Upgrade van Snort 2 naar Snort 3 via FDM

Inhoud

Inleiding

Dit document beschrijft hoe u in Firepower Device Manager (FDM) kunt upgraden van de tweede versie naar de derde versie.

Voorwaarden

Cisco raadt kennis van de volgende onderwerpen aan:

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

Vereisten

Zorg ervoor dat u aan de volgende vereisten voldoet:

- Toegang tot Firepower Device Manager.
- Administratieve voorrechten op de FDM.
- FTD moet ten minste versie 6.7 zijn om snort 3 te kunnen gebruiken.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- FTD 7.2.7

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een

opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

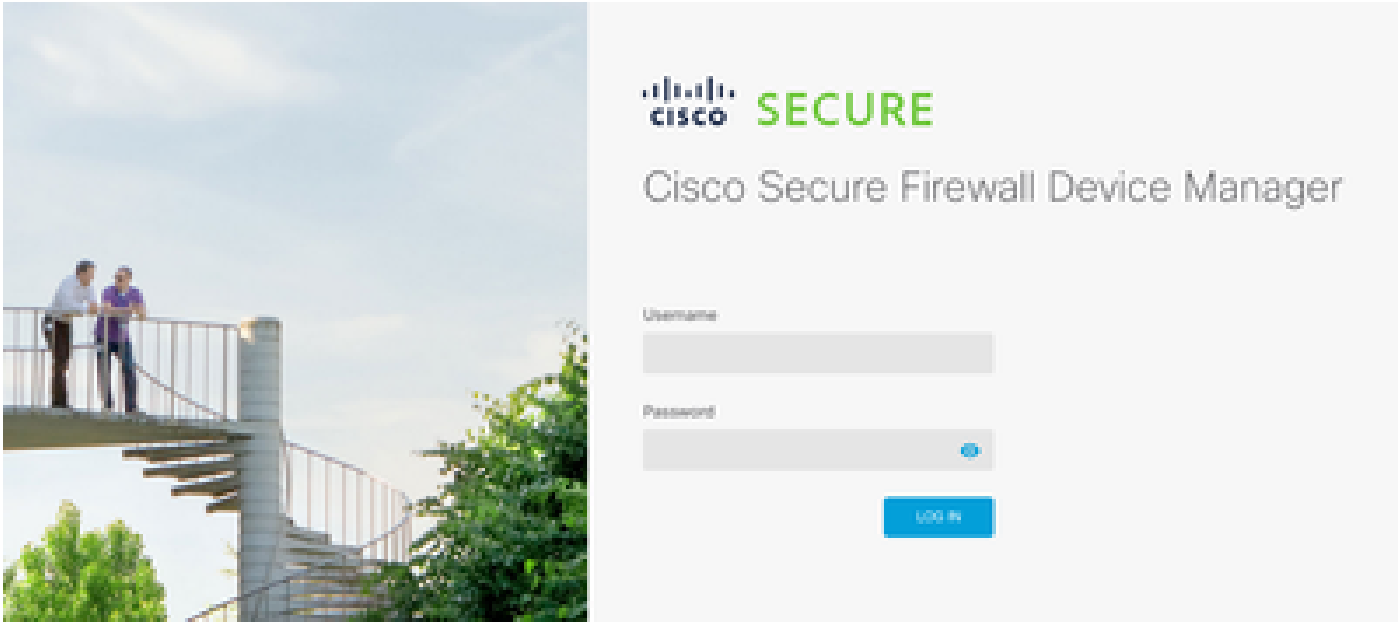
De functie snort 3 is toegevoegd in de 6.7 release voor Firepower Device Manager (FDM). Snort 3.0 is ontworpen om deze uitdagingen aan te gaan:

- Minder geheugen en minder CPU-gebruik.
- Verbeter de HTTP-inspectie-efficiëntie.
- Snellere configuratie laden en snel opnieuw starten.
- Betere programmeerbaarheid voor snellere toevoeging van extra functies.

