

Upgrade von Snort 2 auf Snort 3 über FDM

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Konfigurationen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie im FirePOWER Geräte-Manager (FDM) ein Upgrade von der Version snort 2 auf die Version snort 3 durchführen.

Voraussetzungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Firepower Threat Defense (FTD)
- FirePOWER-Gerätemanager (FDM)
- Snort.

Anforderungen

Stellen Sie sicher, dass Sie die folgenden Anforderungen erfüllen:

- Zugriff auf den FirePOWER Geräte-Manager
- Administratorberechtigungen für den FDM.
- FTD muss mindestens Version 6.7 sein, damit snort 3 verwendet werden kann.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- FTD 7.2.7

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten

Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

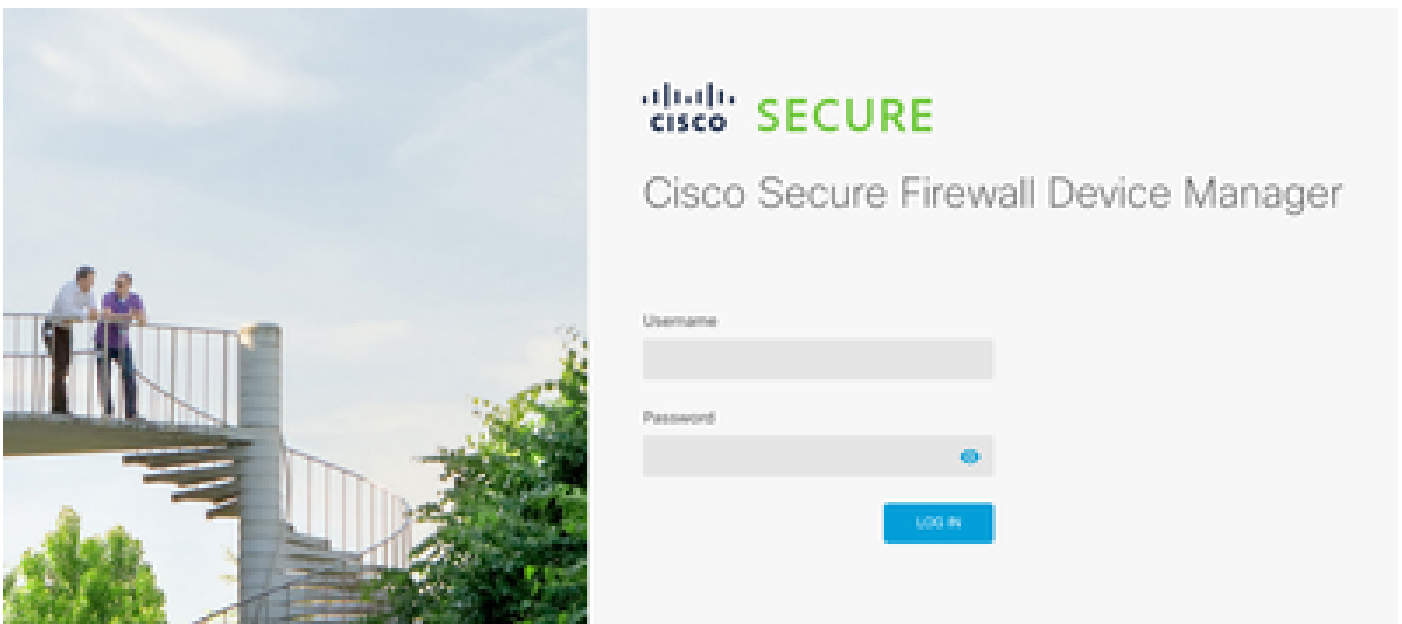
Die Funktion snort 3 wurde in Version 6.7 für den FirePOWER-Geräte-Manager (FDM) hinzugefügt. Snort 3.0 wurde für folgende Herausforderungen entwickelt:

- Reduzierung der Arbeitsspeicher- und CPU-Auslastung
- Verbesserung der Effizienz von HTTP-Prüfungen.
- Schnelleres Laden von Konfigurationen und Neustart von Snort.
- Bessere Programmierbarkeit für schnellere Funktionsbereitstellung

