

# FMC ربع Snort 3 ىل Snort 2 نم ةيقرتلا

## تايتوت حمللا

[قم دقمللا](#)

[ةيساس الابل طتملا](#)

[تابل طتملا](#)

[ةمدخت سمللا تانوكملا](#)

[ةيساس ا تامولعم](#)

[نڭوك تمللا](#)

[ةكش للاف ا رادصا ةيقرت](#)

[1 ةقيرطللا](#)

[2 ةقيرطللا](#)

[لفط تمللا دعاوق ةيقرت](#)

[ةحصلا نم ققحتلا](#)

[اهجالص او عاخذ ال افاشكتسا](#)

[ةلص تاذا تامولعم](#)

## ةمدقمللا

ةقاطلا ري دم زكرم ي ف Snort 3 و Snort 2 رادصا نم ةيقرتلا ةيفي ك دنت سمللا اذه حضوي (FMC) ةيرانلا.

## ةيساس الابل طتملا

### تابل طتملا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأب Cisco ي صوت:

- Firepower Threat Defense
- Firepower ةرادا زكرم
- Snort

### ةمدخت سمللا تانوكملا

ةيلاتلا ةيداملا تانوكملا او جماربلا تارادصا ىل دنت سمللا اذه ي ف ةدراولا تامولعملا دنت ست:

- FMC 7.0
- FTD 7.0

ةصاخ ةيلعم ةئي ب ي ف ةدوجوملا ةزهجال نم دنت سمللا اذه ي ف ةدراولا تامولعملا عاشن ا مت تناك اذ (يضا رتفا). حوسمم نيوكتب دنت سمللا اذه ي ف ةمدخت سمللا ةزهجال عي مج تا دب رم ا ي ال لم تحت حمللا ري ثاتلل كم هف نم دكأت ف ، ليغش تمللا دي ق ك تكبش

# ةيساسأ تامولعم

Cisco Defense Orchestrator (CDO) و FirePOWER Device Manager (FDM) ل 6.7 رادصلإا ف 3 snort ةزيم ةفاضإ تم ت FirePOWER (FMC) ةرادإ زكرم ل 7.0 رادصلإا ف ؛

تاي دحتللا هذه ةجلالعمل Snort 3.0 جم انرب ميمصت مت

1. ةركاذلاو ةيزكرملا ةجلالعمل ةدحو مادختسا ليلقت .
2. HTTP صحف ةيلاعف نيسحت .
3. ةلهذم ةعرسب ليغشتلا ةداعإو ةقئاف ةعرسب ةئيهتلا ليمحت .
4. عرسأ لكشب تازيملا ةدايزل لضفأ ةجمرب ةيلباق .