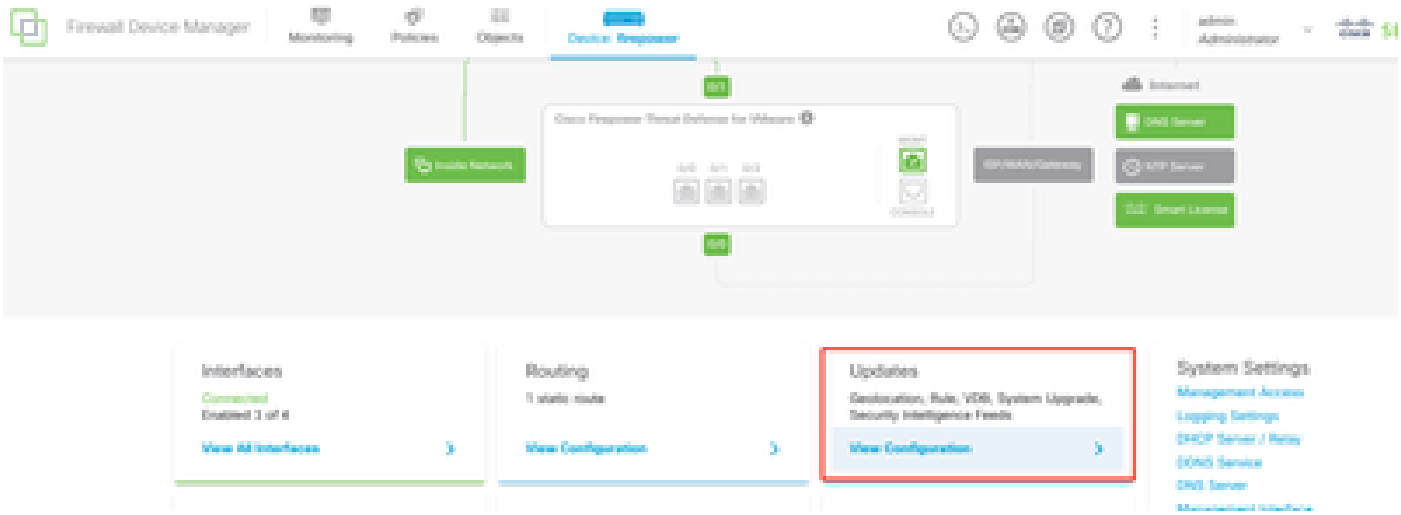
Configureren

Configuraties

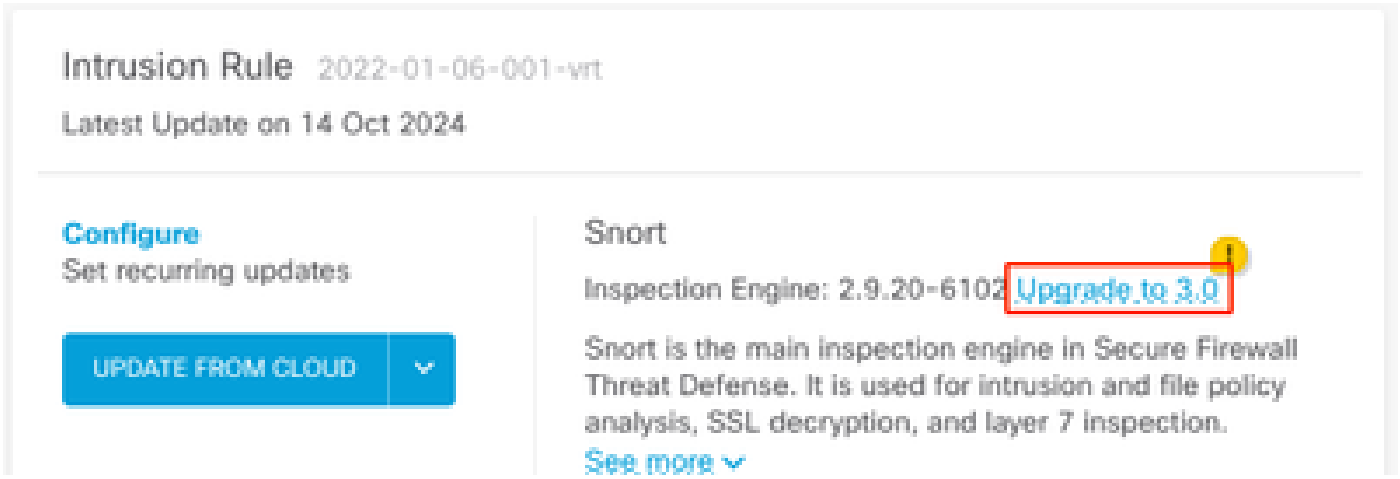
1. Log in op Firepower Device Manager.



