

透過FDM從Snort 2升級到Snort 3

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[背景資訊](#)

[設定](#)

[組態](#)

[驗證](#)

[疑難排解](#)

[相關資訊](#)

簡介

本檔案介紹如何在Firepower裝置管理員(FDM)中從snort 2升級到Snort 3版本。

必要條件

思科建議您瞭解以下主題：

- Firepower Threat Defense (FTD)
- Firepower裝置管理器(FDM)
- Snort。

需求

確保滿足以下要求：

- 訪問Firepower裝置管理器。
- FDM的管理許可權。
- FTD必須至少為6.7版才能使用snort 3。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- FTD 7.2.7

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

背景資訊

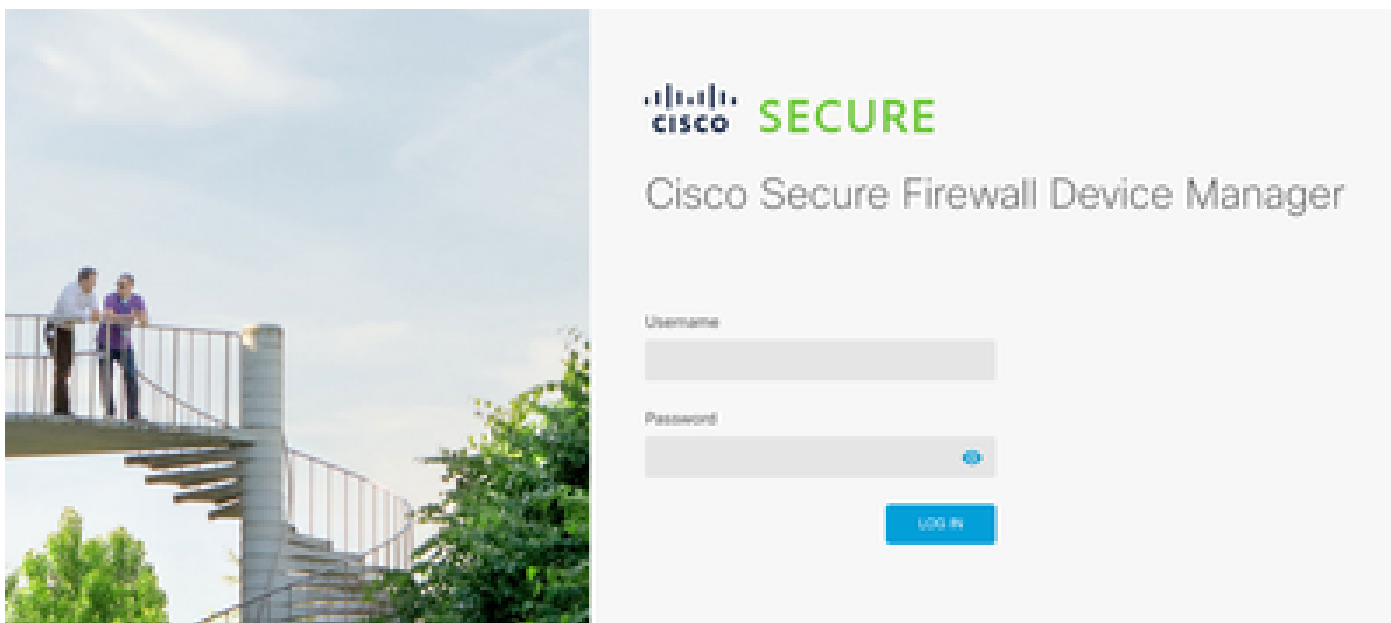
Firepower裝置管理器(FDM)的6.7版本中增加了snort 3功能。Snort 3.0旨在解決以下挑戰：

