Actualización de Snort 2 a Snort 3 mediante FDM

Contenido

Introducción

Este documento describe cómo actualizar desde la versión 2 de Snort a la versión 3 de Snort en Firepower Device Manager (FDM).

Prerequisites

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defense (FTD)
- Administrador de dispositivos Firepower (FDM)
- Snort.

Requirements

Asegúrese de que tiene los siguientes requisitos:

- Acceso al administrador de dispositivos Firepower.
- Privilegios administrativos en FDM.
- FTD debe ser al menos la versión 6.7 para poder utilizar snort 3.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- FTD 7.2.7

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

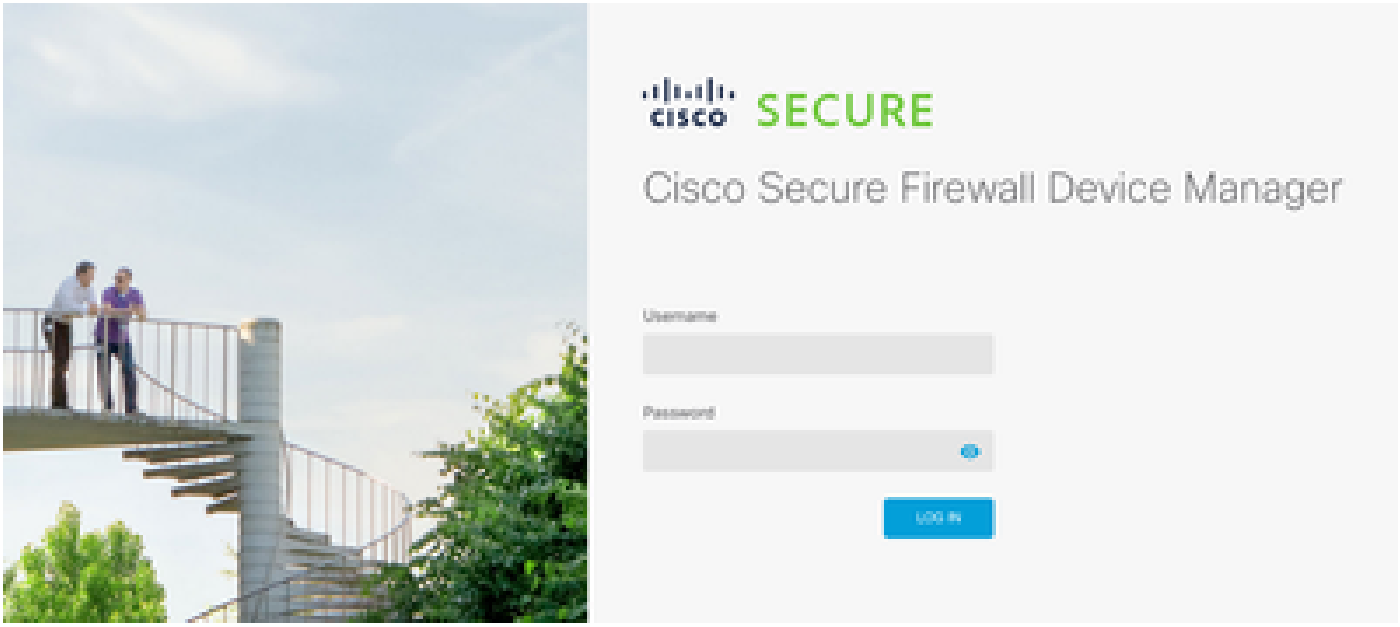
La función snort 3 se añadió en la versión 6.7 para Firepower Device Manager (FDM). Snort 3.0 se ha diseñado para hacer frente a estos retos:

- Reduzca el uso de memoria y CPU.
- Mejore la eficacia de la inspección HTTP.
- Carga de configuración más rápida y reinicio de snort.
- Mejor programabilidad para una incorporación más rápida de funciones.