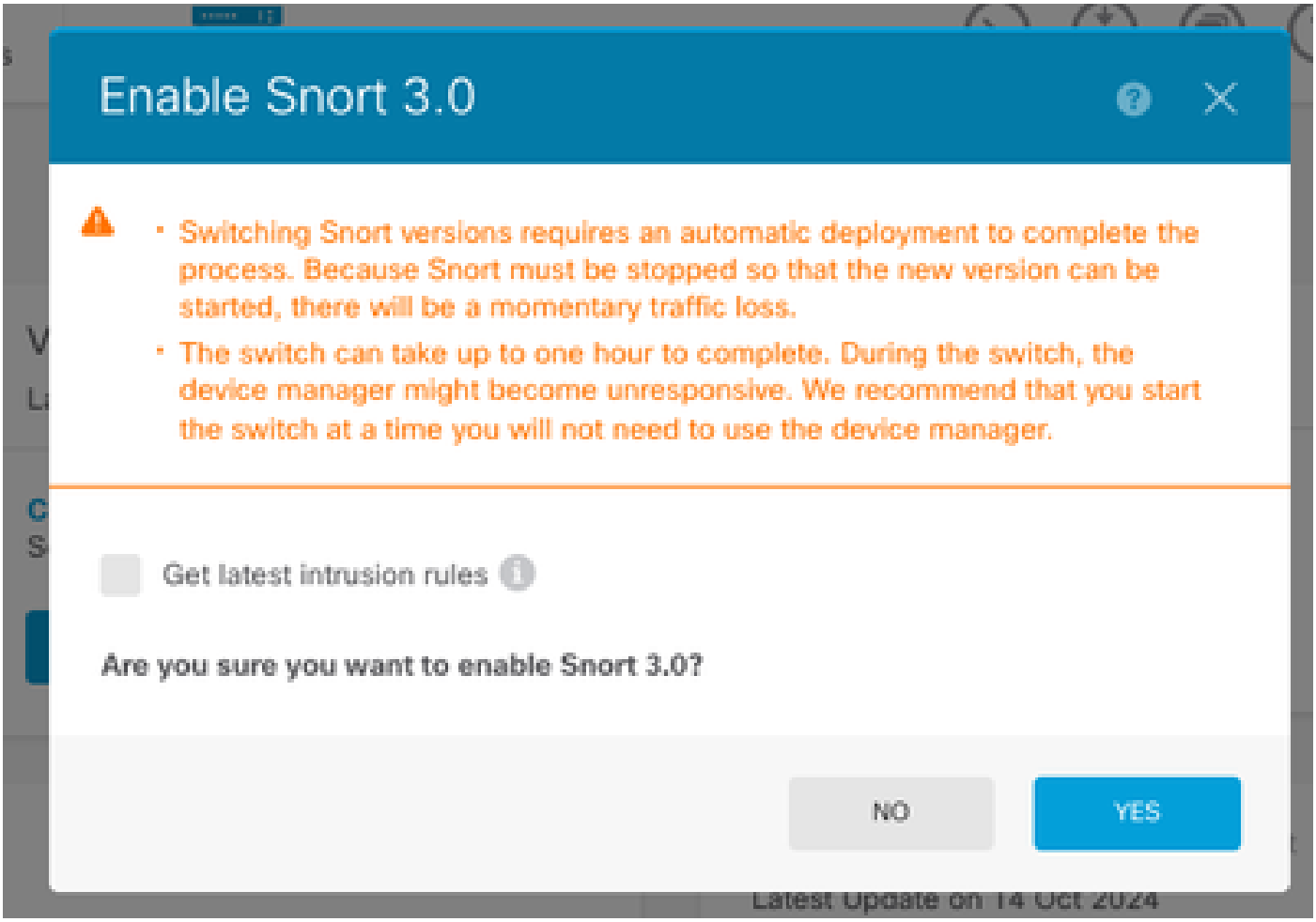
2. Navigeer naar apparaat > updates > Configuratie bekijken.