- 減少記憶體和CPU使用量。
- 提高HTTP檢查效率。
- 更快的配置載入和Snort重新啟動。
- 更佳的可程式設計性，加快功能增加速度。

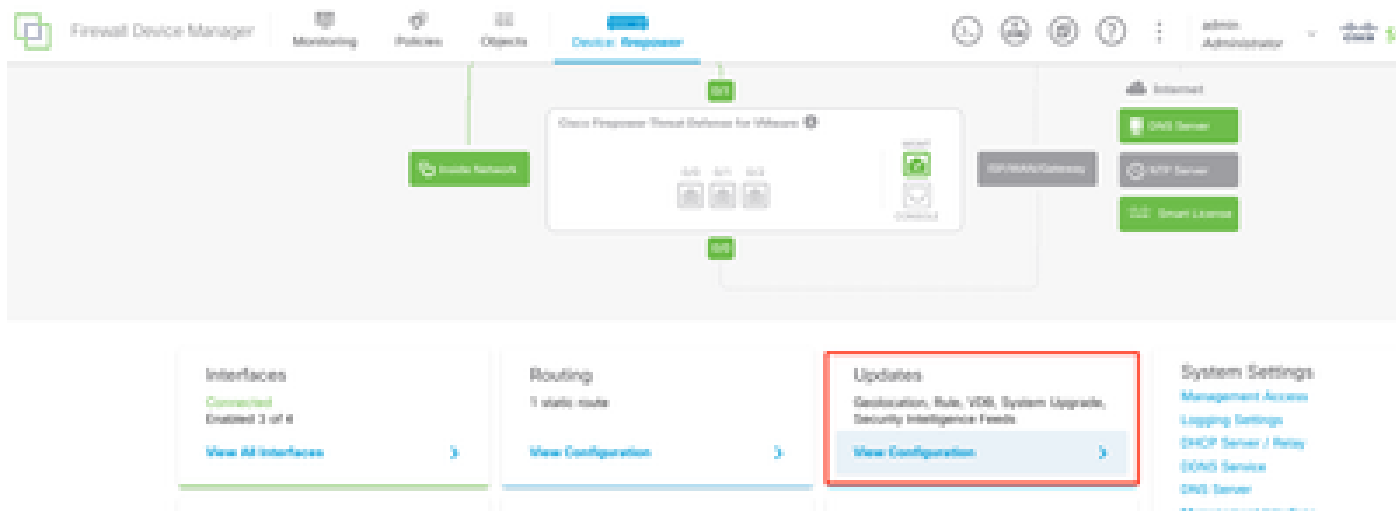
設定

組態

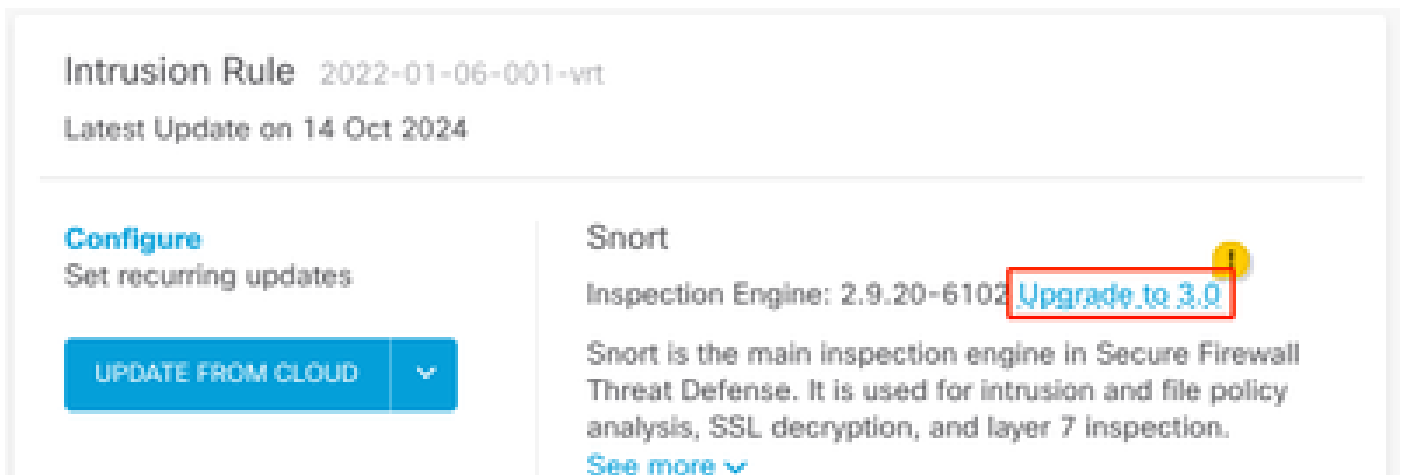
1. 登入Firepower裝置管理器。



2. 導航到裝置>更新>檢視配置。



3. 在intrusion rules部分中，按一下upgrade to snort 3。



Intrusion Rule 2022-01-06-001-vrt
Latest Update on 14 Oct 2024