## نيوكتلا

ةكبشل رادصلإا ةيقرت

1 ةقيرطلا

1. Firepower ةرادإ زكرم ل ل لوخدلا ليجست .



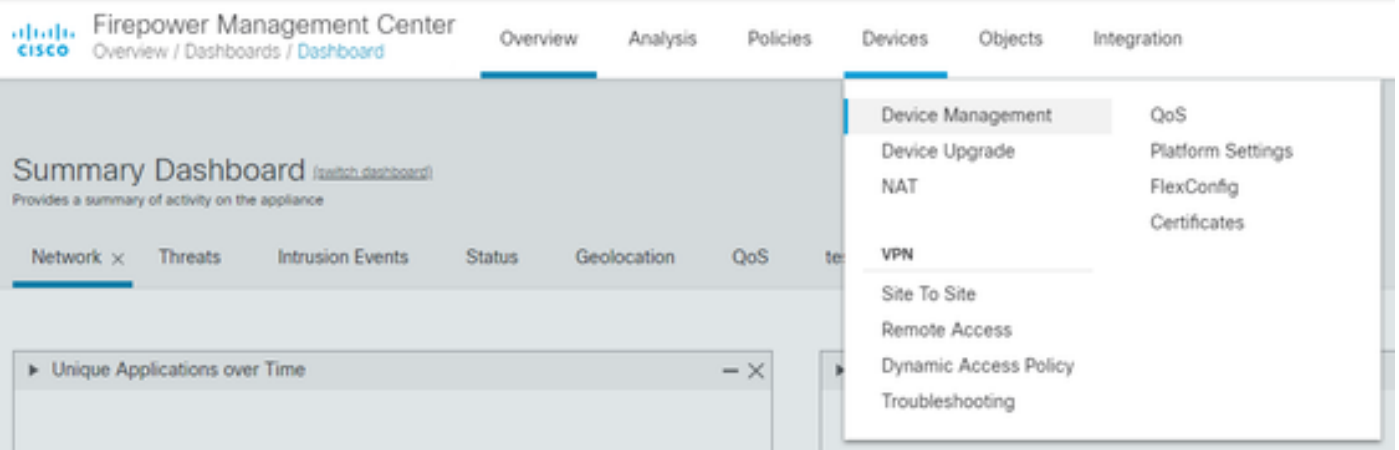
# Firepower Management Center

Username

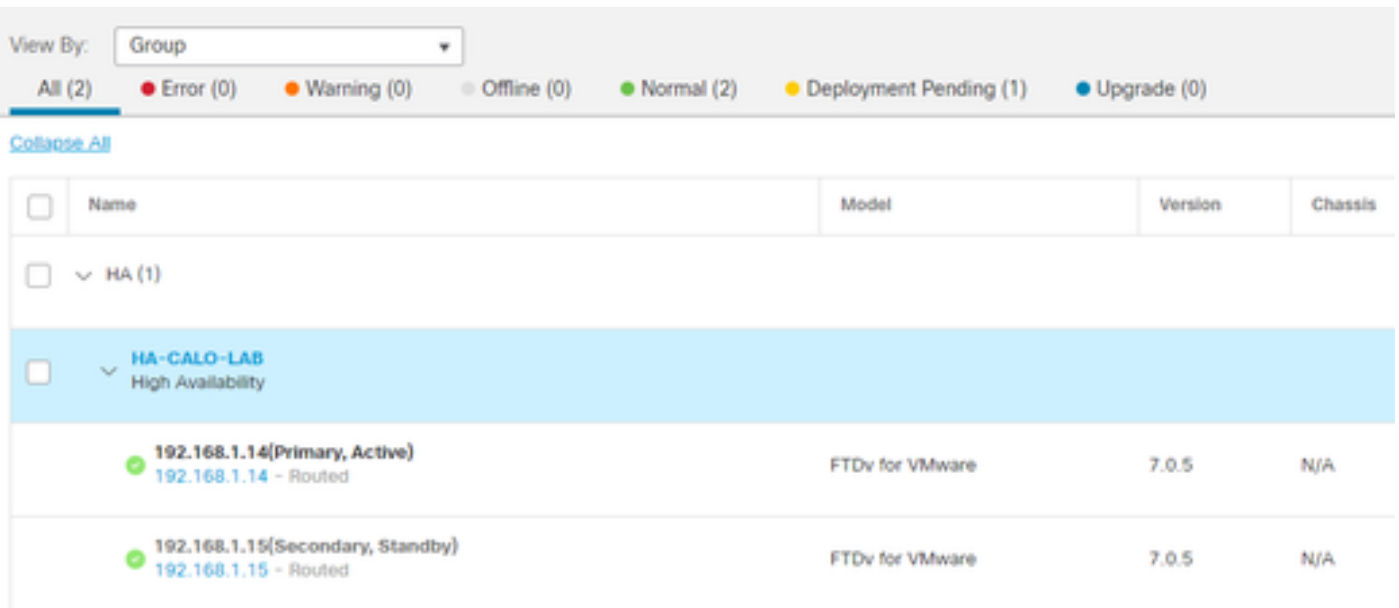
Password

Log In

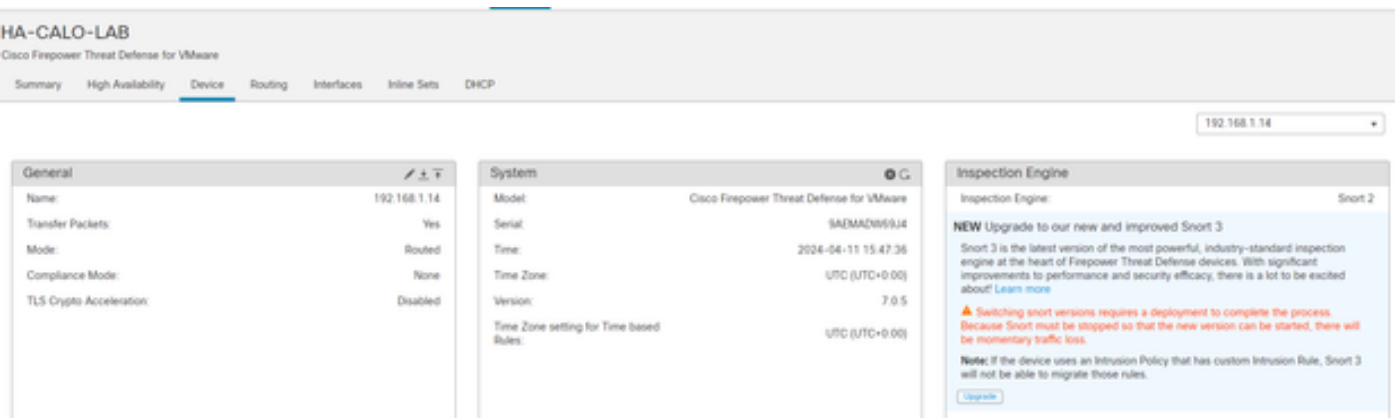
2. ةزهجألا ةرادا > ةزهجألا ىلا لقتنا ، زاهجال بيوبتلا ةمالع يف .