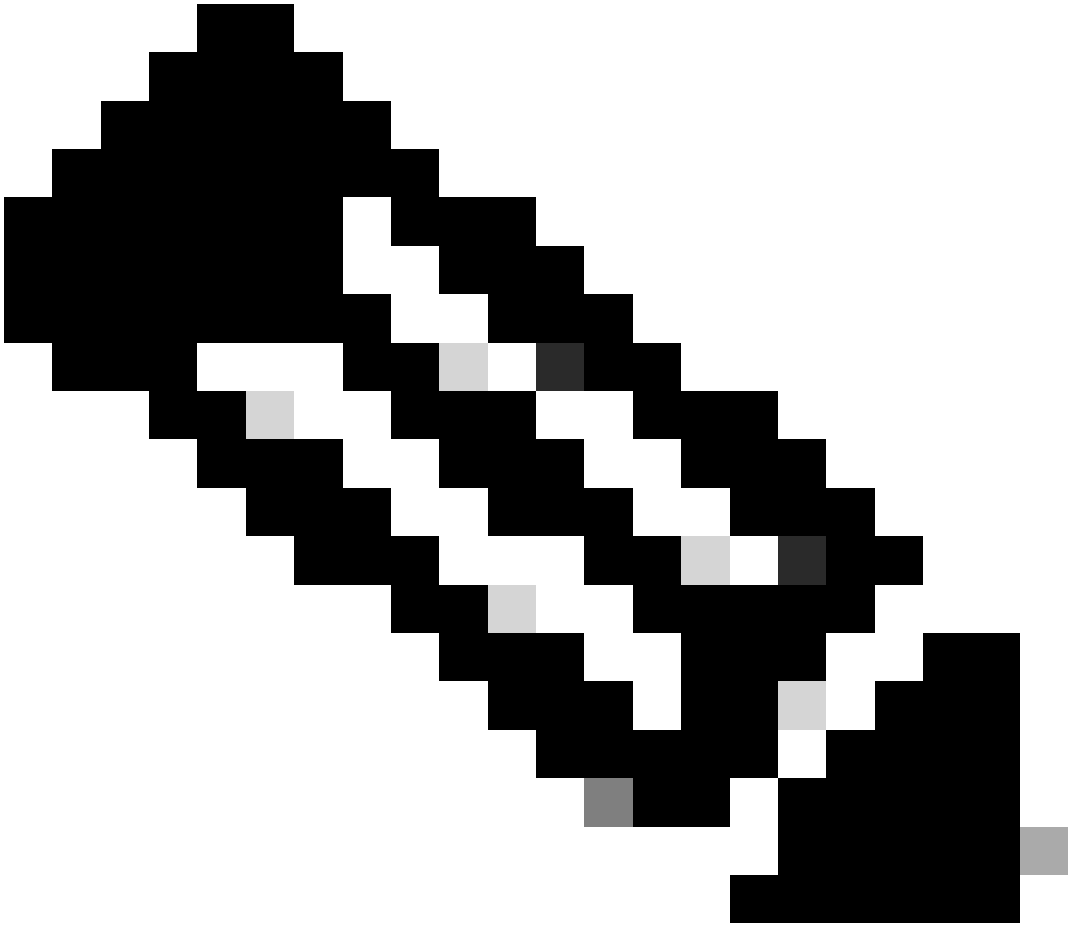


3. Klik in het gedeelte inbraakregels op upgrade naar snurken 3.

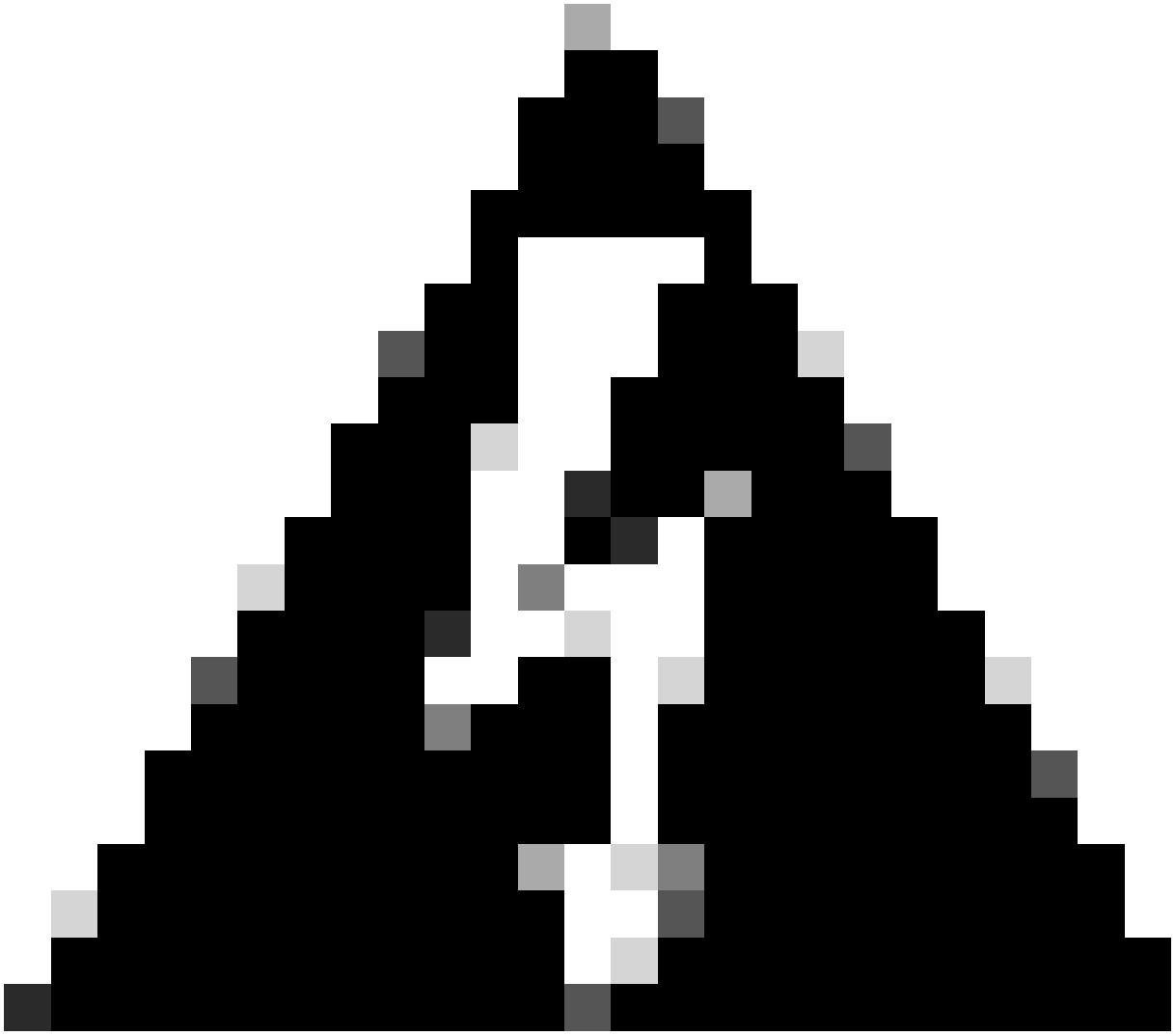


4. Op het waarschuwingsbericht om uw selectie te bevestigen, selecteert u de optie om het laatste pakket inbraakregels te verkrijgen, en klikt u vervolgens op Ja.