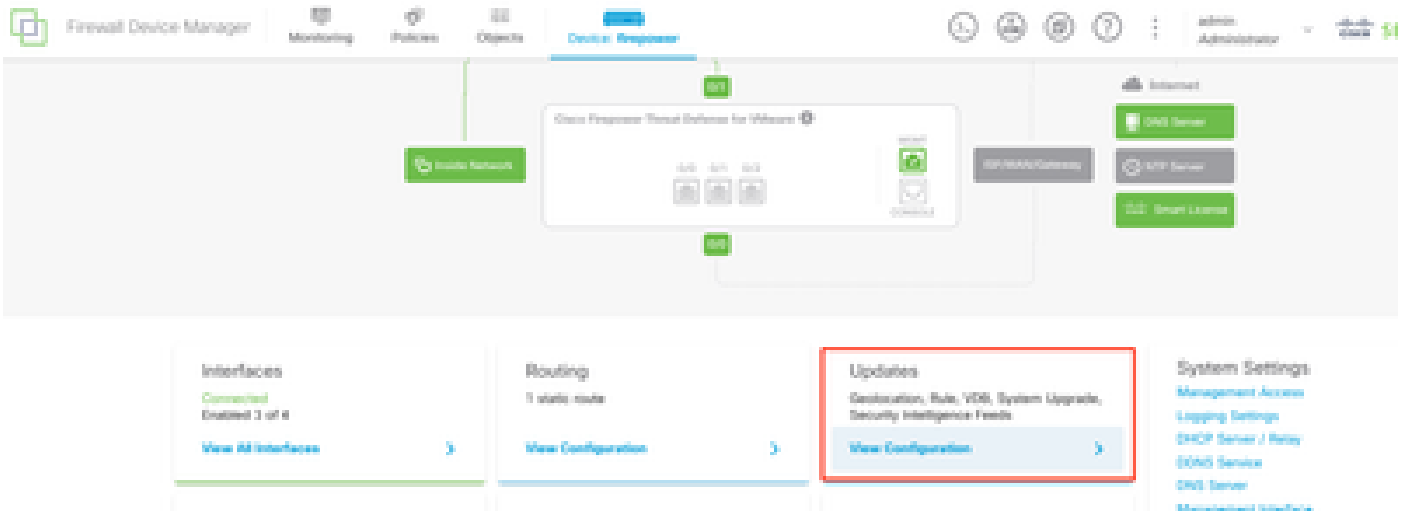
Configurar

Configuraciones

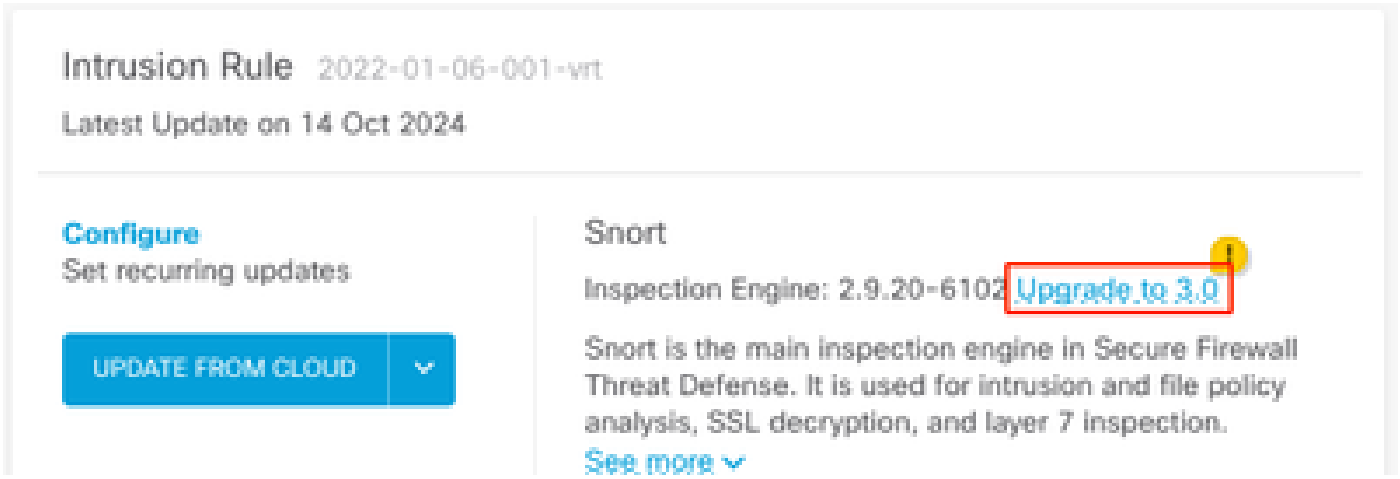
1. Inicie sesión en Firepower Device Manager.



