FDMを介したSnort 2からSnort 3へのアップグレード

内容

はじめに

このドキュメントでは、Firepower Device Manager(FDM)でSnort 2バージョンからSnort 3バージョンにアップグレードする方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Firepower Threat Defense（FTD）
- Firepower Device Manager（FDM）
- Snort.

要件

次の要件を満たしていることを確認してください。

- Firepowerデバイスマネージャへのアクセス。
- FDMの管理権限。
- Snort 3を使用するには、FTDがバージョン6.7以降である必要があります。

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。

- FTD7.2.7

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

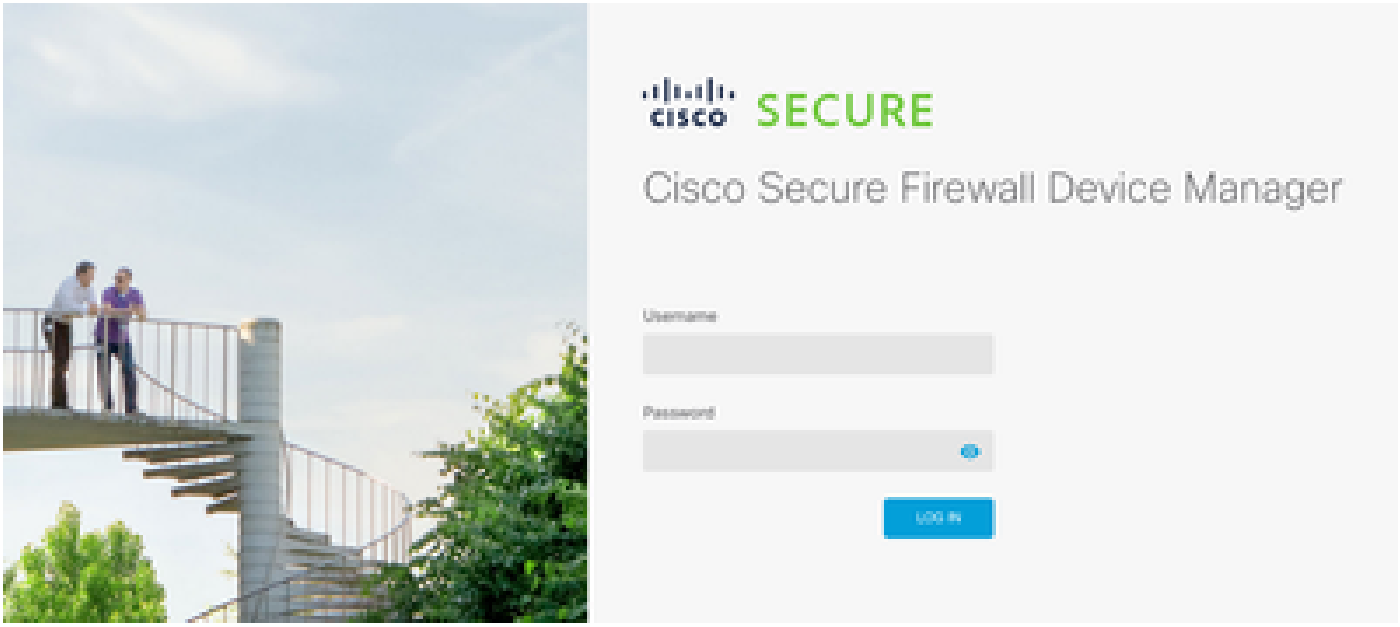
Snort 3機能は、Firepower Device Manager(FDM)用の6.7リリースで追加されました。Snort 3.0は、次の課題に対処するために設計されました。

- メモリとCPUの使用量を削減します。
- HTTPインスペクションの有効性を向上させる。
- 迅速な設定のロードとSnortの再起動
- プログラマビリティの向上による機能追加の迅速化