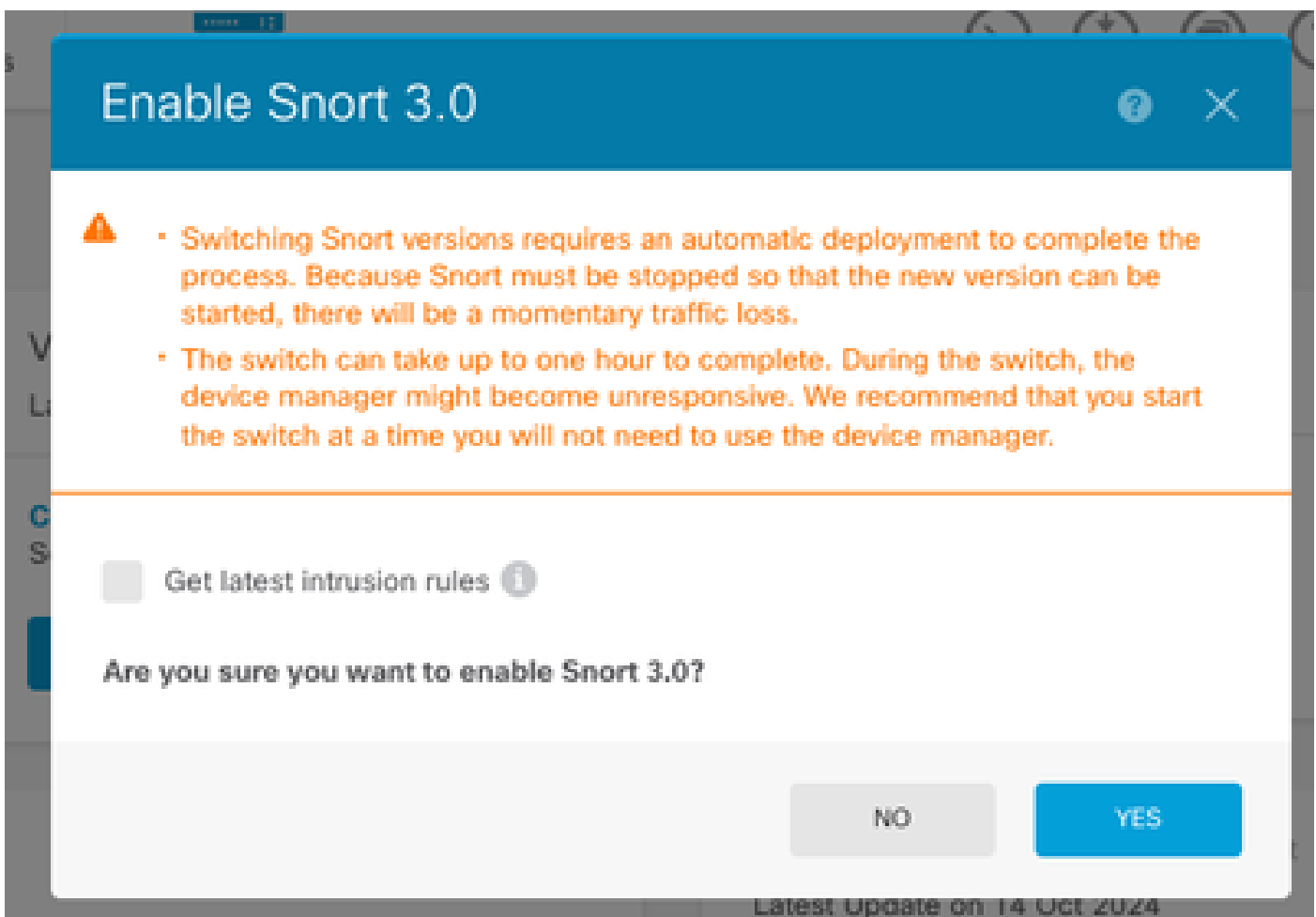
Configure
Set recurring updates

UPDATE FROM CLOUD ▾

Snort
Inspection Engine: 2.9.20-6102 **Upgrade to 3.0**

Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.
[See more](#) ▾

4. 在確認選擇的警告消息上，選擇獲取最新入侵規則包的選項，然後按一下Yes。



Enable Snort 3.0 ⓘ ✕

⚠

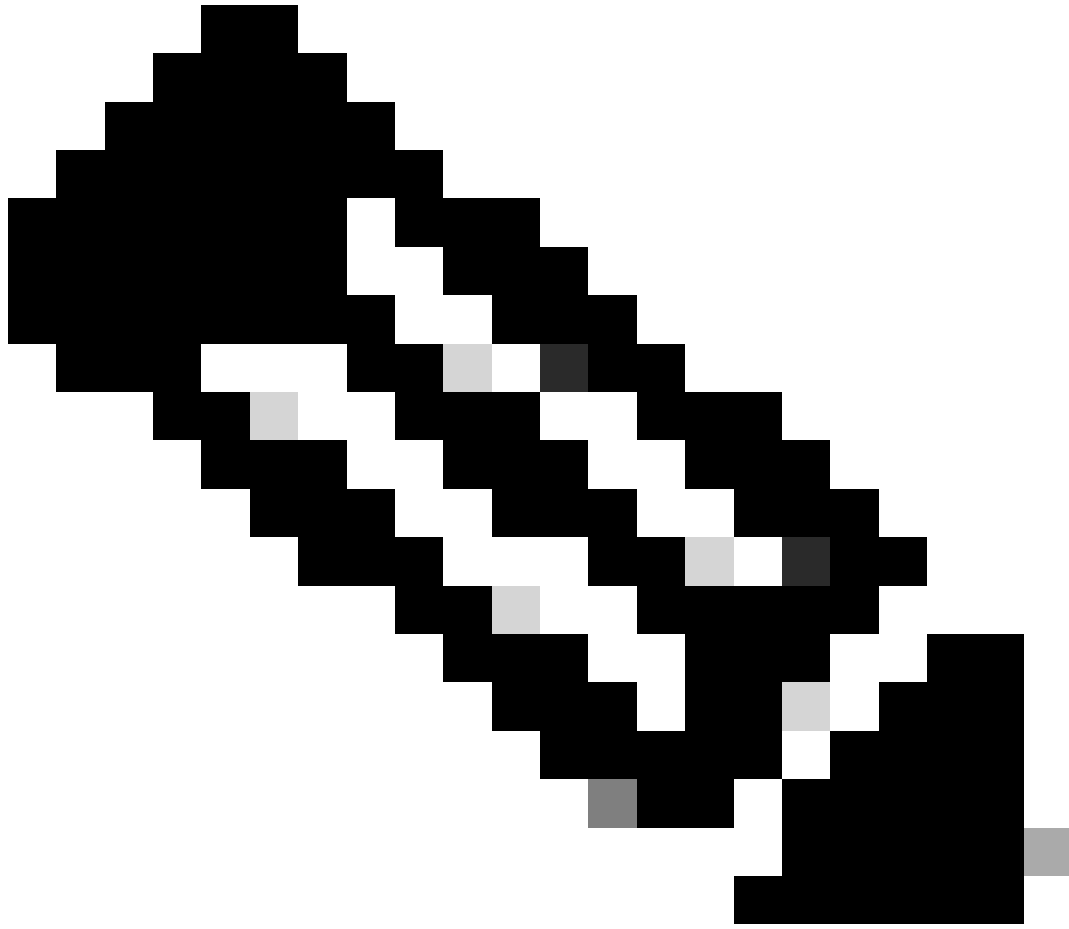
- Switching Snort versions requires an automatic deployment to complete the process. Because Snort must be stopped so that the new version can be started, there will be a momentary traffic loss.
- The switch can take up to one hour to complete. During the switch, the device manager might become unresponsive.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



