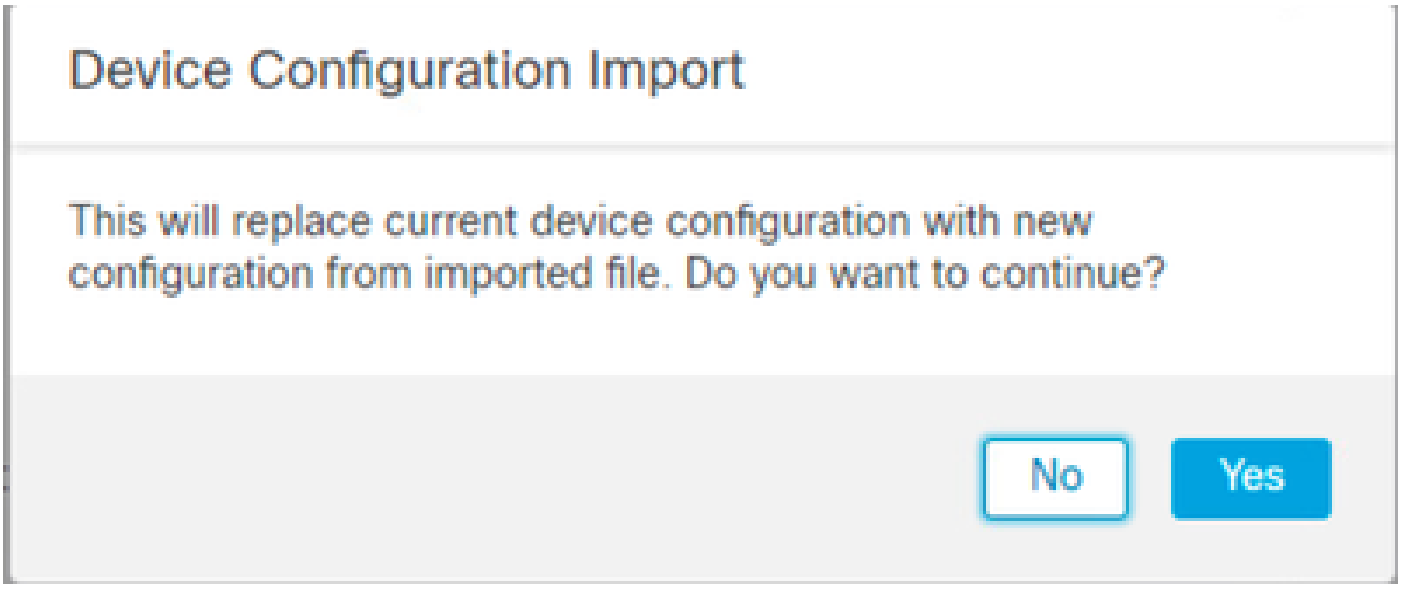
Cancel

Register

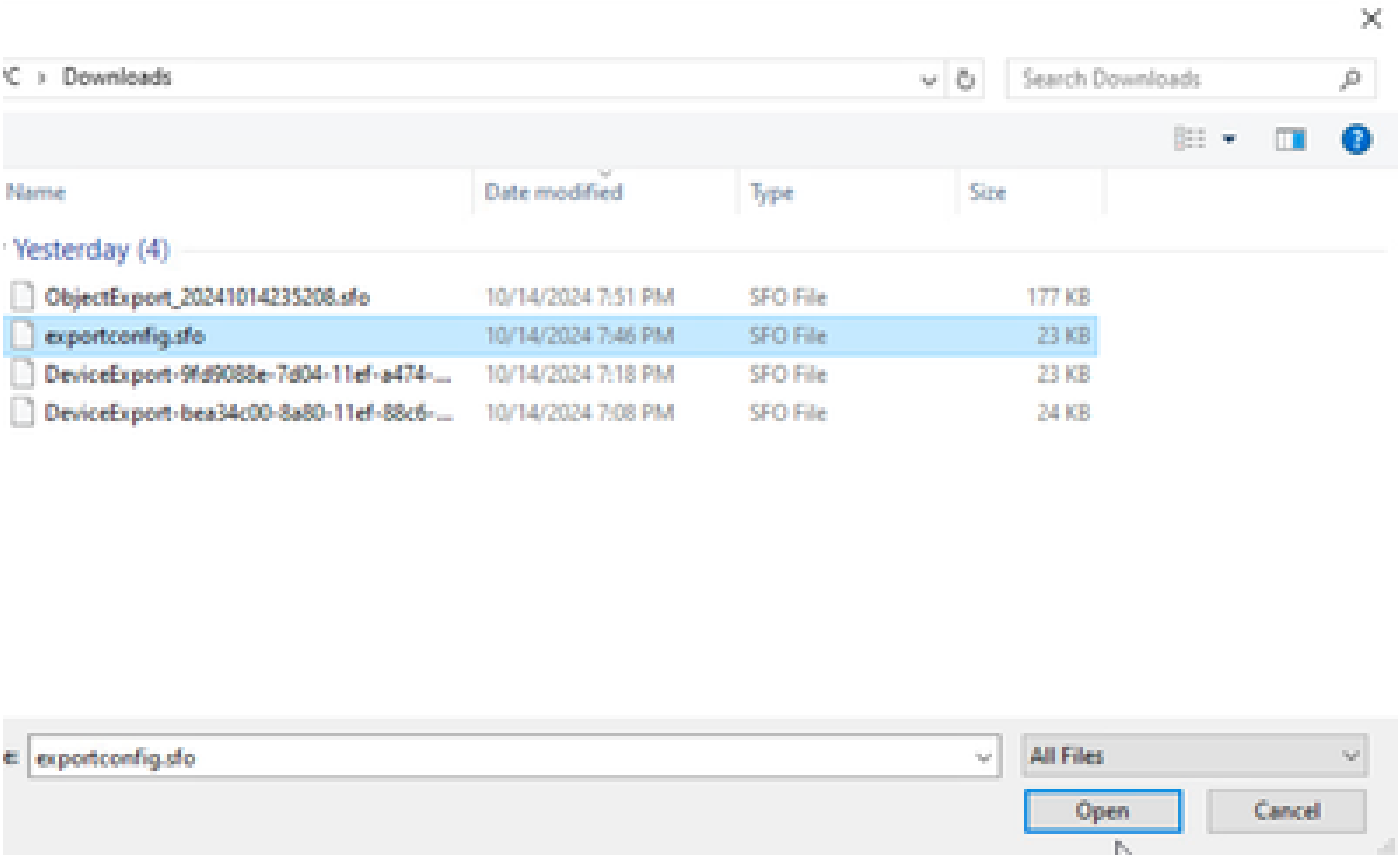
詳細については、『Firepower Management Centerコンフィギュレーションガイド』の「Firepower Management Centerへのデバイスの追加」を参照してください。