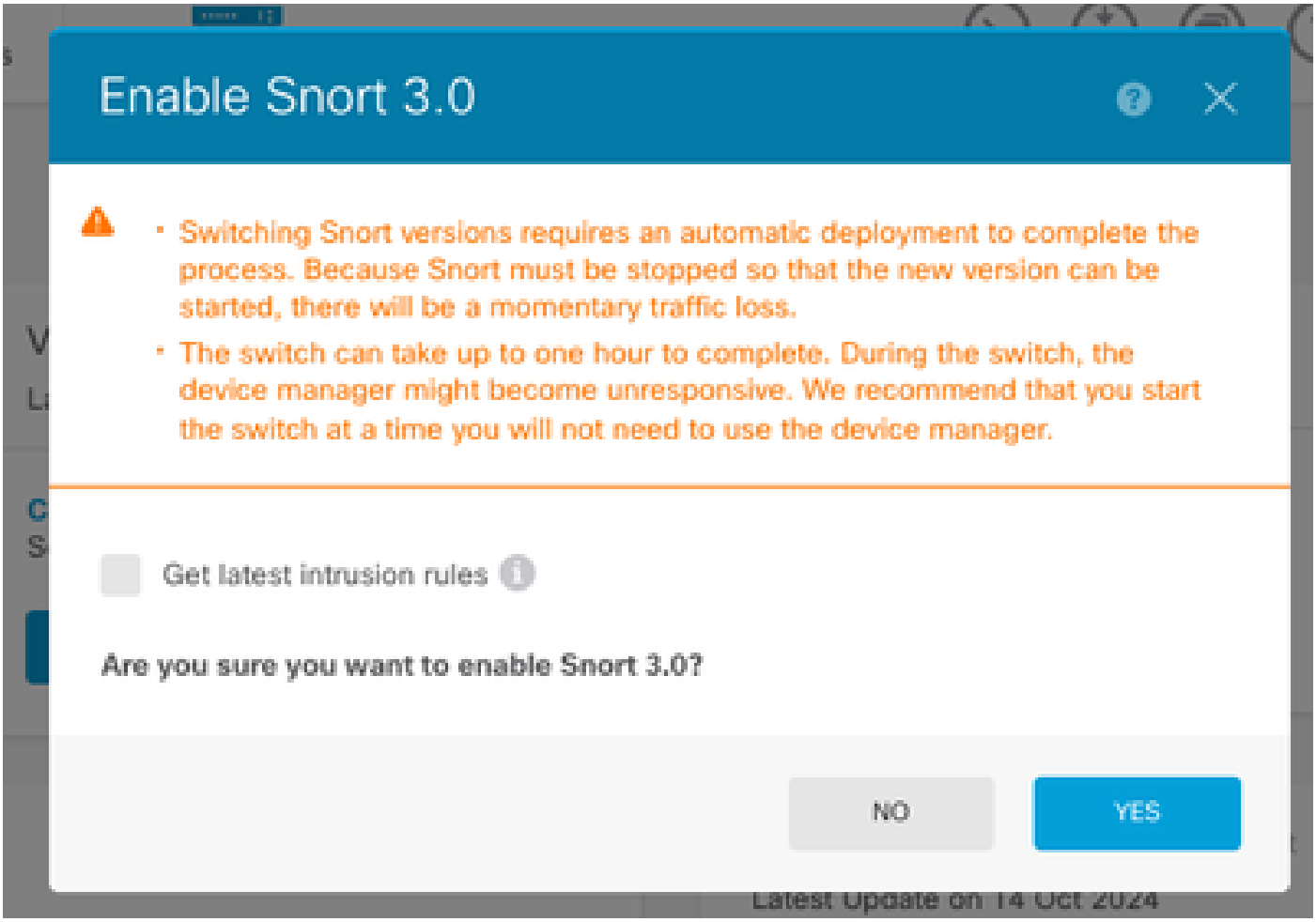
2. Vaya a Dispositivo > Actualizaciones > Ver configuración.