注意：系統僅下載活動Snort版本的軟體套件，因此您安裝用於切換目標的Snort版本的最新軟體套件的可能性不大。必須等到切換版本的任務完成，才能編輯入侵策略。



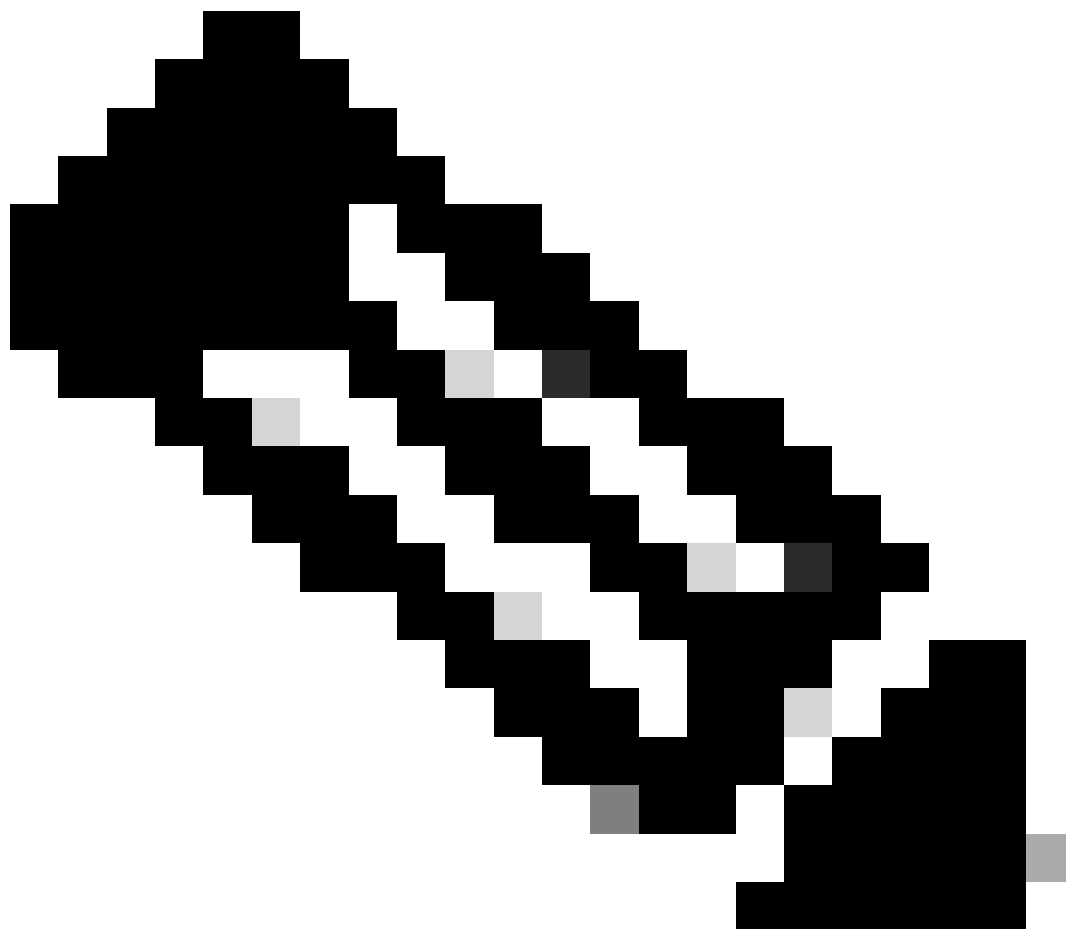
警告：交換snort版本會導致瞬時流量丟失。

5. 您必須在作業清單中確認已開始升級。

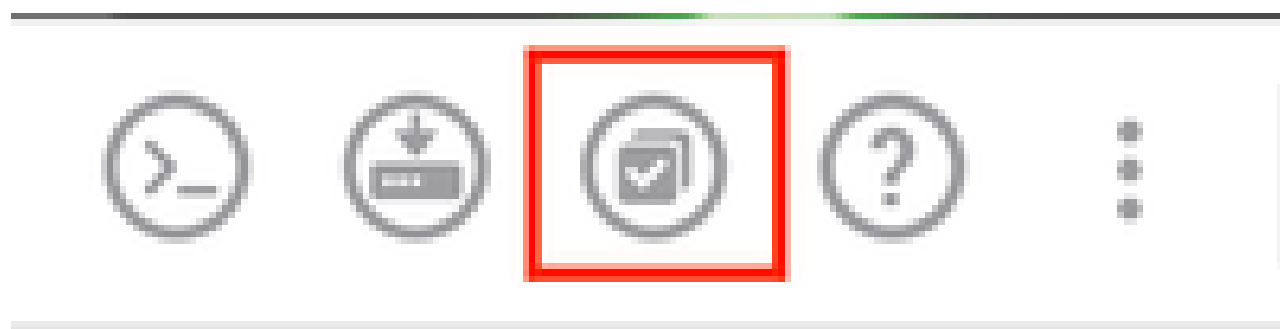
Task List

18 total | 1 running | 13 completed | 4 failures [Delete all finished tasks](#)

Name	Start Time	End Time	Status	Actions
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM		Snort 3 Package Downloading in progress.	