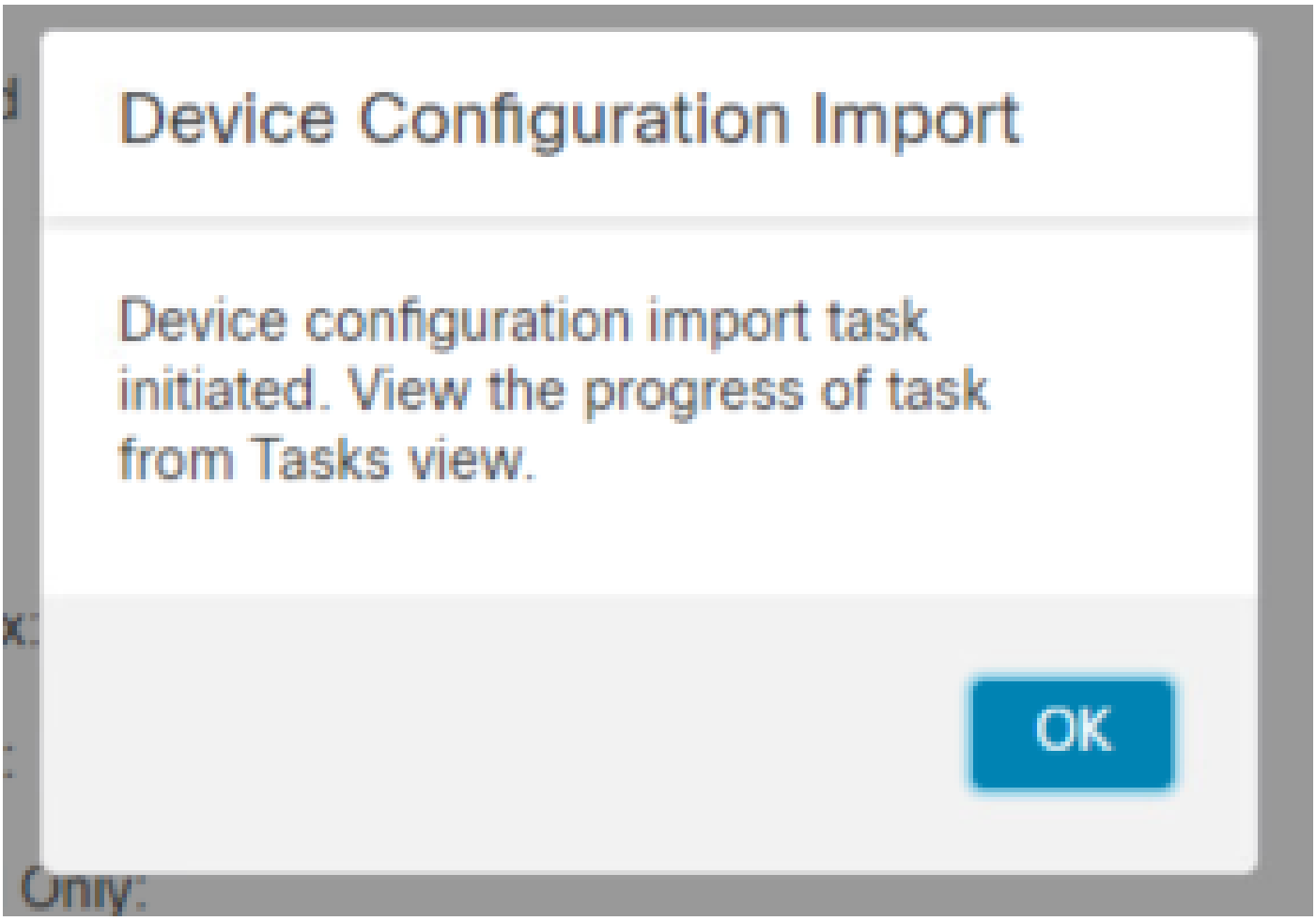
11. Device > Device Managementの順に移動し、FTD > Deviceを選択して、importをクリックします。 デバイスの設定を置き換えるか確認する警告が表示されたら、yesをクリックします。