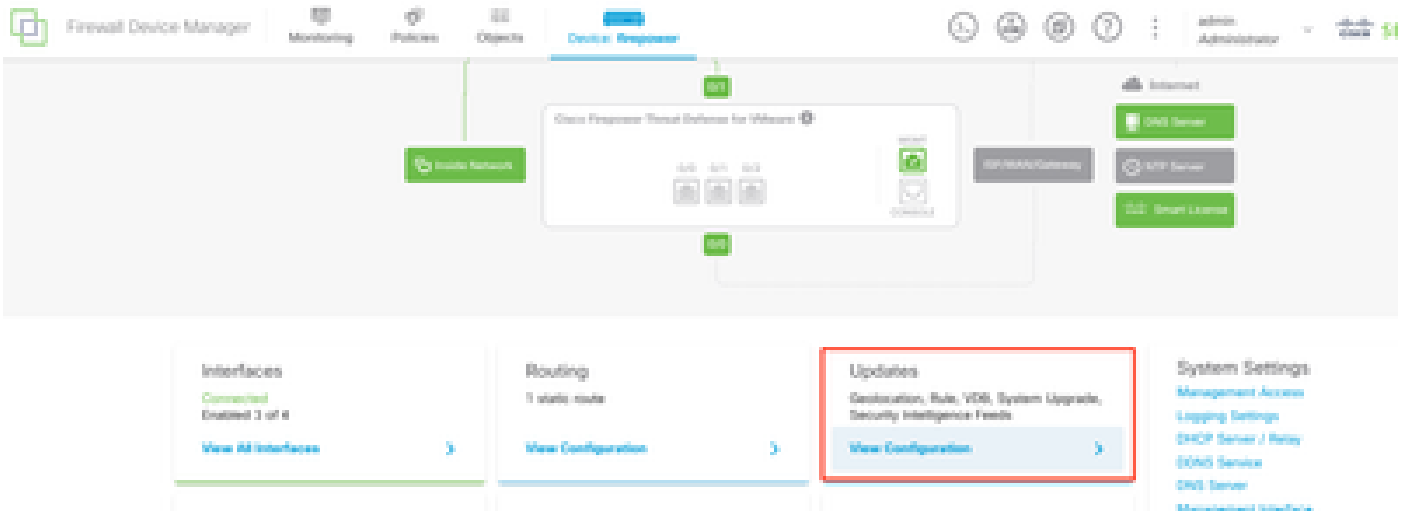
設定

コンフィギュレーション

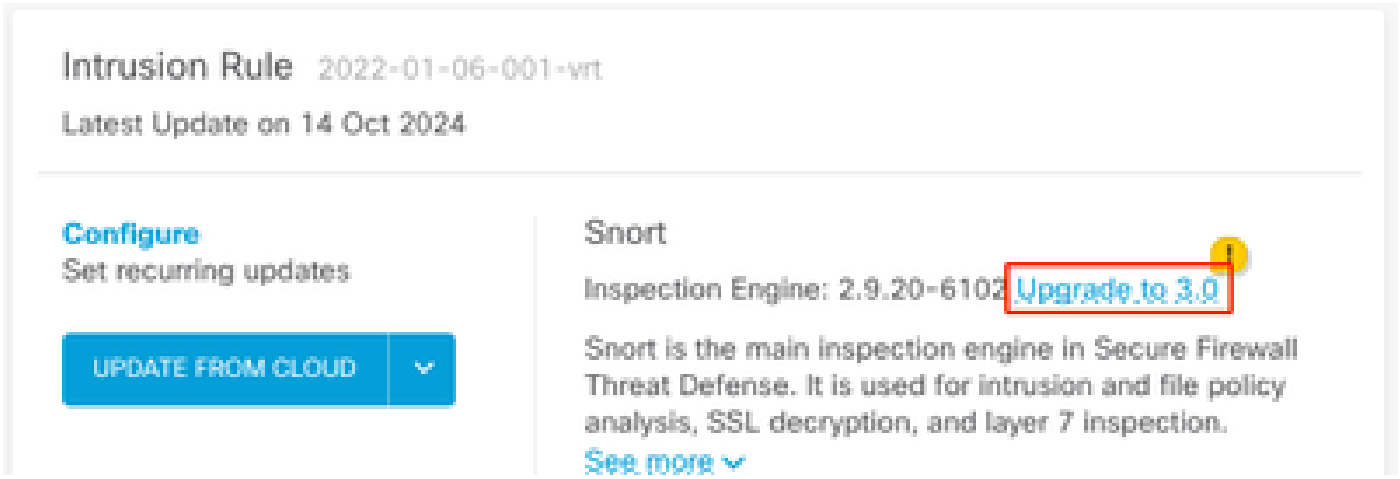
1. Firepowerデバイスマネージャにログインします。



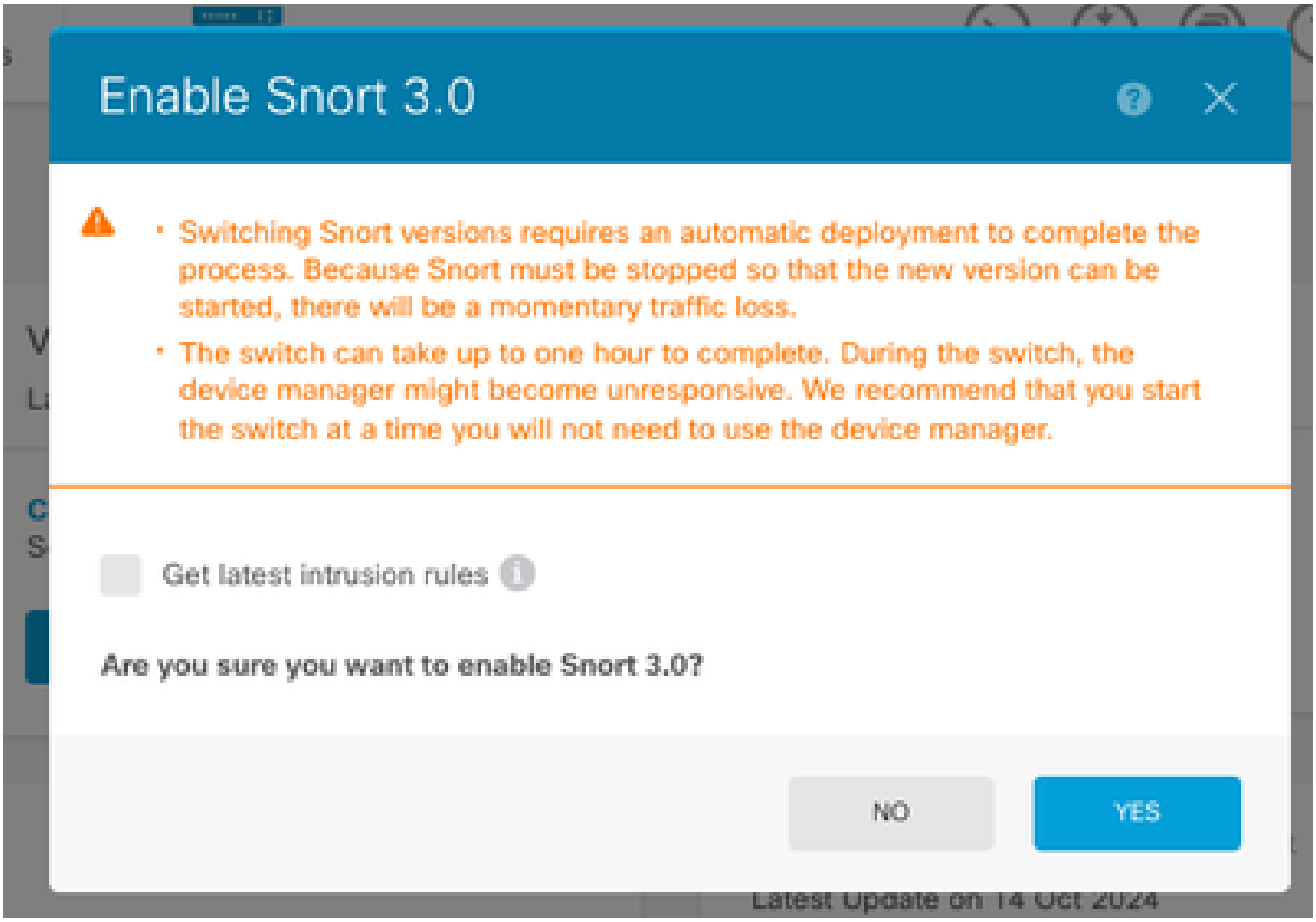