### 3. Snort رادصا ريغ تديرت يذلا زاوجل ادح.



### 4. صحفلا كرحم مسق يف ةيقرت رزلا قوف رقناو زاوجل ابوبتلا ةمالع قوف رقنا.



### 5. كرايتخا نم دكات.

## Enable Snort 3

Are you sure you want to enable Snort 3?

No

Yes

2 قيرطال

1. Firepower ةراد زكرم ىل لوخدلا لىجست .



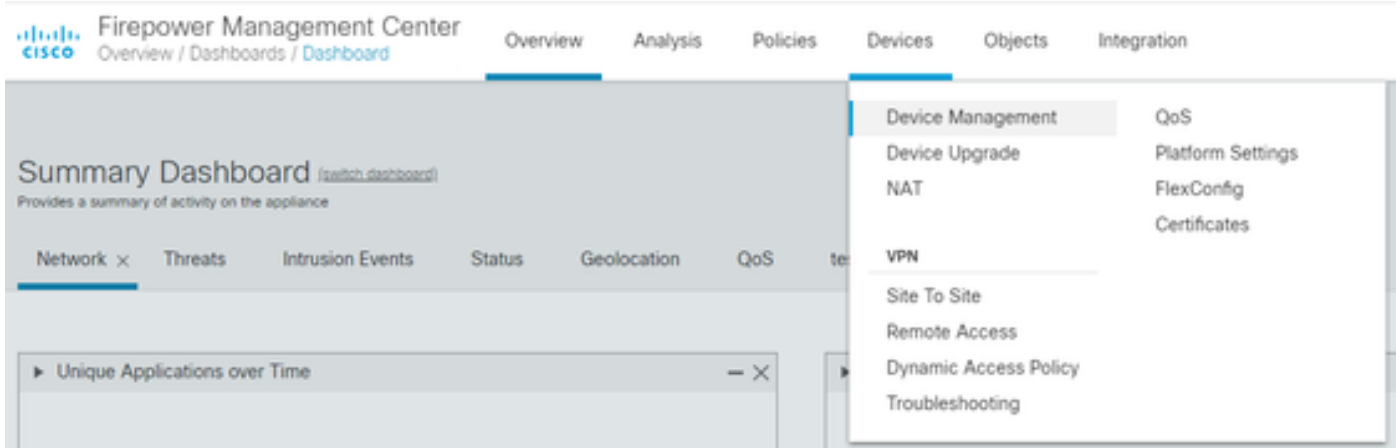
# Firepower Management Center

Username

Password

Log In

2. ةزهجألا ةرادا > ةزهجألا ىلا لقتنا ، زاهجال بيوبتلا ةمالع يف .



3. Snort رادصا ريغ ديتر يذلا زاھجلا دح.

View By:

All (2)
  Error (0)
  Warning (0)
  Offline (0)
  Normal (2)
  Deployment Pending (1)
  Upgrade (0)

[Collapse All](#)

<input type="checkbox"/>	Name	Model	Version	Chassis
<input type="checkbox"/>	HA (1)			
<input type="checkbox"/>	HA-CALO-LAB High Availability			
<input checked="" type="checkbox"/>	192.168.1.14(Primary, Active) 192.168.1.14 - Routed	FTDv for VMware	7.0.5	N/A
<input checked="" type="checkbox"/>	192.168.1.15(Secondary, Standby) 192.168.1.15 - Routed	FTDv for VMware	7.0.5	N/A

4. Snort 3 إلی قورتلا دحو ءارجلا ديحت رزلا قوف رقنا.

View By: Group

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

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

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

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

## لفطتال دعاوق ةيقرت

3. رخشلا دعاوق ىلا 2 ريخشلا دعاوق ليوتحت ىلا جاتحت ،كلذ ىلا ةفاضلا ابو

1. لفظتال دعاوق > تانئاك ةمئاقلا نم ددح.