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

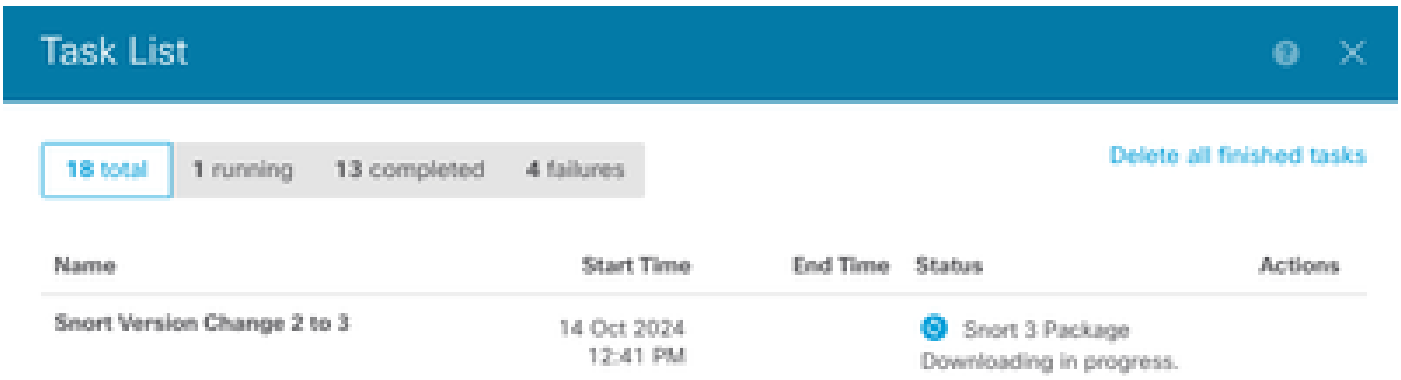


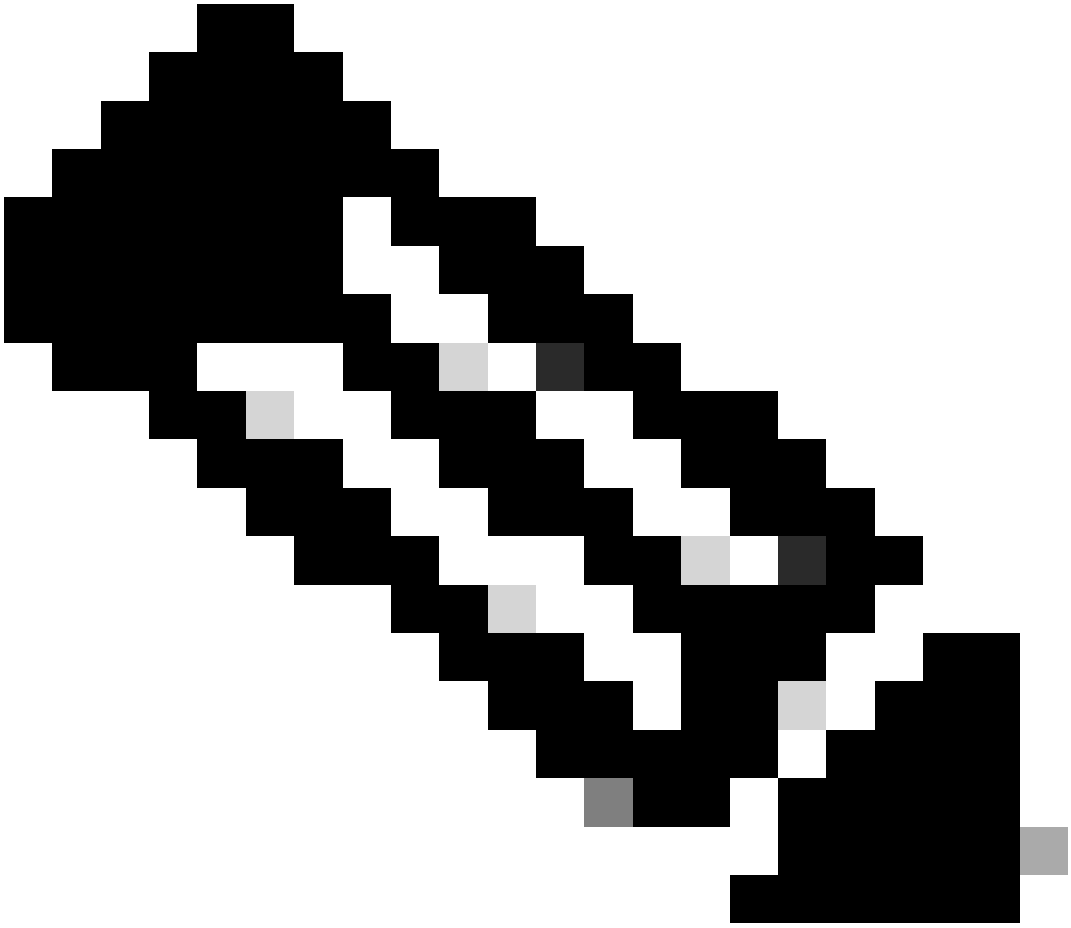
Opmerking: het systeem downloadt alleen pakketten voor de actieve Snort-versie, dus het is onwaarschijnlijk dat u het laatste pakket geïnstalleerd heeft voor de Snort-versie waarop u overschakelt. U moet wachten totdat de switch-versies van de taak zijn voltooid voordat u het inbraakbeleid kunt bewerken.



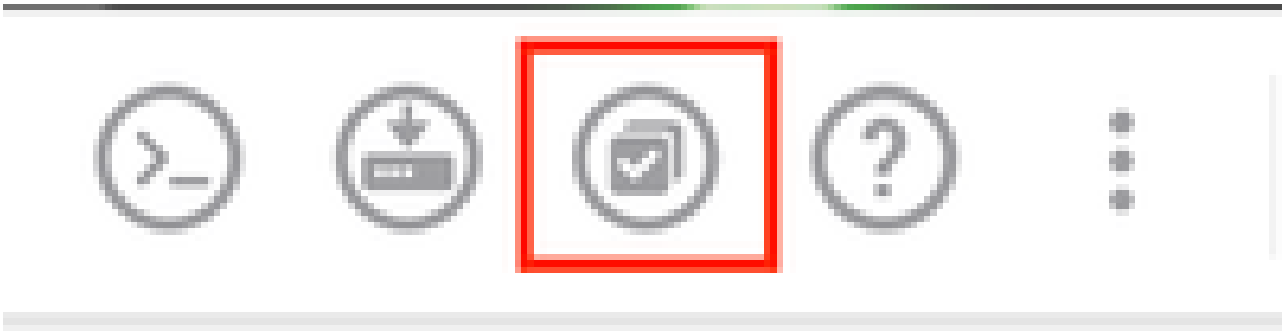
Waarschuwing: Schakelen tussen snort versie leidt tot tijdelijk verkeersverlies.

