

Aggiornamento da Snort 2 a Snort 3 tramite FDM

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[Configurazioni](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

Introduzione

In questo documento viene descritto come eseguire l'aggiornamento dalla versione 2 alla versione 3 di Snort in Firepower Device Manager (FDM).

Prerequisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

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

Requisiti

Verificare di disporre dei seguenti requisiti:

- Accedere a Gestione periferiche di Firepower.
- Privilegi amministrativi su FDM.
- Per utilizzare lo snort 3, FTD deve essere almeno la versione 6.7.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- FTD 7.2.7

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

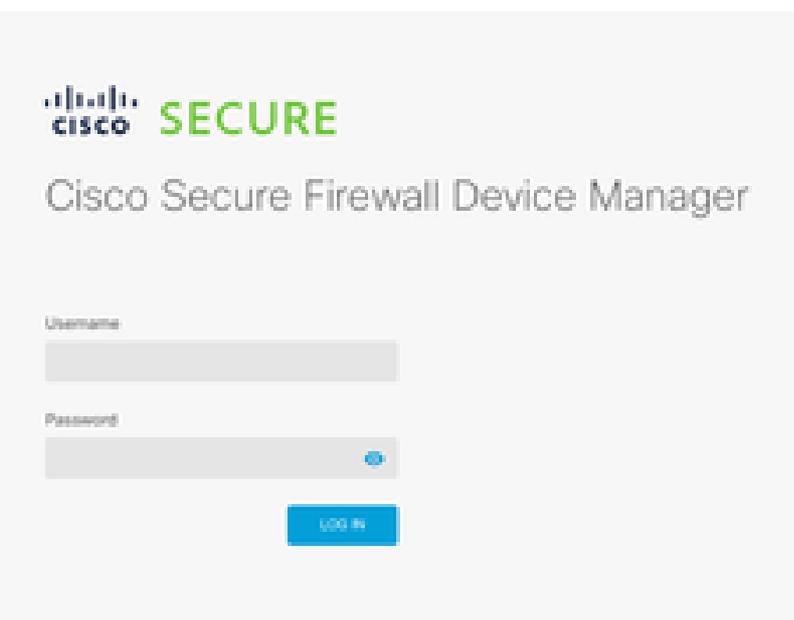
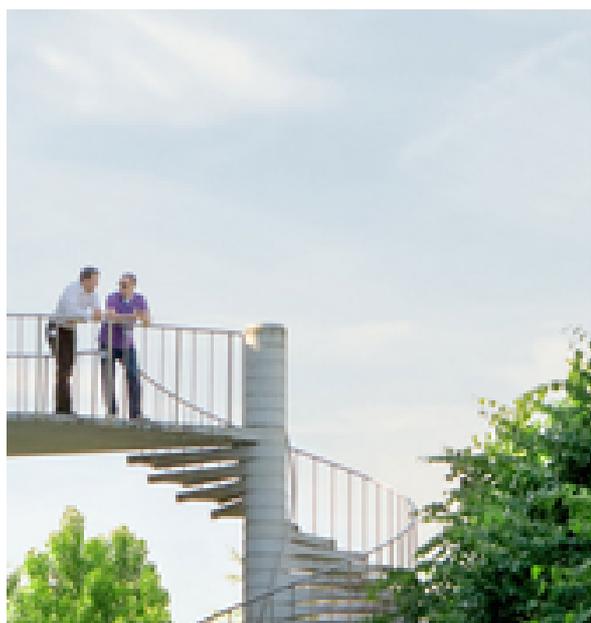
La funzione snort 3 è stata aggiunta nella versione 6.7 di Firepower Device Manager (FDM). Snort 3.0 è stato progettato per affrontare queste sfide:

- Riduzione dell'utilizzo della memoria e della CPU.
- Migliorare l'efficacia dell'ispezione HTTP.
- Caricamento più rapido della configurazione e riavvio automatico.
- Migliore programmabilità per una più rapida aggiunta di funzionalità.

