

م تي يذلا طشننلا ةكبشلا رادصا دي دحت ديدهت دض عافدلا چمانرب ىلع هليغشت FirePOWER (FTD)

تايوت حمللا

[ةمدقملا](#)

[ةيساس الابلطتلا](#)

[تابلطتلا](#)

[ةمدختس مالتانوكلا](#)

[ةيساس ا تامولعم](#)

[FTD ىلع هليغشت م تي يذلا Active Snort رادصا دي دحت](#)

[FTD ل \(CLI\) برم اول برطس ةهجاو](#)

[Cisco FDM ةطساوب FTD ةرادا متت](#)

[Cisco نم FMC م كحتلا ةدجو ةطساوب FTD چمانرب ةرادا متت](#)

[Cisco نم CDO ةطساوب FTD ةرادا متت](#)

[ةلص تاذا تامولعم](#)

ةمدقملا

م تي يذلا (FTD) طشننلا ةكبشلا رادصا دي كاتل ةمزاللا تاوطخلا دنتس مالا اذه فص ي نامأ زاهج ري دم ةطساوب هترادا دن ع (FTD) Cisco Firepower Threat Defense نم هليغشت Cisco Defense وأ Cisco نم (FMC) FirePOWER ةرادا زكرم وأ Cisco نم (FDM) FirePOWER Orchestrator (CDO).

ةيساس الابلطتلا

تابلطتلا

ةيلاتلا عيضاوملاب ةفرعم كي دل نوكت نأ Cisco ي صوت:

- Cisco نم (FMC) FireSIGHT ةرادا زكرم
- Cisco نم (FTD) FirePOWER ديهت دض عافدلا
- Cisco نم (FDM) FirePOWER زاهج ري دم
- Cisco Defense Orchestrator (CDO)

ةمدختس مالتانوكلا

ةيلاتلا ةيداملا تانوكملاو چماربلا تارادصا ىل دنتس مالا اذه في ةدراولا تامولعملا دنتست:

- Cisco Firepower Threat Defense (FTD) رادصا 7.0.0 و 6.7.0

- Cisco Firepower (FMC) رادصلإا 6.7.0 و 7.0.0 ةرادإ زكرم
- Cisco Defense Orchestrator (CDO)

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسمل اذه يف ةدراول تامولعمل عاشنإ مت تناك اذا. (يضارتفا) حوسمم نيوكتب دنتسمل اذه يف ةمدختسمل ةزهجال عيمج تادب رما يال لمحتحمل ريثأتلل كمهف نم دكأتف، ليغشتلا ديق كتكبش


ةيساسأ تامولعم


ةلماش ةيقرت نع ةرابع وهو، ايمسر Snort 3 جم انرب قالطإب SNORT® ماحتقالا عنم ماظن ماق ةيلباقو ةعيرسلا ةجلعمل او ةادال نيسحت ىلع لمعت ةديج تازيمو تانيسحتب زيمتت 200+ نع ديزت يتلا تافاضالا نم ةعومجم ىلا ةفاضالاب، كتكبشل ةنسحمل ريوطتلا مهتكبشل صصخم دادعإ عاشنإ نم نومدختسمل نكمتي ثيحب

ي: لي ام، رصحلا ال لاثملا ليبس ىلع، 3 تروشل ايازم لمشتو

- نسحم اءا
- SMBv2 صحف نيسحت
- ةديجل ةيصنللا جم انربلا فاشتك تاناكلما
- HTTP/2 صحف
- ةصصخملل دعاوقلا تاعومجم
- ةباتكلل ةلوهس رثكأ ةصصخملل لفظتلا دعاوق لعجي يذلا ةلمجلل انب
- لسلتلا ثادحأ لخاد جئاتن "ضفخييس ناك" ل بابسألا
- لوجملل تانايب ةدعاق ىلا تاريغيغتلا رشن دنع ريغيغت تايلمع ي ليغشت ةداعإ متت ال ةصصخملل تاقيبطتلا فاشتك ةزهجاو (SSL) ةنمألا سباقملا ةقبط جهنو (VDB) TLS مءاخ ةيوه فاشتك او ديقملا لءدملا ةيوه رءاصمو
- ةزهجا 3 ب ةصاخ تانايب عبتت تانايب لاسررا بسبب، ةنسحم ةنايص ةيلباق لكشب اهالصل او ءاطخألا فاشكتسأ تالءسو Cisco ءاغن ةكبش ىلا دعب نع راعشتسإ لصفأ