5. U moet in de taaklijst bevestigen dat de upgrade is gestart.



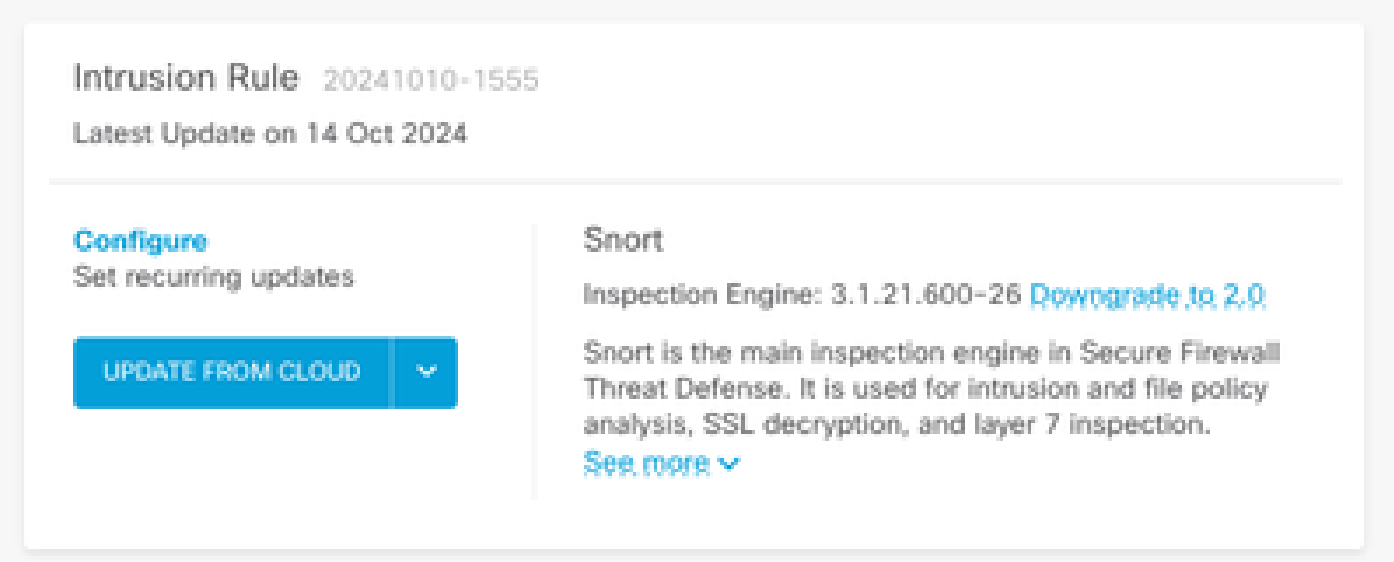


Opmerking: de taaklijst staat in de navigatiebalk naast het pictogram implementaties.