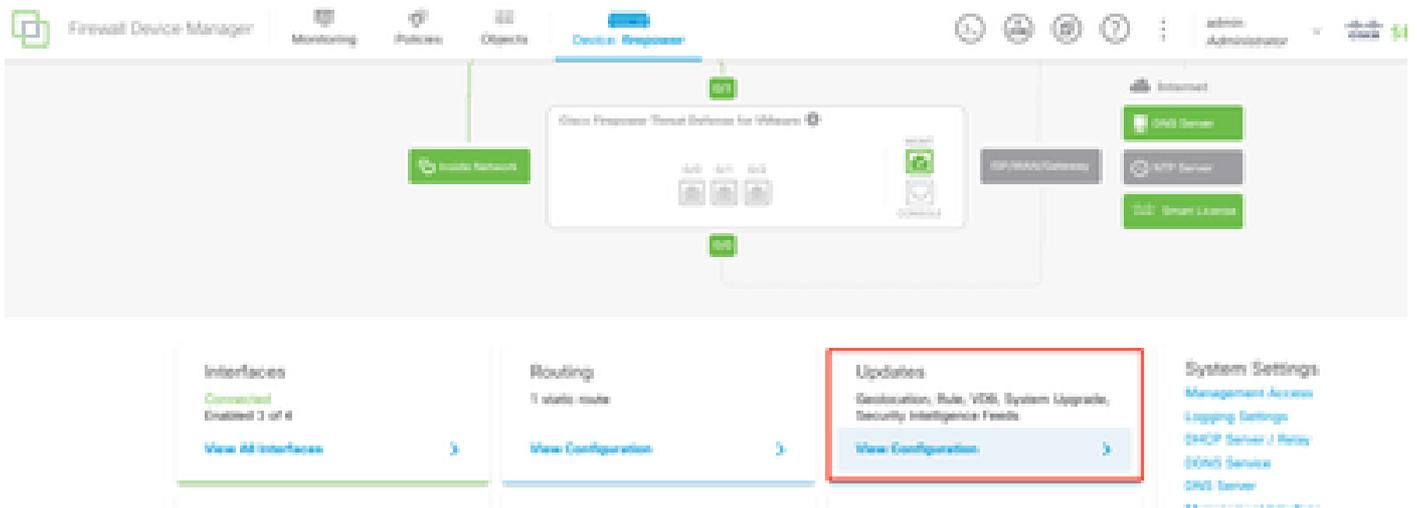
Configurazione

Configurazioni

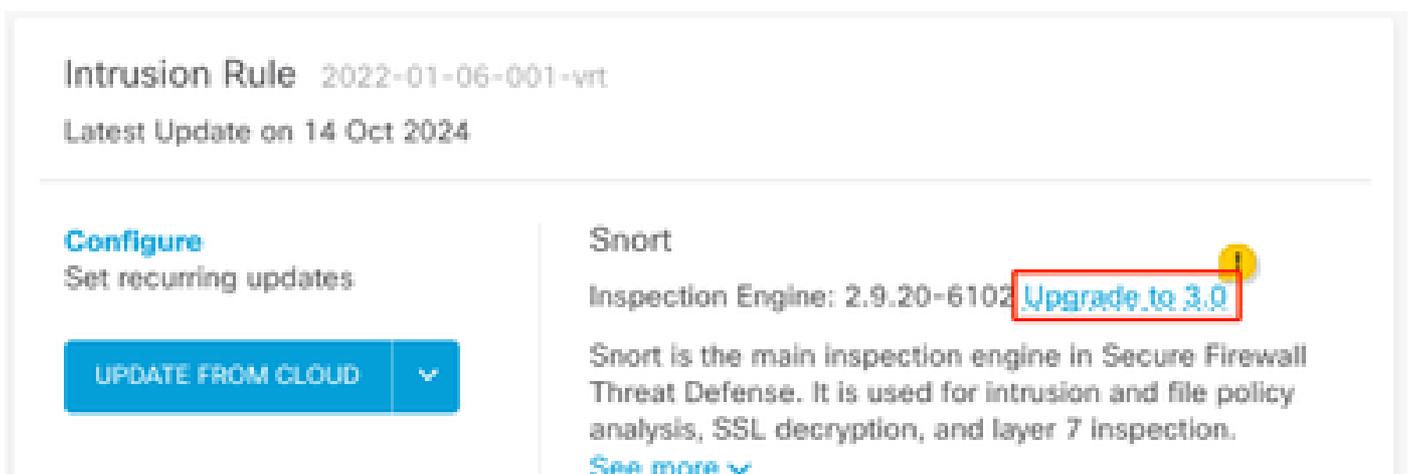
1. Accedere a Firepower Device Manager.