2. [デバイス] > [更新] > [構成の表示] に移動します。

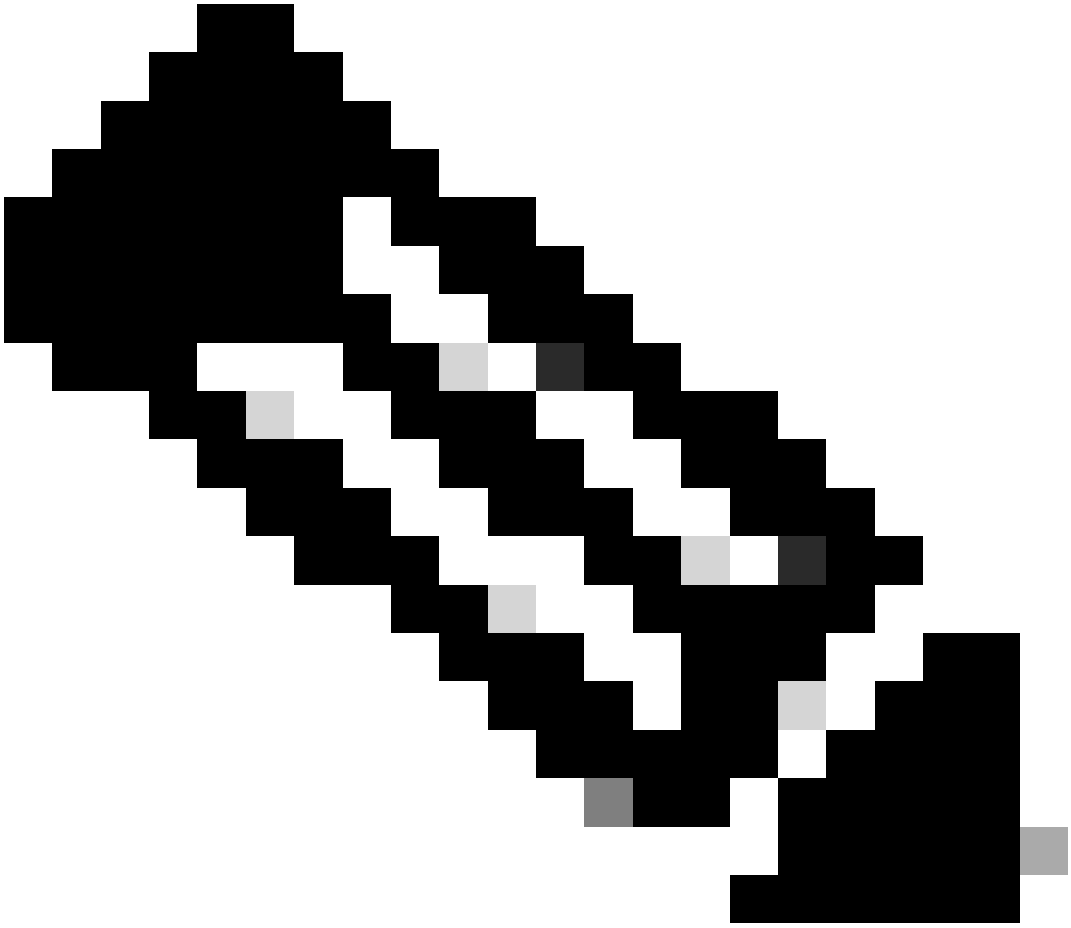


3. 侵入ルールセクションで、upgrade to snort 3をクリックします。

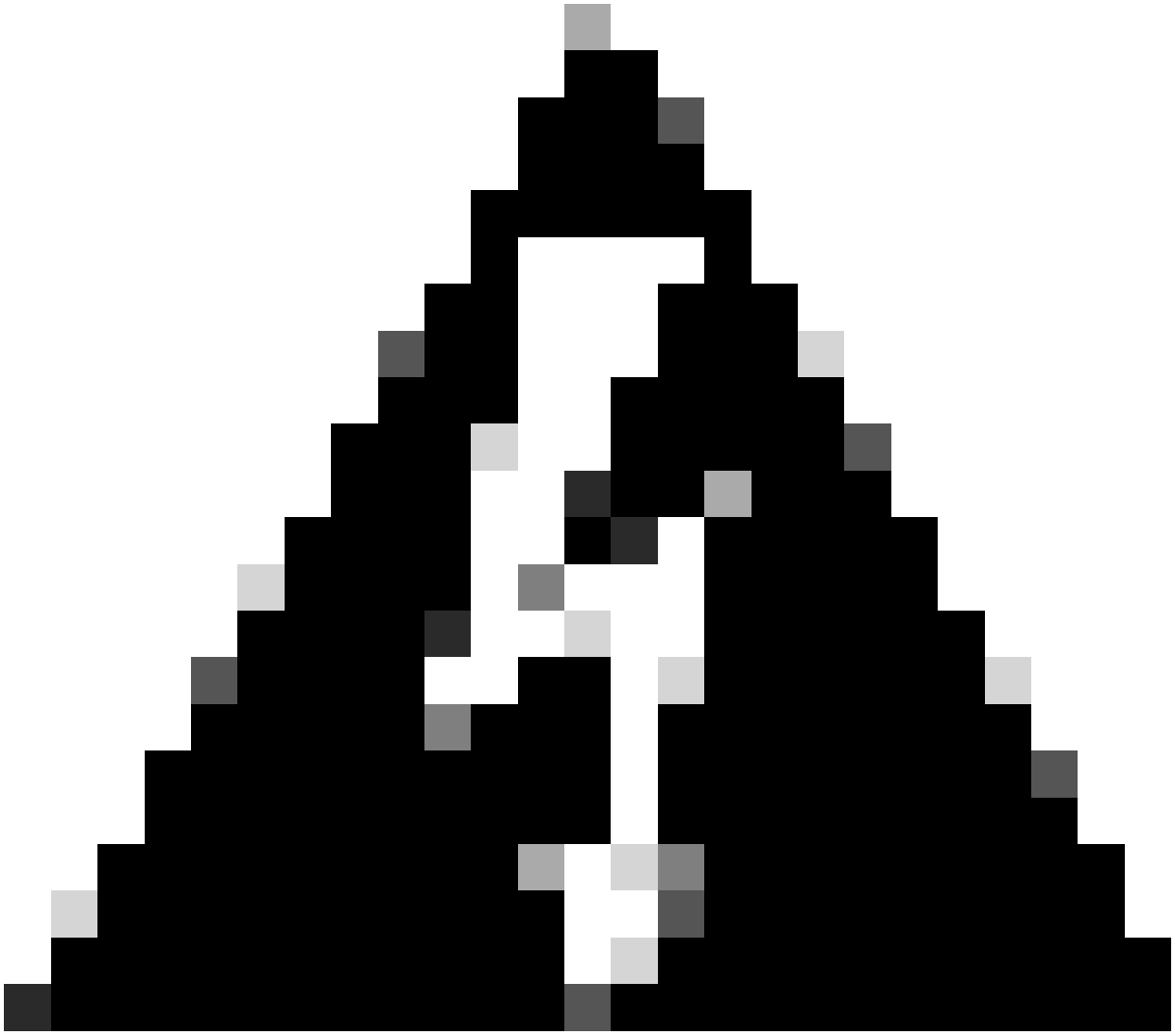


4. 選択を確認する警告メッセージが表示されたら、get the latest intrusion rules packageオプションを選択し、Yesをクリックします。


Enable Snort 3.0
Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive. We recommend that you start the switch at a time you will not need to use the device manager.
Get latest intrusion rules
Are you sure you want to enable Snort 3.0?
NO
YES
Latest Update on 14 Oct 2024

