

Upgrade von Snort 2 auf Snort 3 über FMC

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Snort-Version aktualisieren](#)

[Methode 1](#)

[Methode 2](#)

[Aktualisierung von Angriffsregeln](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird das Upgrade von der Snort 2- und Snort 3-Version im Firepower Manager Center (FMC) beschrieben.

Voraussetzungen

Anforderungen

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

- FirePOWER Threat Defence
- FirePOWER Management Center
- Snort

Verwendete Komponenten

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

- FMC 7.0
- FTD 7.0

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 Snort 3-Funktion wurde in Version 6.7 für FirePOWER Device Manager (FDM) und Cisco Defense Orchestrator (CDO) sowie in Version 7.0 für FirePOWER Management Center (FMC) hinzugefügt.

Snort 3.0 wurde für folgende Herausforderungen entwickelt:

1. Reduzierung der Arbeitsspeicher- und CPU-Auslastung
2. Verbesserung der Effizienz von HTTP-Prüfungen.
3. Schnelleres Laden der Konfiguration und Neustart von Snort.
4. Bessere Programmierbarkeit für schnellere Funktionsbereitstellung

Konfigurieren

Snort-Version aktualisieren

Methode 1

1. Melden Sie sich bei FirePOWER Management Center an.



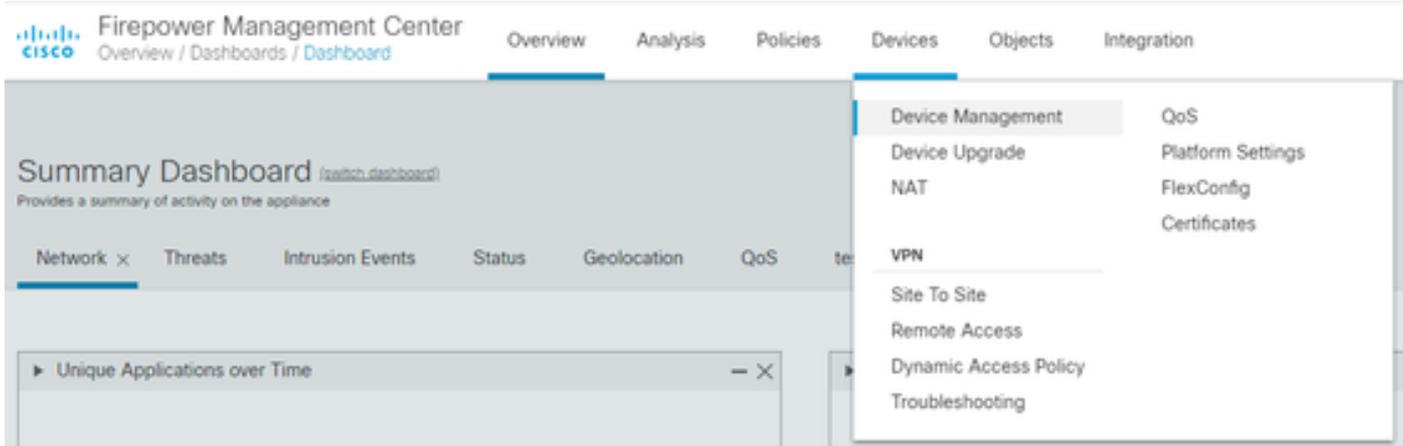
Firepower Management Center

Username

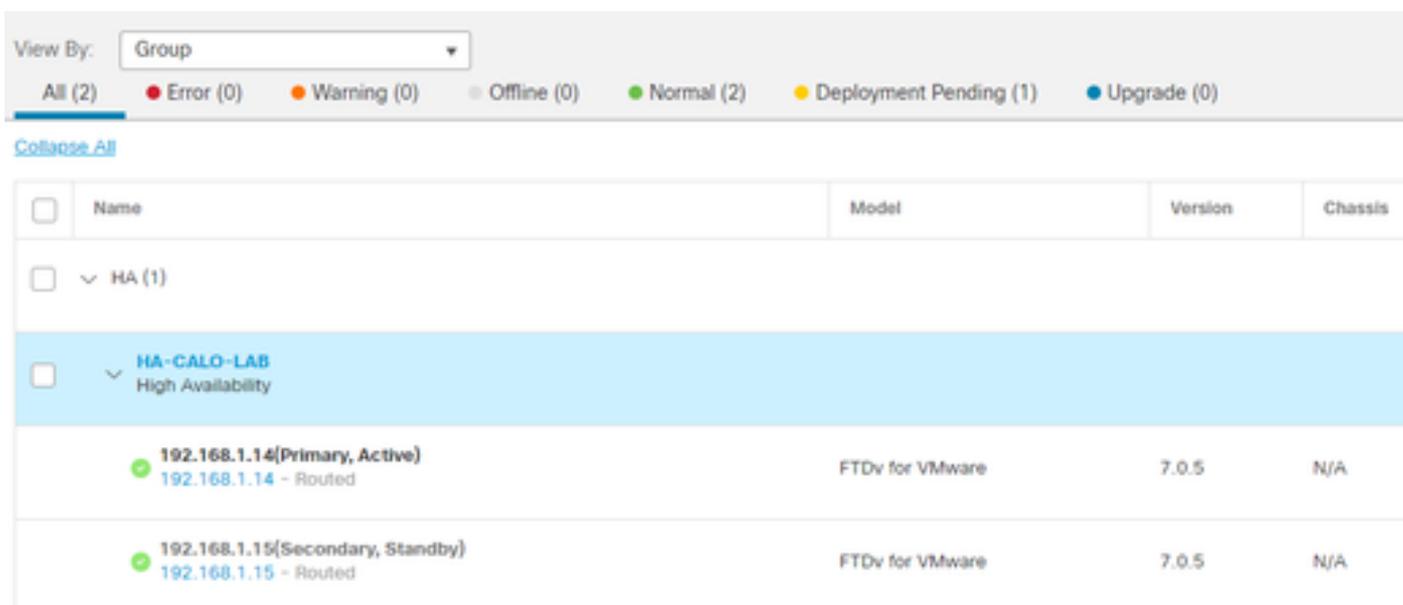
Password

Log In

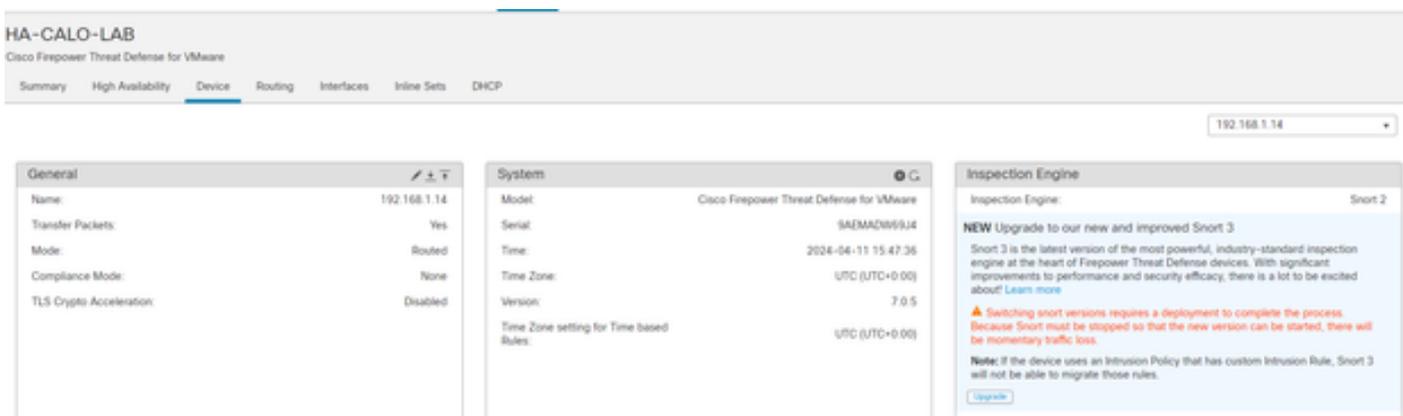
2. Navigieren Sie auf der Registerkarte Gerät zu Geräte > Geräte-Manager.



3. Wählen Sie das Gerät, das Sie die Snort-Version ändern möchten.



4. Klicken Sie auf die Registerkarte Gerät und dann im Abschnitt Inspektionsmodul auf die Schaltfläche Upgrade.



5. Bestätigen Sie Ihre Auswahl.

Enable Snort 3

Are you sure you want to enable Snort 3?