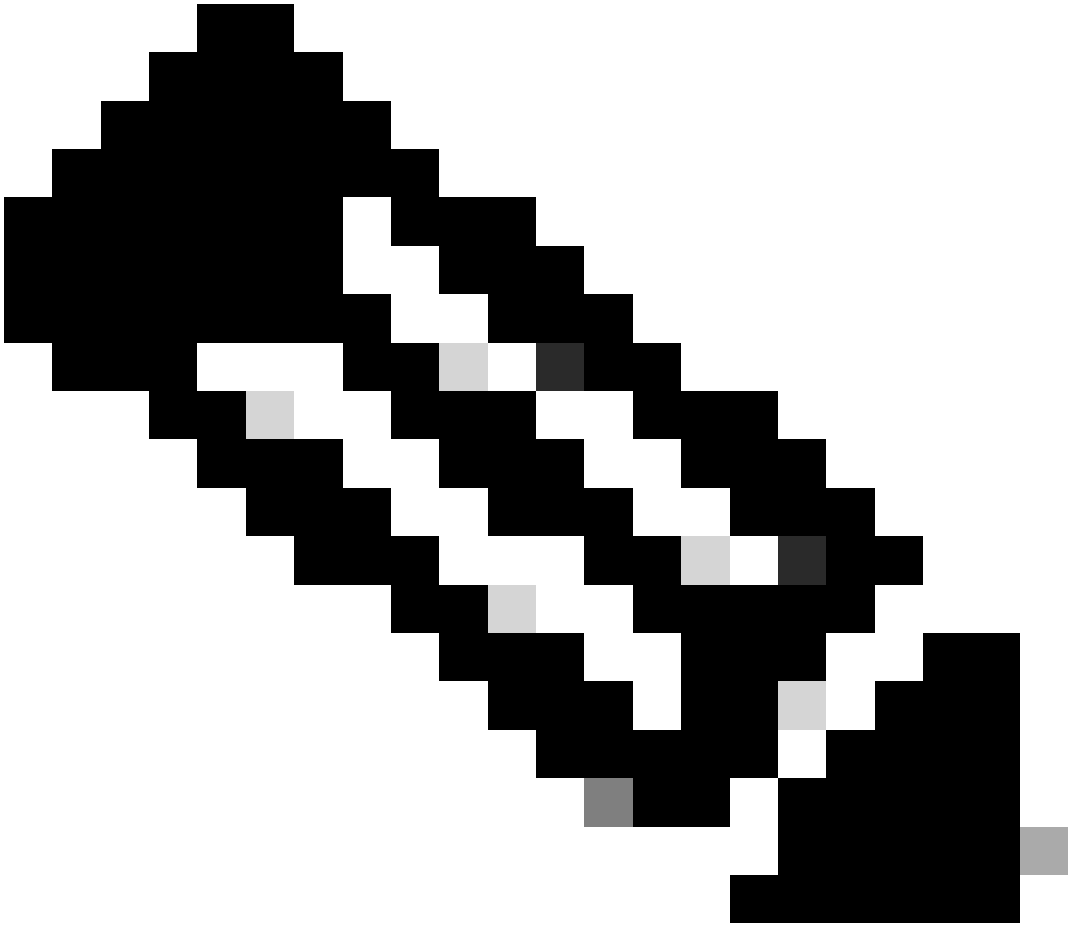


3. En la sección de reglas de intrusión, haga clic en actualizar a snort 3.



4. En el mensaje de advertencia para confirmar la selección, seleccione la opción para obtener el paquete de reglas de intrusión más reciente y, a continuación, haga clic en Sí.