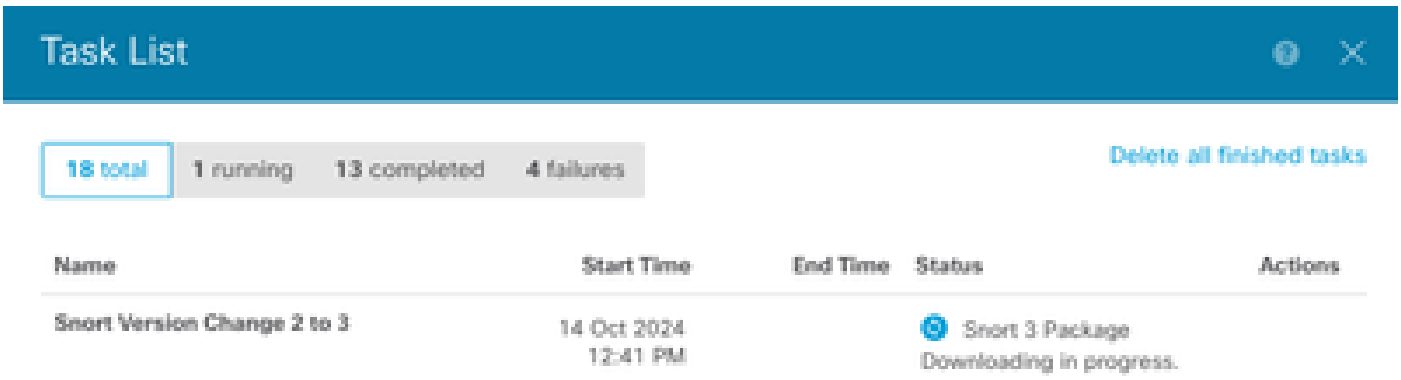


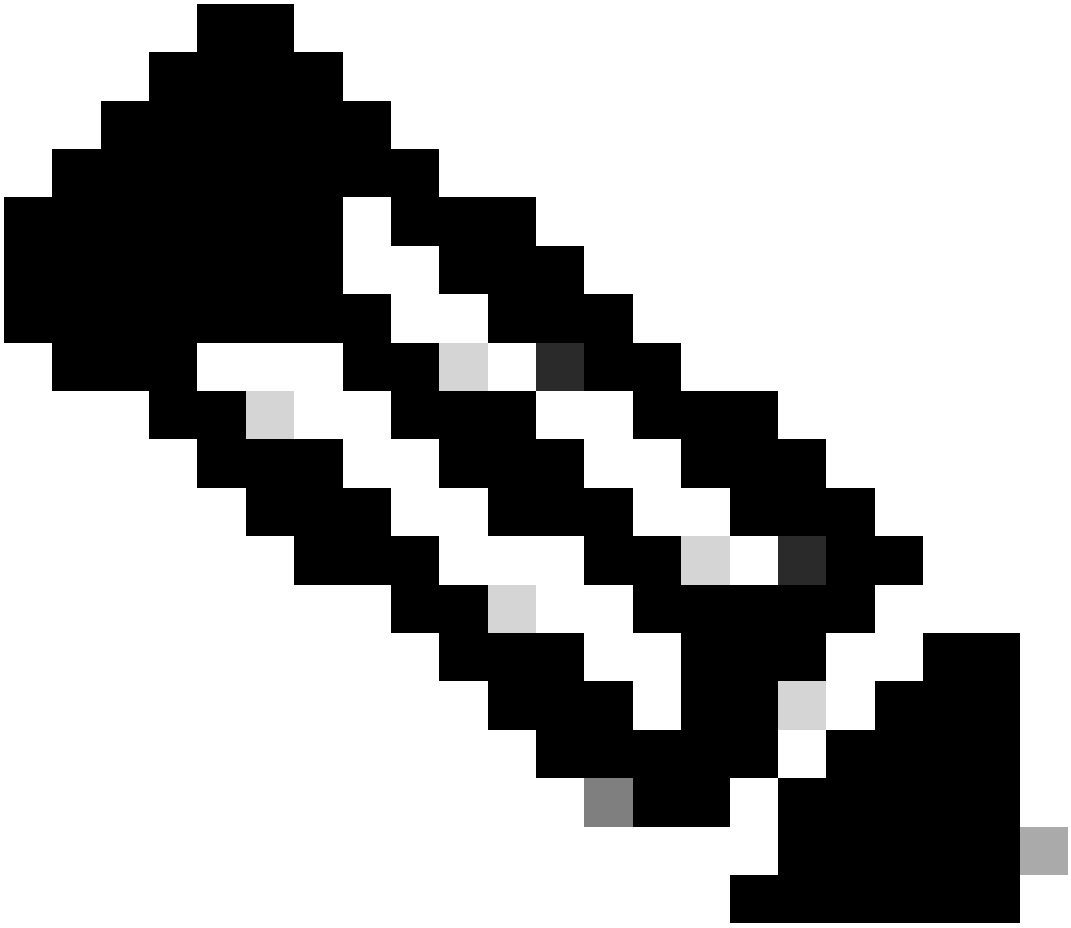
注：システムがダウンロードするパッケージは、アクティブなSnortバージョンのパッケージだけです。したがって、切り替え先のSnortバージョン用の最新のパッケージがインストールされている可能性は低くなります。侵入ポリシーを編集する前に、バージョンの切り替えタスクが完了するまで待つ必要があります。



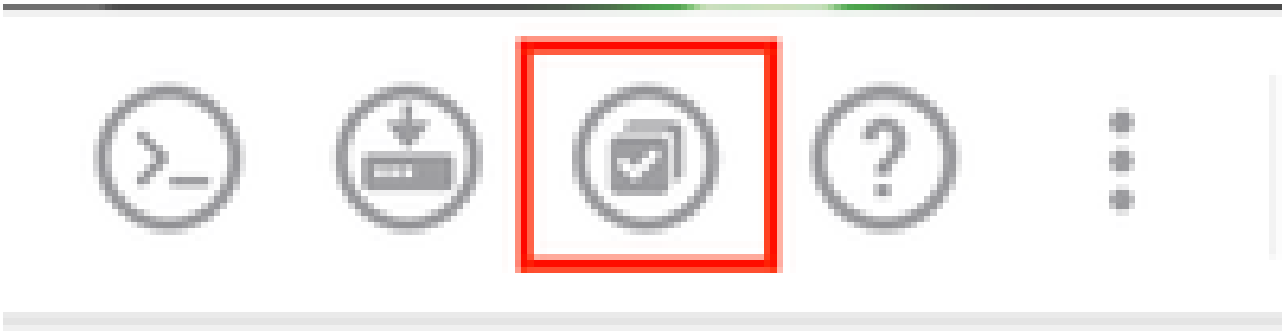
警告: Snortのバージョンを切り替えると、一時的にトラフィックが失われます。