No

Yes

Methode 2

1. Melden Sie sich bei FirePOWER Management Center an.



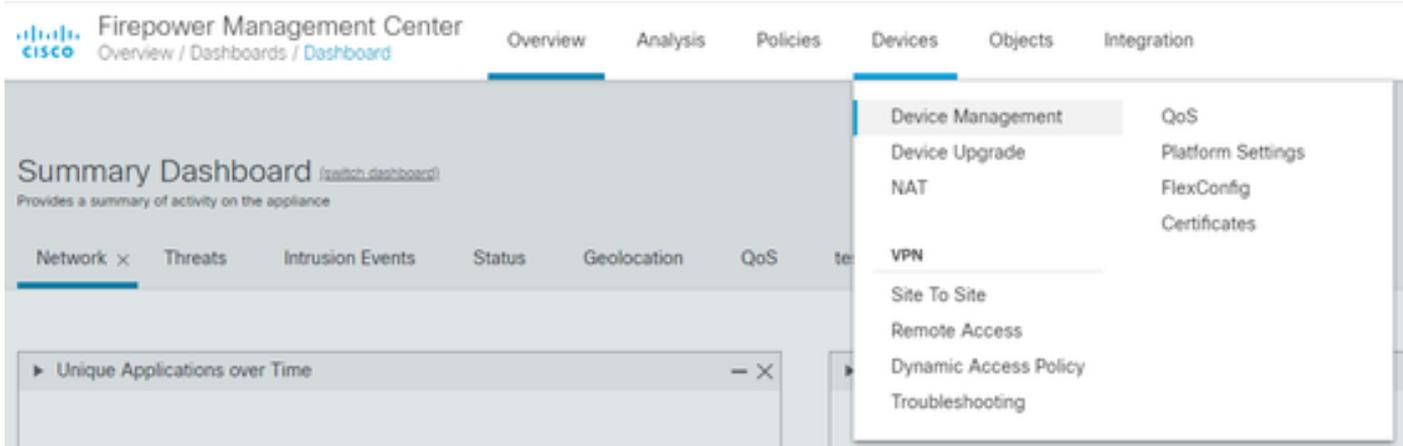
Firepower Management Center

Username

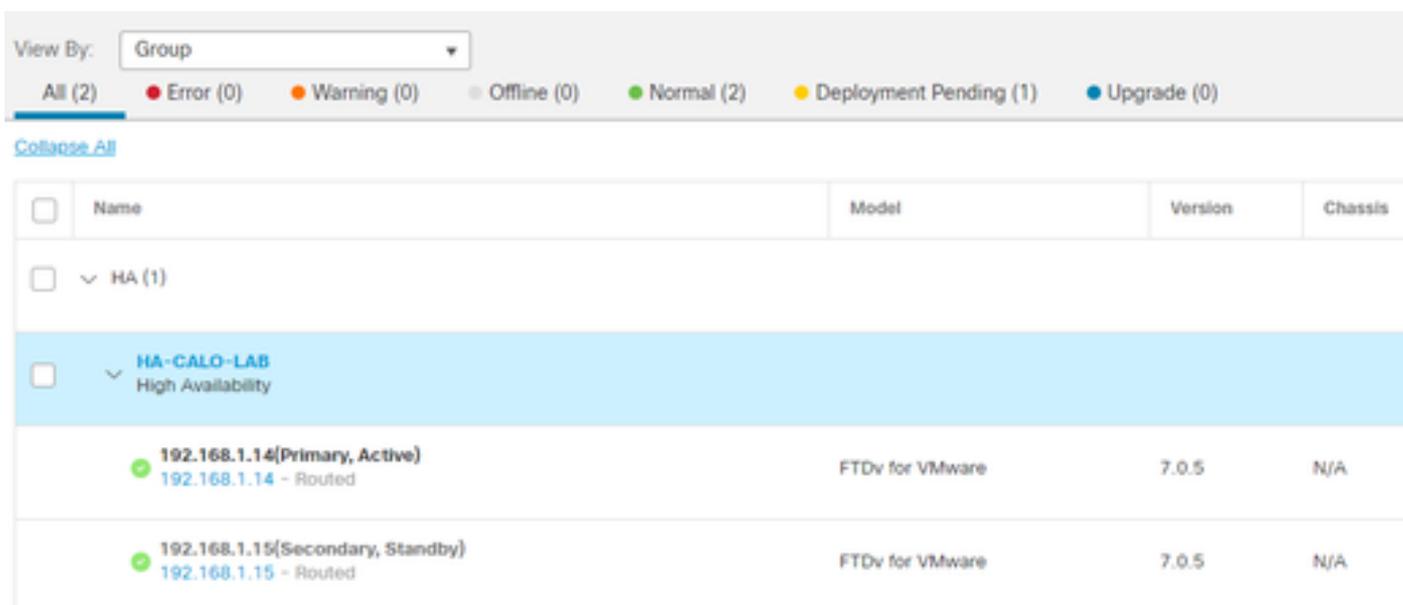
Password

Log In

2. Navigieren Sie auf der Registerkarte Gerät zu Geräte > Geräte-Manager.



3. Wählen Sie das Gerät, das Sie die Snort-Version ändern möchten.



4. Klicken Sie auf die Schaltfläche Aktion auswählen und wählen Sie Auf Snort 3 aktualisieren.

View By: Group

All (1)
Error (0)
Warning (0)
Offline (1)
Normal (0)

[Collapse All](#)
1 Device Selected
Select Action

<input type="checkbox"/>	Name