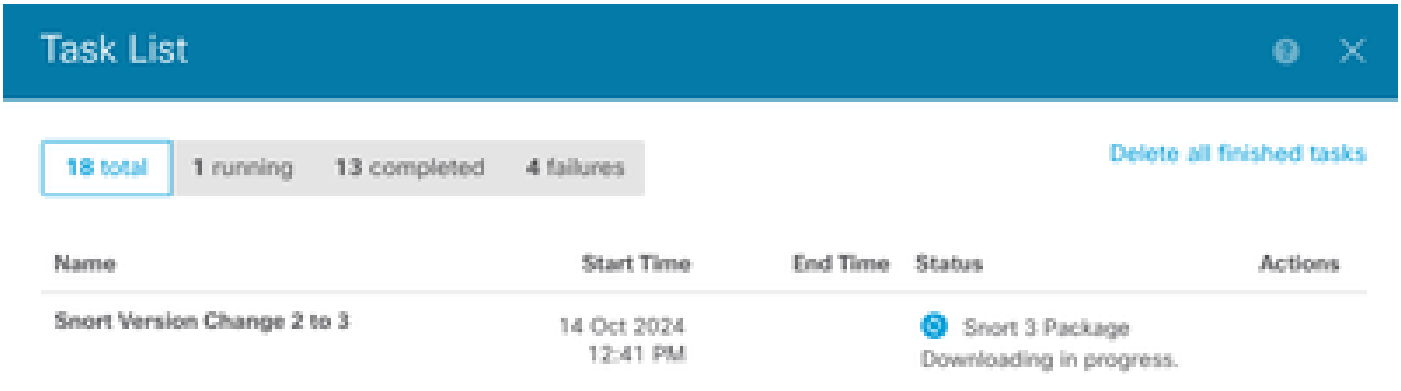

Enable Snort 3.0
Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
The switch can take up to one hour to complete. During the switch, the device manager might 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



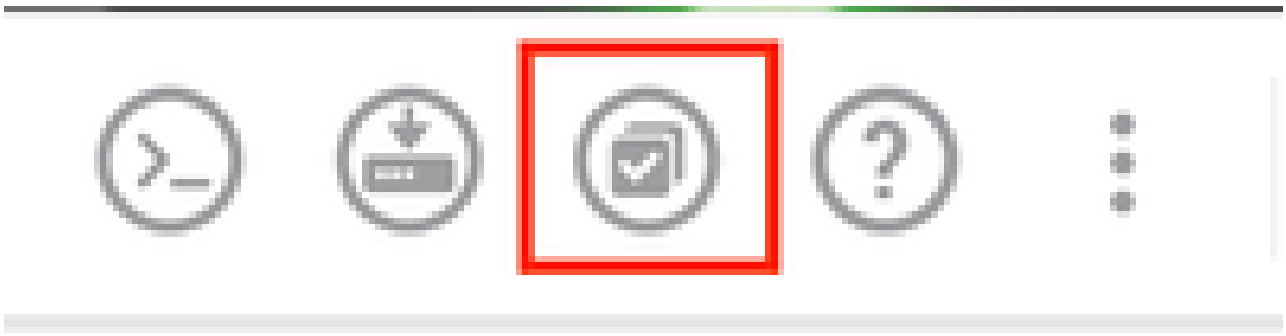
Nota: El sistema descarga paquetes sólo para la versión activa de Snort, por lo que es poco probable que tenga instalado el paquete más reciente para la versión de Snort a la que está cambiando. Debe esperar hasta que se complete la tarea de cambio de versión antes de poder editar las directivas de intrusión.

Advertencia: el cambio de la versión del snort provoca una pérdida momentánea del tráfico.