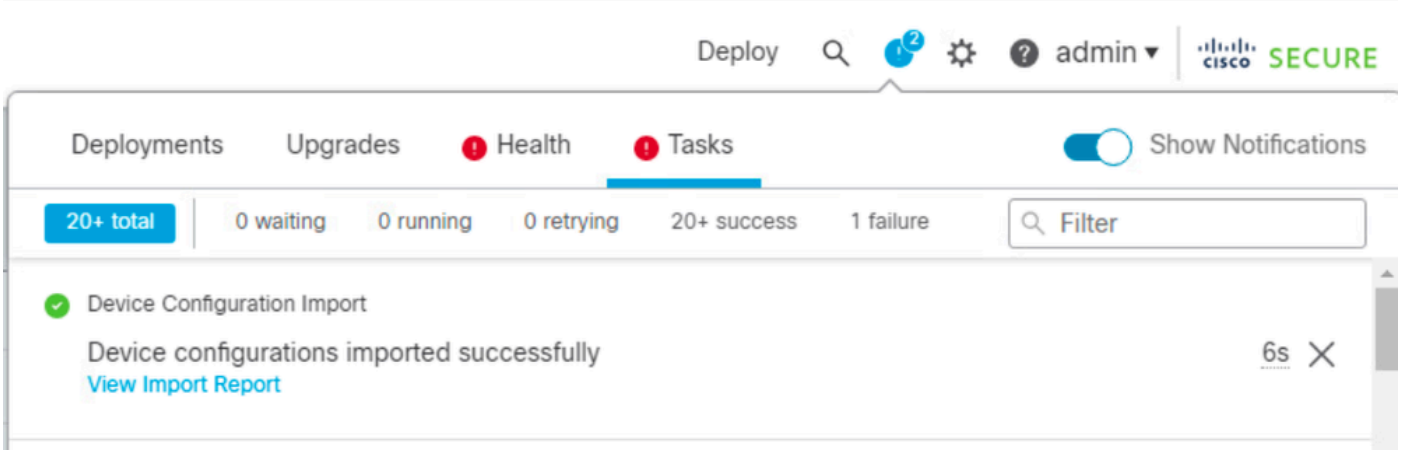


12. インポート設定ファイル（拡張子.SFO）を選択し、uploadをクリックします。インポートが開始されたことを示すメッセージが表示されます。





13. 最後に、インポートが完了するとアラートが表示され、レポートが自動的に生成されます。これにより、インポートされたオブジェクトとポリシーを確認できます。



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

確認

移行が完了したら、FTDデバイスが正しく登録され、宛先FMCで機能していることを確認します。

- 宛先FMCのデバイスステータスをチェックします。
- すべてのポリシーと設定が正しく適用されていることを確認します。
- テストを実行して、デバイスが動作可能であることを確認します。

トラブルシュート

移行プロセス中に問題が発生した場合は、次のトラブルシューティング手順を検討してください。

- FTDデバイスと両方のFMCの間のネットワーク接続を確認します。
- 両方のFMCのソフトウェアバージョンが同じであることを確認します。
- 両方のFMCでエラーメッセージまたは警告がないかアラートを確認します。

関連情報

- Cisco Secure Firewall Management Centerアドミニストレーションガイド
- Firepowerデバイス登録の設定、確認、トラブルシューティング

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。