5. アップグレードが開始したことをタスク・リストで確認する必要があります。



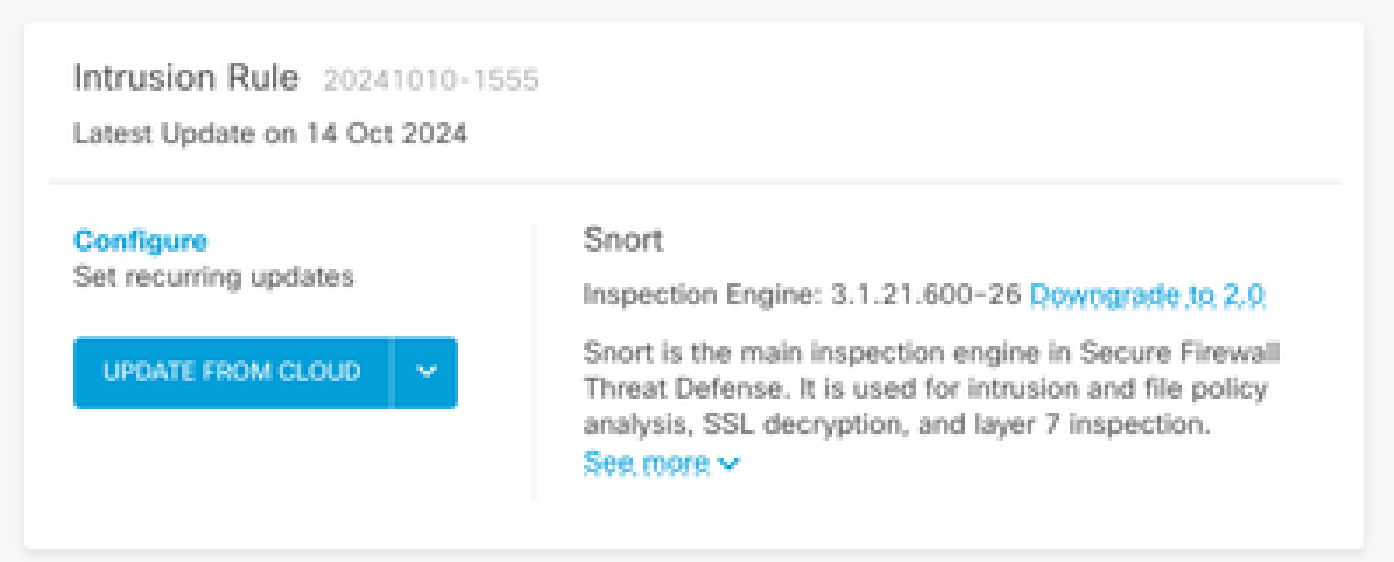


注：タスクリストは、展開アイコンの横にあるナビゲーションバーにあります。

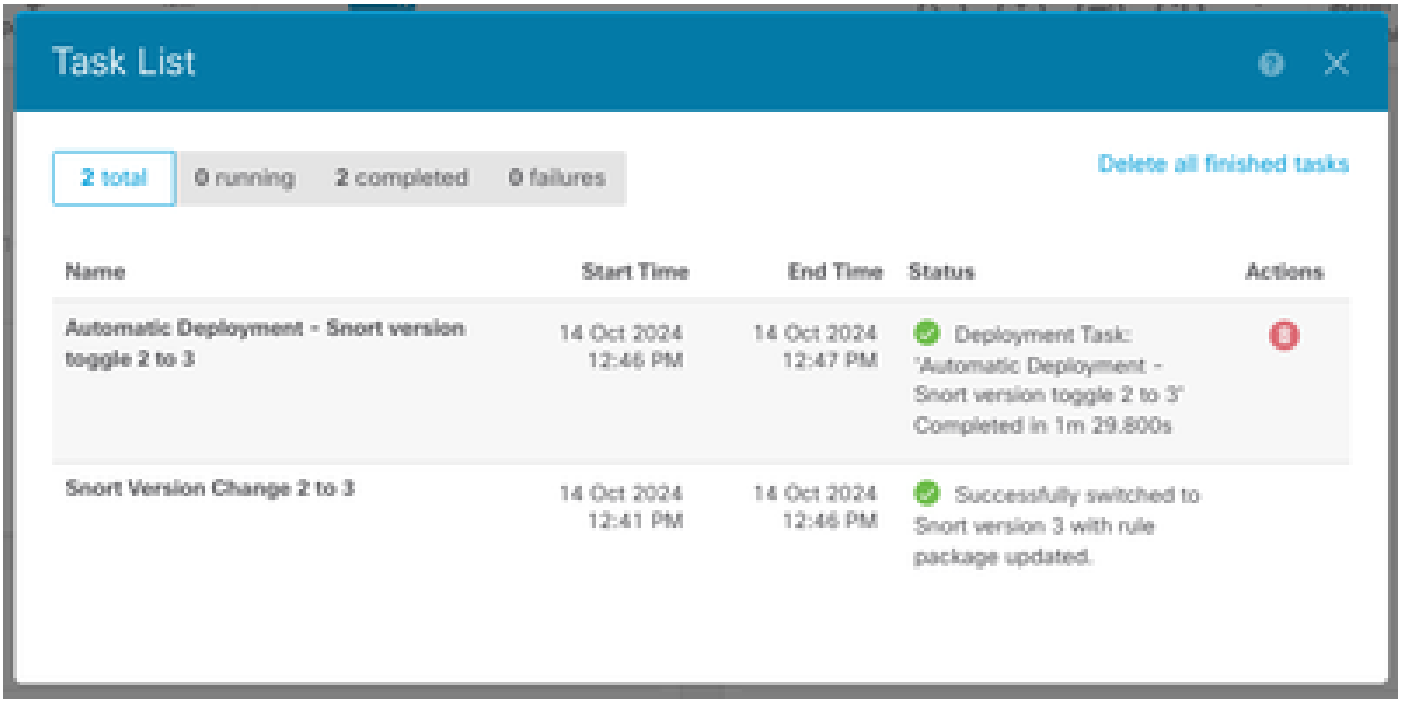


確認

「インスペクションエンジン」セクションには、Snortの現在のバージョンがSnort 3であると表示されます。



最後に、タスクリストで、Snort 3への変更が正常に完了して展開されていることを確認します。



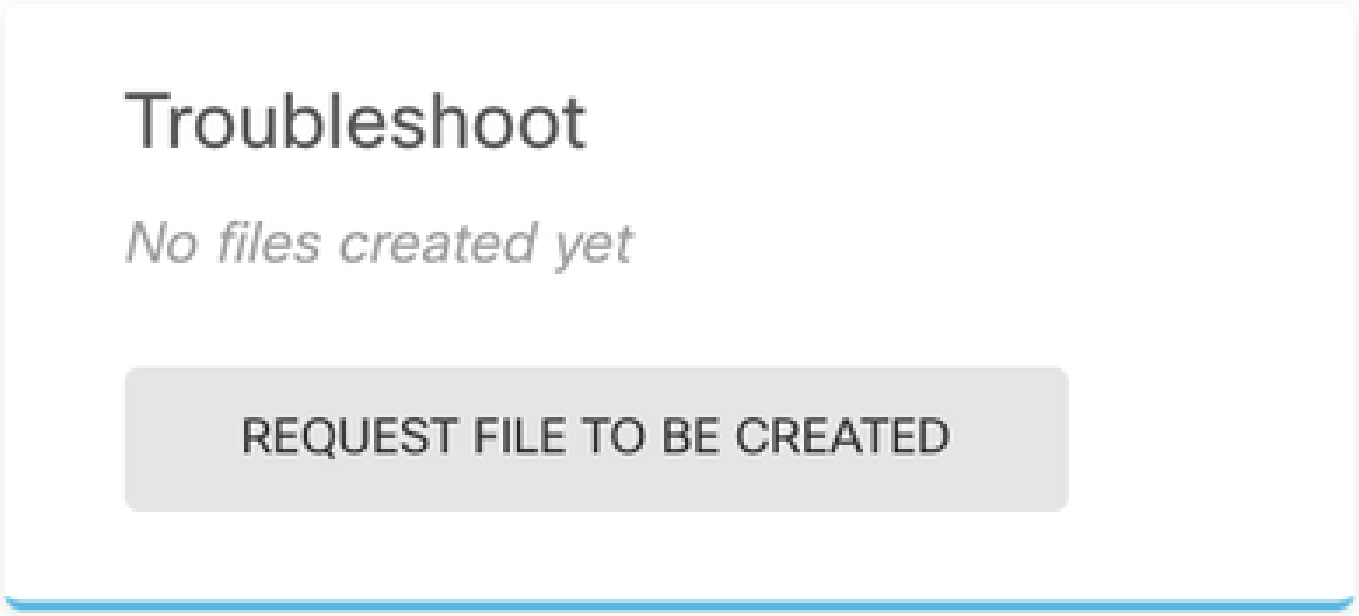
トラブルシュート

アップグレード中に問題が発生した場合は、次の手順を検討してください。

- 使用しているFTDのバージョンがSnort 3と互換性があることを確認します。

詳細については、『Cisco Secure Firewall Threat Defense Compatibility Guide』を参照してください。

- FDMでトラブルシューティングファイルを収集します。Deviceタブに移動し、Request file to be createdをクリックします。収集したら、TACでケースを開き、さらにサポートを得るために、ファイルをケースにアップロードします。



関連情報

- Snort 3の導入
- Snortに関する文書
- Cisco Secure Firewall Device Managerコンフィギュレーションガイド、バージョン7.2

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。