Overview Analysis Policies Devices **Objects** AMP Intelligence

Object Management  
Intrusion Rules

Description, or Base Policy

دعاوقلا" > "ةومجمل دعاوق" > "دعاوقلا ةفاك" بيوتتال ةمالع Snort 2 ةمئاقلا نم ددح.2  
"ةيحلحمل



Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

Group Rules By

✓ Category

Local Rules

Microsoft Vulnerabilities

Microsoft Worms

Platform Specific

Priority

SANS Top 20 (version 5.0)

SANS Top 20 (version 6.01)

دعاوقلا عيجم دي دحت نم دكأتو Snort 3 All Rules بيوبتلا ةمالع قوف رقنا 3.

Snort 2 All Rules

Snort 3 All Rules

< Intrusion Policy

67 items

Search Rule Group

All Rules

داريت ساو لي وحت دح، ةمهمل ةلدسنملا ةمئاقلا ي ف.4

Tasks



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

Upload

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

Convert and import



Convert and download

"

5. ريذحتلا ةلاسري ف "قفاوم قوف رونا .

### Convert and import

The Snort 2 local rules are not auto-converted to the Snort 3 version, as Snort 3 rules are written differently compared to Snort 2 rules. This action will convert all Snort 2 local rules to Snort 3 rules. All the enabled rules per the Snort 2 version of the policy will be added into different groups and enabled in the corresponding Snort 3 version of the policy.

Cancel **OK**

## ةحصلا نم ققحتلا


snort 3 وه snort 2 نم يلاحلا رادصالا نأ شيتفتلا كرحم مسق رهظي

### Inspection Engine

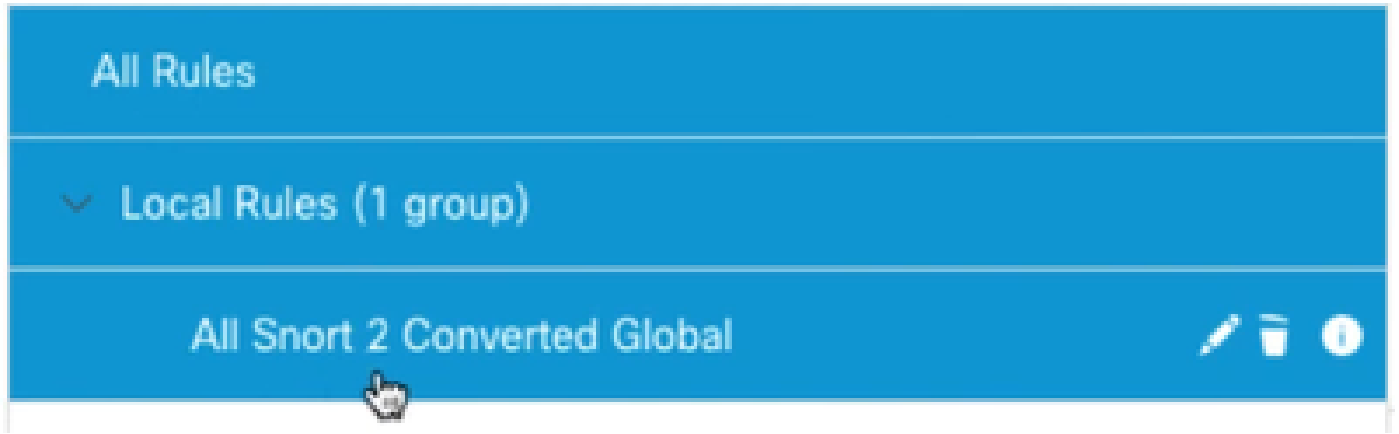
Inspection Engine: Snort 3

[Revert to Snort 2](#)

ةلاسرلا هذه ةيؤر درجم ب حاجنب ةدعاقلا ليوت مت

 The custom rules were successfully imported 

يذلاو ، Snort 2 Convert Global ةفاك مسق ةيلاحملا دعاقولا ةومجم يلع دجت نأ بجي ، اريخأ ةلوحملا Snort 3 يل Snort 2 دعاقو ةفاك يلع يوتحي .



## اهحال صإو ءاطخأل ا فاشك تسا

ةلواحم لا دعأو Snort 2 رادصإ إلا عوجرلاب مق ،هلطعت وأ ليحرتلا لشف ةلاح يف

## ةلص تاذا تامولعم

- [3 ترون إلا 2 ترون نم رجاهت فيك](#)
- [Cisco Secure - Snort 3 زاهج ةيقرت - \(يچراخ YouTube ويديف\)](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبلاو  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاغل مهتغب  
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىلإ أمئاد ةوچرلاب ي صؤتو تامچرتل هذه ةقدنع اهتيلوئسم Cisco  
Systems (رفوتم طبارلا) ي لصلأل يزي لچنل دن تسمل