A screenshot of the Cisco Secure Firewall Device Manager login page. The page features the Cisco logo and the word "SECURE" in green. Below the logo, the text "Cisco Secure Firewall Device Manager" is displayed. There are two input fields: "Username" and "Password". The "Password" field has a blue eye icon to toggle visibility. A blue "LOG IN" button is located at the bottom right of the form.

2. Passare a Dispositivo > Aggiornamenti > Visualizza configurazione.



3. Nella sezione regole di intrusione, fare clic su aggiorna a snort 3.



4. Nel messaggio di avvertenza per confermare la selezione, selezionare l'opzione per ottenere il pacchetto delle regole di intrusione più recente, quindi fare clic su Sì.

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: il sistema scarica i pacchetti solo per la versione Snort attiva, quindi è improbabile che sia installata la versione più recente per la versione Snort a cui si sta passando. Prima di modificare i criteri per le intrusioni, è necessario attendere il completamento dell'attività di cambio di versione.



Avviso: la commutazione della versione snort comporta una perdita temporanea del traffico.

5. È necessario confermare nell'elenco di task che l'aggiornamento è stato avviato.

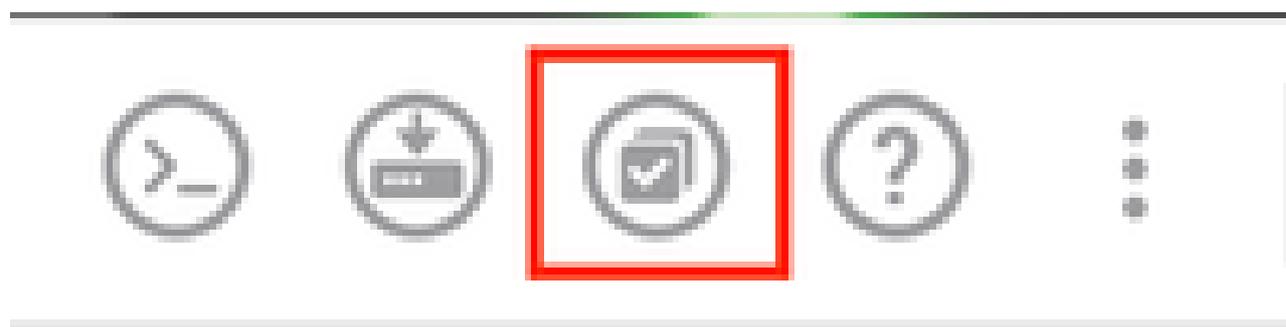
Task List

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.	



Nota: l'elenco di task si trova nella barra di navigazione accanto all'icona Distribuzioni.



Verifica

La sezione Motore di ispezione mostra che la versione corrente di Snort è Snort 3.