<input checked="" type="checkbox"/>	Ungrouped (1)
<input checked="" type="checkbox"/>	FTD 1 Snort 3 10.31.124.226 - Routed

Edit Advanced Settings
 Upgrade to Snort 3
 Upgrade Firepower Software
 Edit Deployment Settings

Aktualisierung von Angriffsregeln

Außerdem müssen Sie Ihre Snort 2-Regeln in Snort 3-Regeln umwandeln.

1. Wählen Sie im Menü Objekte > Zugriffsregeln aus.

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management
 Intrusion Rules

description, or Base Policy

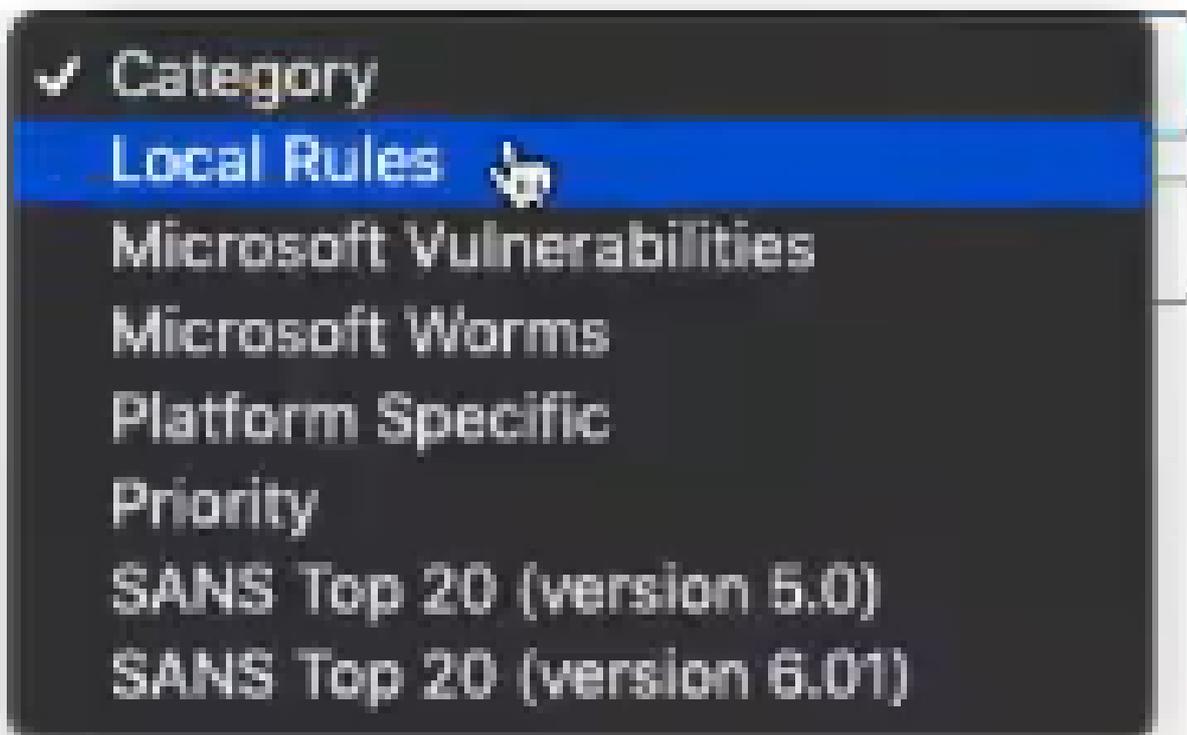
2. Wählen Sie im Menü Snort 2 All Rules (Alle Regeln) > Group Rules By (Regeln gruppieren nach) > Local Rules (Lokale Regeln).