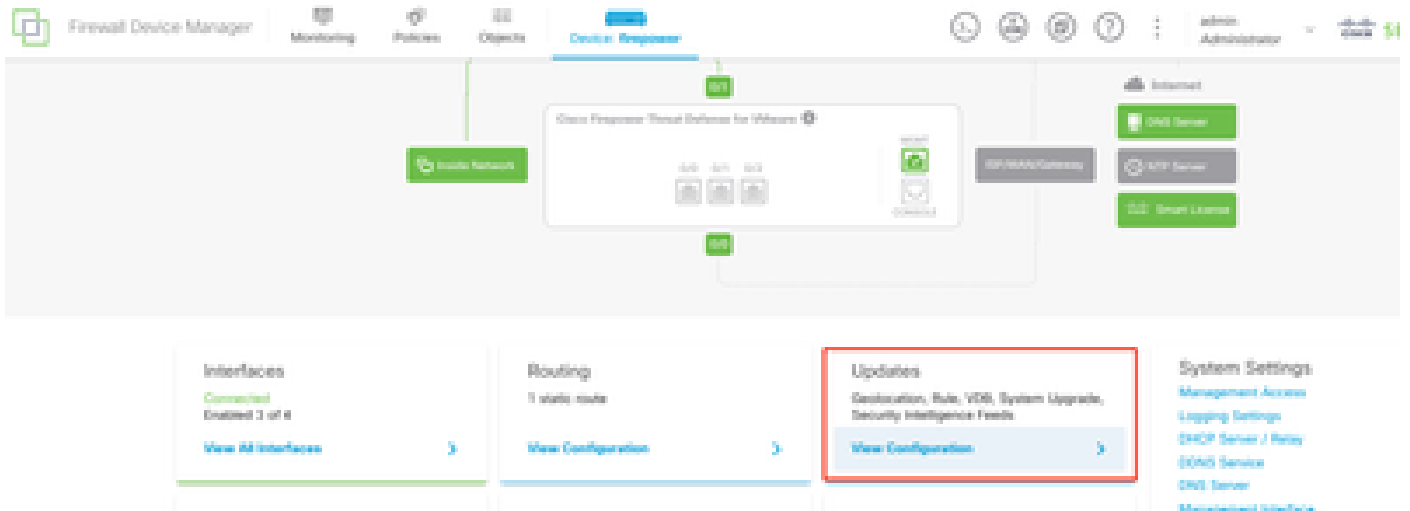
Konfigurieren

Konfigurationen

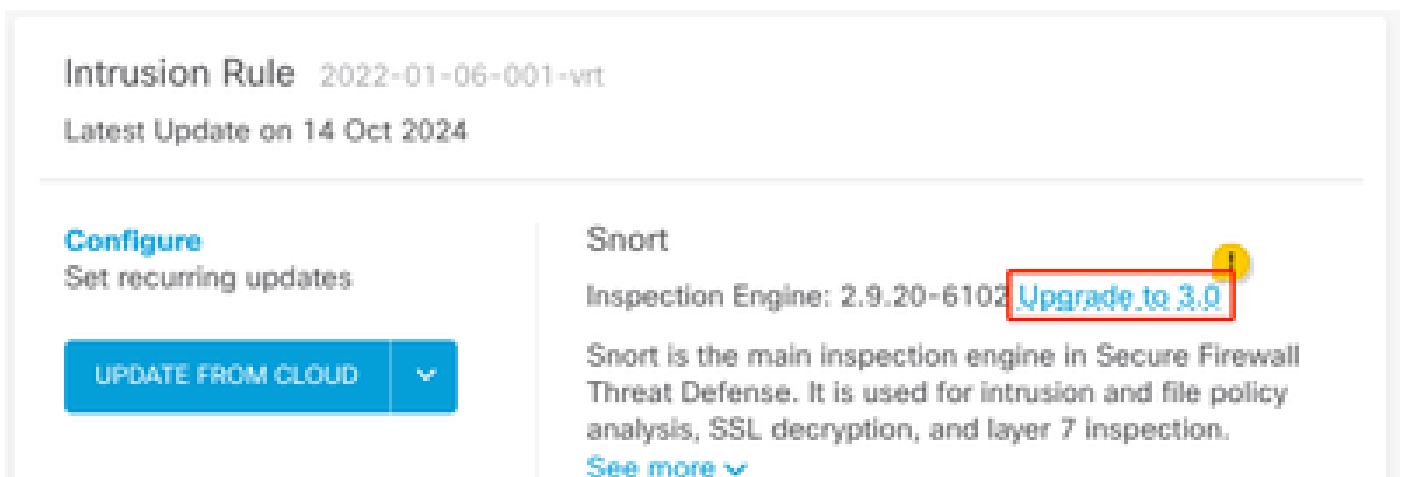
1. Melden Sie sich beim FirePOWER Geräte-Manager an.