附註：工作清單位於建置圖示旁的導覽列中。



驗證

「檢測引擎」部分顯示Snort的當前版本為Snort 3。

Intrusion Rule 20241010-1555

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

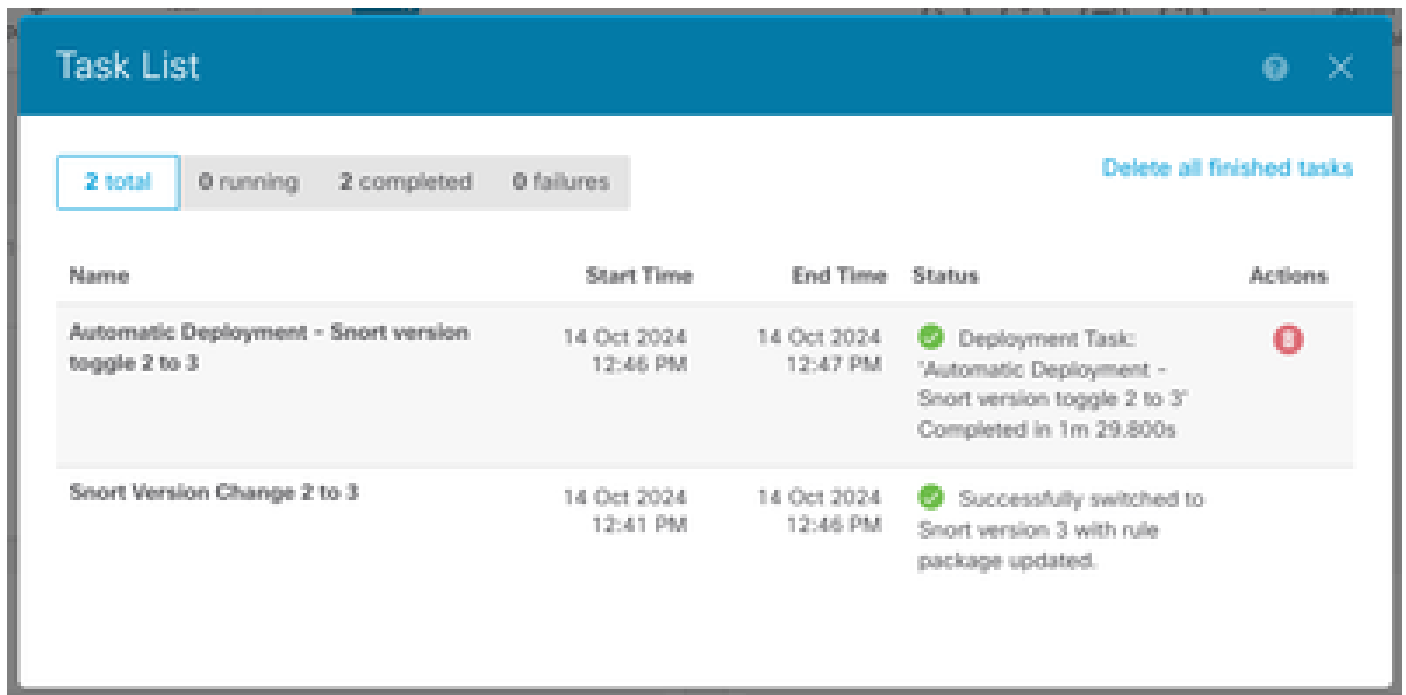
Snort

Inspection Engine: 3.1.21.600-26 [Downgrade to 2.0](#)

Snort is the main inspection engine in Secure Firewall Threat Defense. It is used for intrusion and file policy analysis, SSL decryption, and layer 7 inspection.

[See more](#)

最後，在工作清單中，確保已成功完成並部署對snort 3的更改。



The screenshot shows a 'Task List' window with a blue header. Below the header, there are filters for task counts: 2 total, 0 running, 2 completed, and 0 failures. A 'Delete all finished tasks' link is visible on the right. The main area contains a table with columns for Name, Start Time, End Time, Status, and Actions. Two tasks are listed, both with a green checkmark icon indicating completion.

Name	Start Time	End Time	Status	Actions
Automatic Deployment - Snort version toggle 2 to 3	14 Oct 2024 12:46 PM	14 Oct 2024 12:47 PM	✔ Deployment Task: 'Automatic Deployment - Snort version toggle 2 to 3' Completed in 1m 29.800s	🗑️
Snort Version Change 2 to 3	14 Oct 2024 12:41 PM	14 Oct 2024 12:46 PM	✔ Successfully switched to Snort version 3 with rule package updated.	

疑難排解

如果在升級期間遇到問題，請考慮以下步驟：

- 確認您的FTD版本與Snort 3相容。

有關其他詳細資訊，請檢視[Cisco安全防火牆威脅防禦相容性指南](#)

- 導航到裝置頁籤，然後點選請求建立檔案，收集FDM上的故障排除檔案。收集後，使用TAC開啟案件並上傳檔案至案件以尋求進一步協助。

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

相關資訊

- [Snort 3採用](#)
- [Snort檔案](#)
- [思科安全防火牆裝置管理器配置指南7.2版](#)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。