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

Group Rules By



3. Klicken Sie auf Snort 3 Alle Regeln Registerkarte und stellen Sie sicher, dass Alle Regeln ausgewählt ist.

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

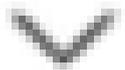
67 items

Search Rule Group

All Rules

4. Wählen Sie im Dropdown-Menü Task die Option Konvertieren und importieren aus.

Tasks



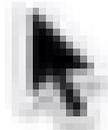
-----Snort 3-----

Upload

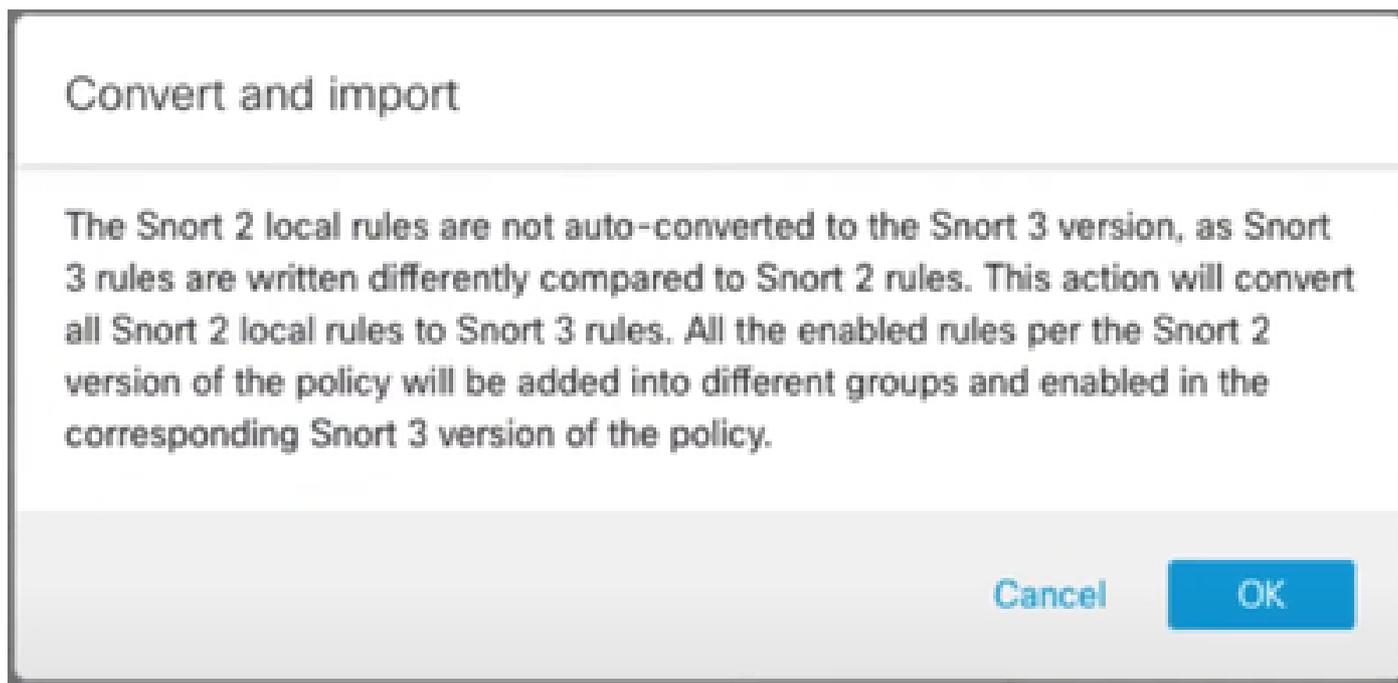
-----Snort 2-----

Convert and import

Convert and download



5. Klicken Sie in der Warnmeldung auf OK.



Überprüfung

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



Die Regelkonvertierung war erfolgreich, nachdem folgende Meldung angezeigt wurde:



Schließlich müssen Sie in der Gruppe Lokale Regeln den Abschnitt Alle Snort 2 konvertiert global finden, der alle von Snort 2 zu Snort 3 konvertierten Regeln enthält.



Fehlerbehebung

Wenn die Migration fehlschlägt oder abstürzt, setzen Sie den Rollback-Modus auf Snort 2 zurück, und versuchen Sie es erneut.

Zugehörige Informationen

- [So migrieren Sie von Snort 2 auf Snort 3](#)
- [Cisco Secure - Upgrade von Snort 3-Geräten \(externes YouTube-Video\)](#)

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.