2. Navigieren Sie zu Gerät > Updates > Konfiguration anzeigen.



3. Klicken Sie im Abschnitt Intrusion rules (Angriffsregeln) auf upgrade (Aktualisieren), um 3 zu snort.



4. Wählen Sie in der Warnmeldung zur Bestätigung Ihrer Auswahl die Option, um das neueste Paket mit den Angriffsregeln zu erhalten, und klicken Sie dann auf 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



Hinweis: Das System lädt nur Pakete für die aktive Snort-Version herunter, daher ist es unwahrscheinlich, dass Sie das neueste Paket für die Snort-Version installiert haben, zu der Sie wechseln. Sie müssen warten, bis die Aufgabe zum Wechseln der Versionen abgeschlossen ist, bevor Sie Angriffsrichtlinien bearbeiten können.



Warnung: Switching-Snort-Version führt zu kurzzeitigem Datenverlust.

5. Sie müssen in der Aufgabenliste bestätigen, dass das Upgrade gestartet wurde.

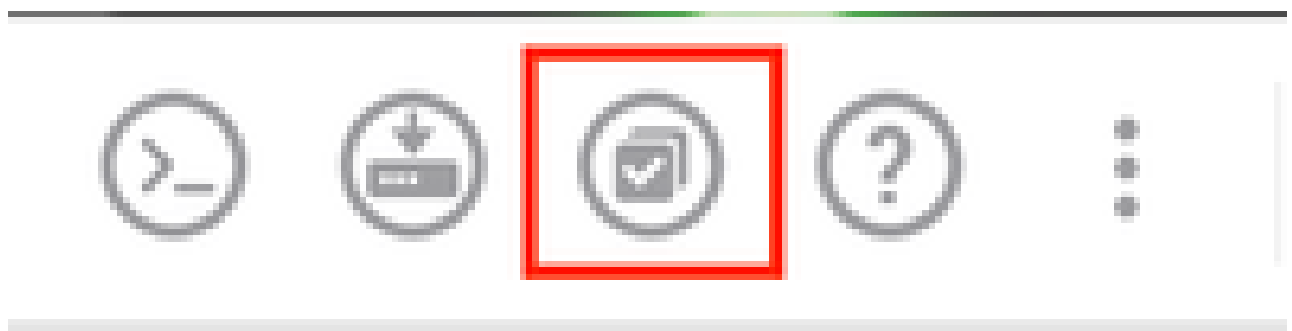
Task List

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.	



Hinweis: Die Aufgabenliste befindet sich in der Navigationsleiste neben dem Symbol für Bereitstellungen.



Überprüfung

Der Abschnitt Inspection Engine zeigt, dass die aktuelle Version von Snort Snort 3 ist.