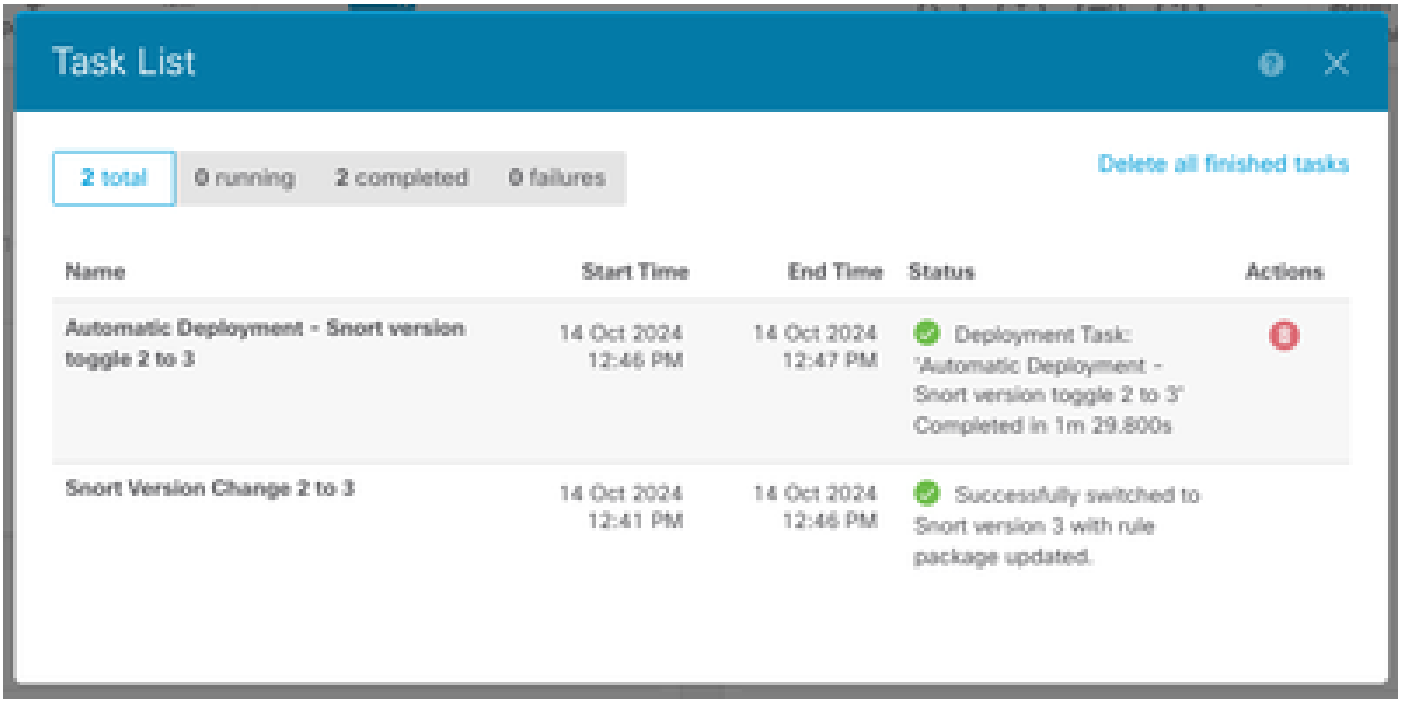


Verifiëren

De sectie Inspection Engine laat zien dat de huidige versie van Snort Snort 3 is.



Zorg er tot slot in de taaklijst voor dat de wijziging in snurk 3 met succes is voltooid en geïmplementeerd.



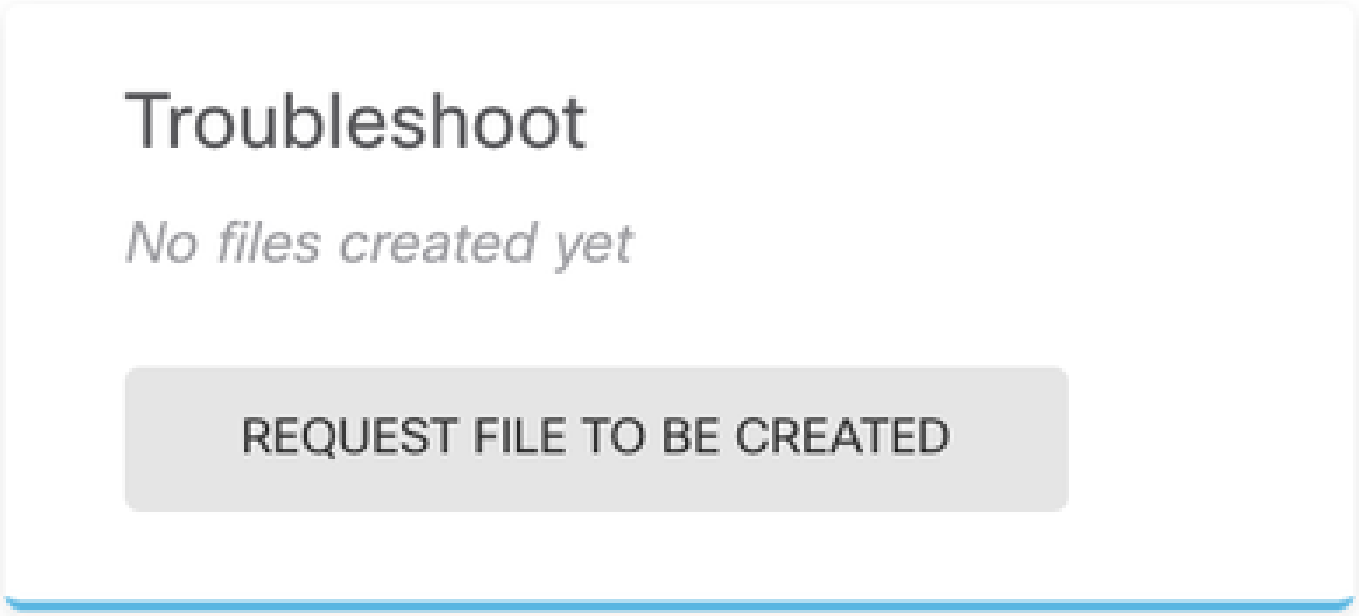
Problemen oplossen

Als u tijdens de upgrade problemen ondervindt, neemt u de volgende stappen:

- Zorg ervoor dat uw FTD versies compatibel zijn met Snort 3.

Raadpleeg de Compatibiliteitsgids voor Cisco Secure Firewall Threat Defence voor meer informatie

- Verzamel de probleemoplossingsbestanden op de FDM door naar het tabblad Apparaat te navigeren en vervolgens op Aanvraagbestand te klikken. Zodra verzameld, open een case met TAC en upload het bestand naar de case voor verdere assistentie.



Gerelateerde informatie

- SNORT 3-adoptie
- Documenten snurken
- Configuratiehandleiding voor Cisco Secure Firewall Device Manager, versie 7.2

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.