5. Debe confirmar en la lista de tareas que se ha iniciado la actualización.

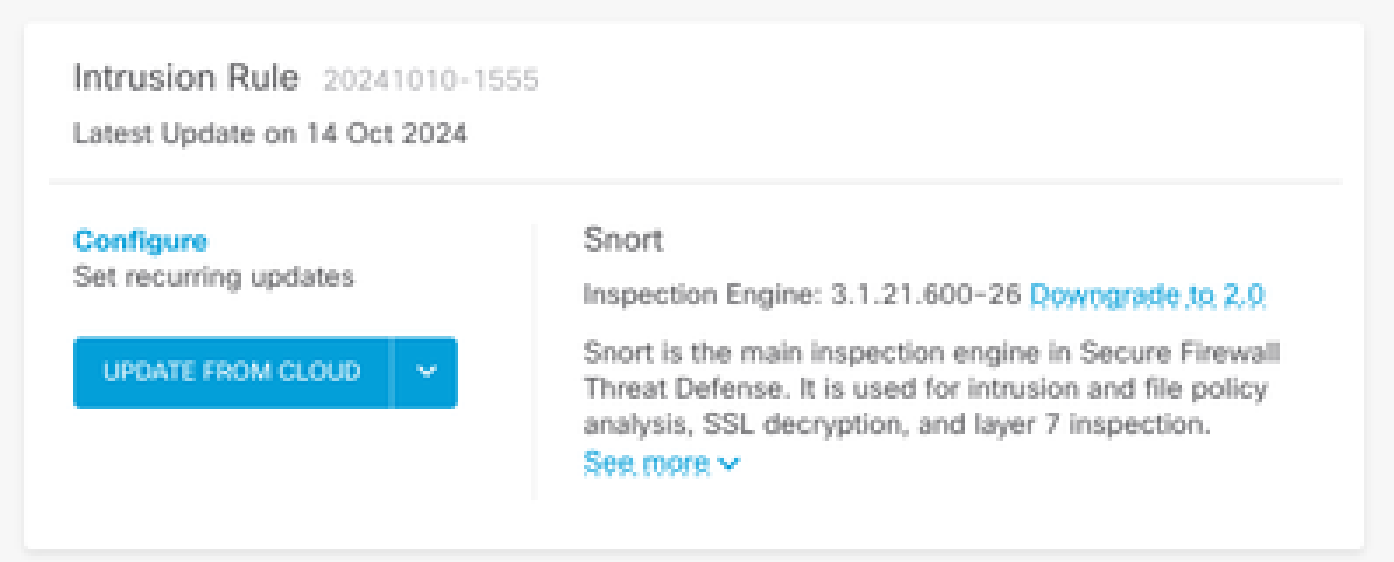


Nota: La lista de tareas se encuentra en la barra de navegación junto al icono de despliegues.