Intrusion Rule 20241010-1555

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

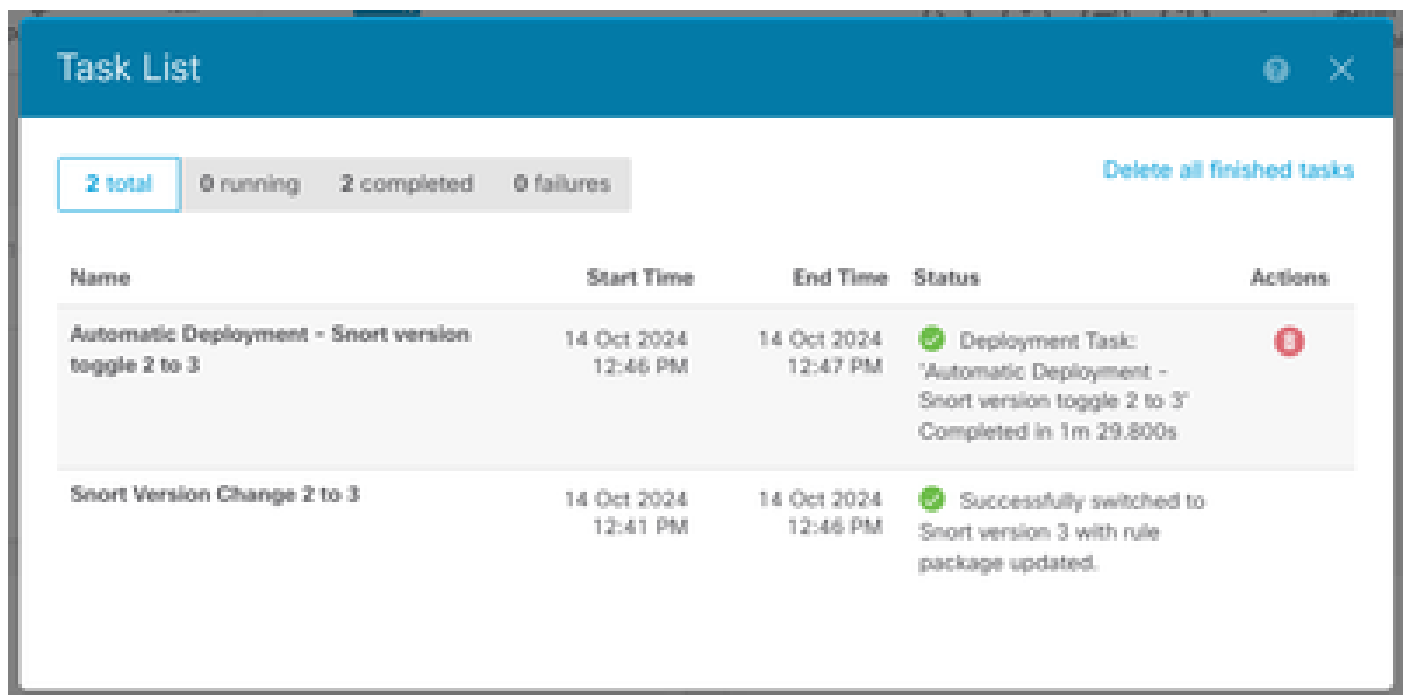
Snort

Inspection Engine: 3.1.21.600-26 [Downgrade to 2.9](#)

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](#)

Stellen Sie abschließend in der Aufgabenliste sicher, dass die Änderung von snort 3 erfolgreich abgeschlossen und bereitgestellt wurde.



The screenshot shows a 'Task List' window with a blue header. Below the header, there are filters: '2 total', '0 running', '2 completed', and '0 failures'. A 'Delete all finished tasks' link is on the right. The main area contains a table with the following data:

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.	

Fehlerbehebung

Wenn während des Upgrades Probleme auftreten, gehen Sie wie folgt vor:

- Stellen Sie sicher, dass Ihre FTD-Versionen mit Snort 3 kompatibel sind.

Weitere Informationen finden Sie im [Cisco Secure Firewall Threat Defense Compatibility Guide](#)

- Sammeln Sie die Fehlerbehebungsdateien im FDM, indem Sie zur Registerkarte Device (Gerät) navigieren und dann auf Request file to be created (Zu erstellende Datei anfordern) klicken. Öffnen Sie nach der Erfassung ein Ticket beim TAC, und laden Sie die Datei in das Ticket hoch, um weitere Unterstützung zu erhalten.

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

Zugehörige Informationen

- [Einführung von Snort 3](#)
- [Snort-Dokumente](#)
- [Konfigurationsleitfaden für Cisco Secure Firewall Device Manager, Version 7.2](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.