Intrusion Rule 20241010-1555

Latest Update on 14 Oct 2024

Configure

Set recurring updates

UPDATE FROM CLOUD

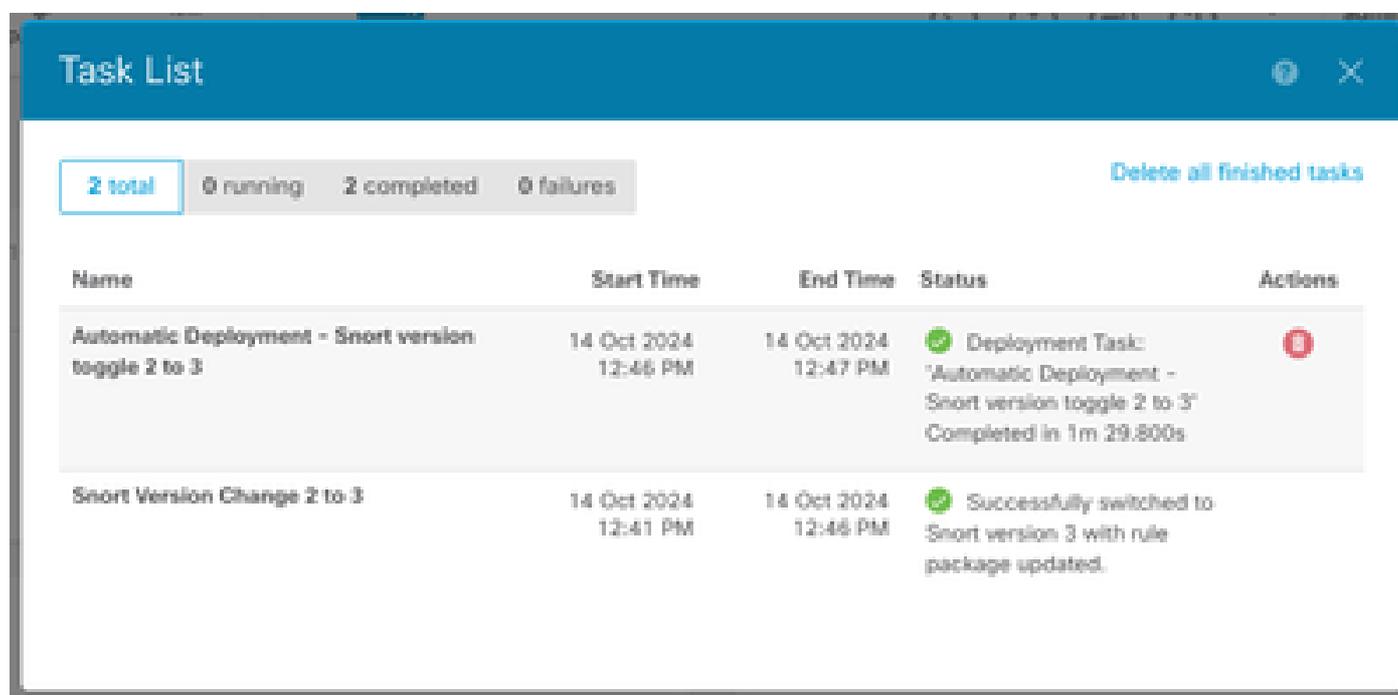
Snort

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](#)

Infine, nell'elenco delle attività, assicurarsi che la modifica all'ordine 3 sia stata completata e distribuita correttamente.



The screenshot shows a 'Task List' window with a blue header. Below the header, there are summary statistics: '2 total', '0 running', '2 completed', and '0 failures'. A 'Delete all finished tasks' link is visible on the right. The main content is a table with columns for Name, Start Time, End Time, Status, and Actions.

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.	

Risoluzione dei problemi

Se si verificano problemi durante l'aggiornamento, considerare i seguenti passaggi:

- Verificare che le versioni FTD siano compatibili con Snort 3.

Per ulteriori informazioni, consultare la [guida alla compatibilità di Cisco Secure Firewall Threat Defense](#)

- Raccogliere i file di risoluzione dei problemi in FDM passando alla scheda Dispositivo e quindi facendo clic su Richiedi file da creare. Una volta raccolto, aprire una richiesta con TAC e caricare il file nella richiesta per ricevere ulteriore assistenza.

Troubleshoot

No files created yet

REQUEST FILE TO BE CREATED

Informazioni correlate

- [Adozione Snort 3](#)
- [Ordina documenti](#)
- [Guida alla configurazione di Cisco Secure Firewall Device Manager, versione 7.2](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).