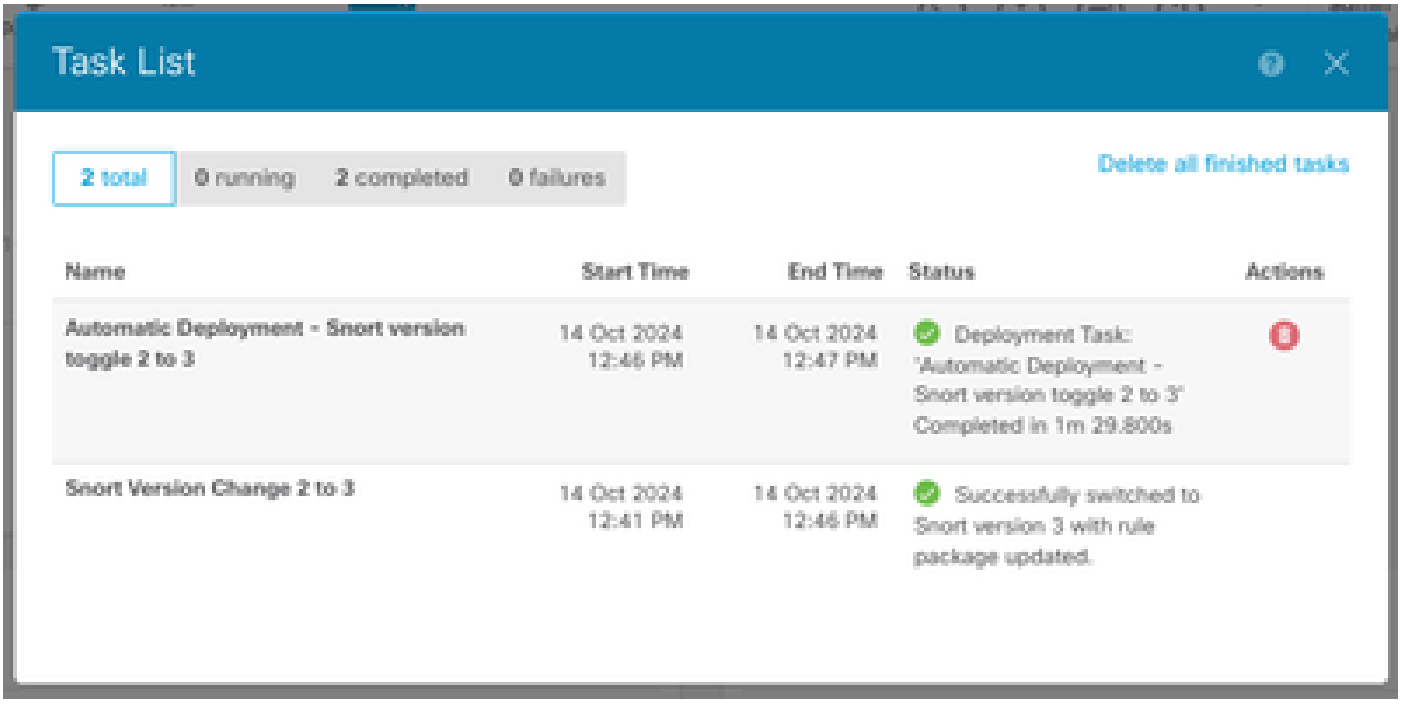


Verificación

La sección Motor de inspección muestra que la versión actual de Snort es Snort 3.



Por último, en la lista de tareas, asegúrese de que el cambio a snort 3 se ha completado e implementado correctamente.



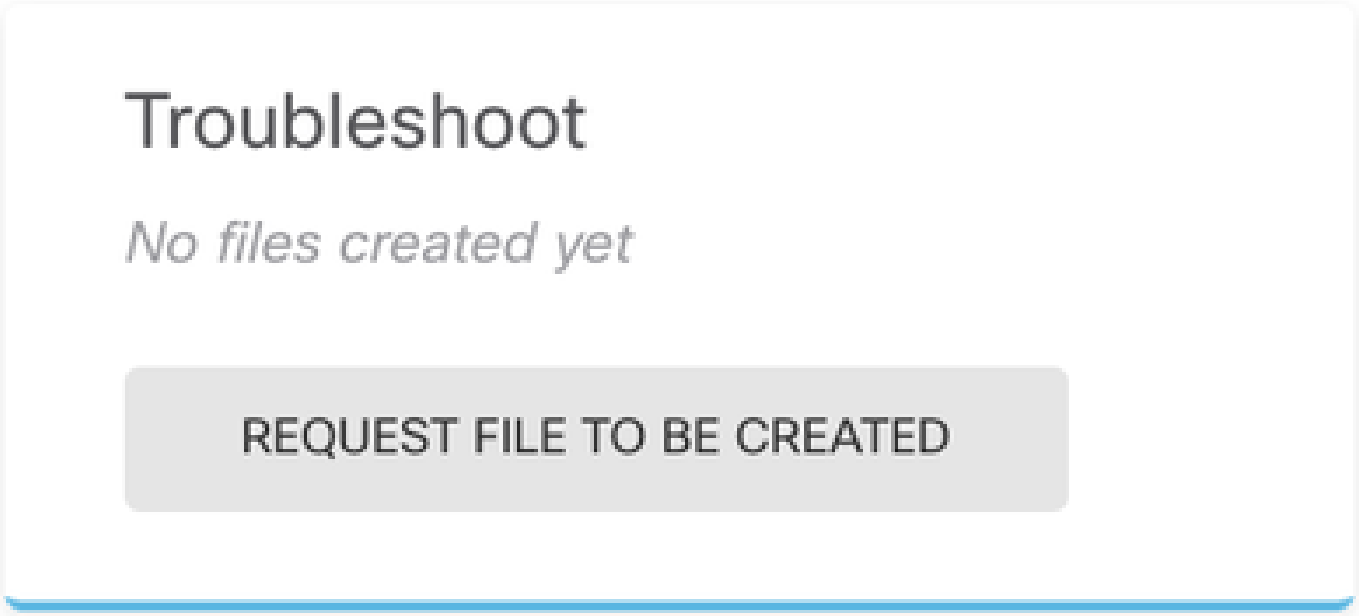
Troubleshoot

Si experimenta problemas durante la actualización, tenga en cuenta estos pasos:

- Asegúrese de que sus versiones de FTD son compatibles con Snort 3.

Para obtener más información, consulte la Guía de compatibilidad de Cisco Secure Firewall Threat Defence

- Recopile los archivos de solución de problemas en FDM navegando a la pestaña Device y luego haciendo clic en Request file to be create. Una vez recopilado, abra un caso con el TAC y cargue el archivo en el caso para obtener más ayuda.



Información Relacionada

- Adopción de Snort 3
- Snort Documents
- Guía de configuración de Cisco Secure Firewall Device Manager, versión 7.2

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).