FTD ةرادإ دنع طقف، Cisco Firepower Threat Defense (FTD) 6.7.0 ل Snort 3.0 ل مءدل مءدقت مت Cisco. FirePOWER (FDM) ةزهجا رءم لءالء نم

 (FTD) ةعيرسلا قئاف لاسررلا جم انرب يف ةديجلل رشنل تايلمعل ةبسنللاب: ةظءالم صءفلا كءم Snort 3.0 جم انرب دعى، FDM ةطساوب اهءرادإ متت يتلا 6.7.0 رادصلإا كءم ىقبي Snort 2.0 نإف، مءقأ رادصلإا نم 6.7 ىلا FTD ةيقرت ب تمق اذا. يضرءفالا Snort 3.0 ىلا لءبءتلا كءم ي نكل، طشنللا شيتفتلا

 دعاوق و ةيرهاظلا تاءوملا Snort 3.0 جم انرب مءءى ال، رادصلإا اءهل ةبسنللاب: ةظءالم و TLS 1.1 تالاصءا ريفشت كف و ءاقتولا ىلا ةدنتسمل لوصول يف مكءتلا

تازيمل هذه لىل ةجاحب نكت مل اذا طقف snort 3.0 نيكمتب مق .لقأل تالاصتال

يتال FirePOWER ديدهت نع عافدل ةزهأل SNORT 3.0 معد 7.0 رادصلال Firepower مدق ،كلذ دعب
Cisco نم FirePOWER (FMC) ةرادل زكرم و Cisco FDM نم لك ةطساوب اهترادل متت

ةعرسال قئاف لاسرالل جمانرب يف ةديجلال رشنال تايلمعل ةبسنلاب :ةظحال م
رشنال تايلمعل رمتست .يضارتفال صحتل كرحم نأل ال Snort 3 زارطلال دعي ،7.0 رادصلال
تقوي يف ليدبتال كنكمي نكلو ،Snort 2 مادختس يف اهتيقرتت مت يتال

الى عوجلال كنكمي يتح ،3.0 و 2.0 نيتروشال نيب ةيرحب ليدبتال كنكمي :ريذحت
تارادصلال ليدبت دنع رورملال ةكرح ةعطاقم متت .رمأل مزل اذا ريغتل

تاداشراو تازيملال دويقل اصاخ امامته ايلوت نأ كليلع .همهفو [FirePOWER نيوكت ليلد](#) ةءارقب ةدشب ي صوي ،Snort 3 لىل ليدبتال لبق :ريذحت
دحل لىل ريثأتلال ليلقتل ةممصم Snort 3 لىل ةيقرتلال نأ نم مغرل لىل .ليحرتل
ريضحتلالو ةطخلال كدعاست نأ نكمي .ةقذب نييعتلاب موقت ال تازيملال نأ ال ؛يندأل
عقوتم وه امك رورملال ةكرح ةجلالعم نم دكأتلال لىل ةيقرتلال لبق

FTD لىل هلليغشت متي يذل Active Snort رادصلال ديذحت

FTD ل (CLI) رماوالا رطس ةهجاو

ةهجاو لىل لوخدلال ليجستب مق ،FTD لىل هلليغشت متي يذل طشنال snort رادصلال ديذحتل
show snort3 status رمالا لىلغشتب مق و FTD يف (CLI) رماوالا رطس:

snort 2 لىلغشتب FTD موقوي ،ضورعم جارخا دجوي ال امندنع :1 لاثم

```
<#root>
```

```
>
```

```
show snort3 status
```

```
>
```

snort 2 لىلغشتب FTD موقوي ،"الاح 2 snort لىلغشت متي" جارخالال ضرعي امندنع :2 لاثم

```
<#root>
```

```
>
```

```
show snort3 status
```

```
Currently running Snort 2
```

snort 3 ليغش ت ب FTD موق ي ،"اي لاج snort 3 ليغش ت متي" جارخال اضري ام دن ع :3 لاثم ل

```
<#root>
```

```
>
```

```
show snort3 status
```

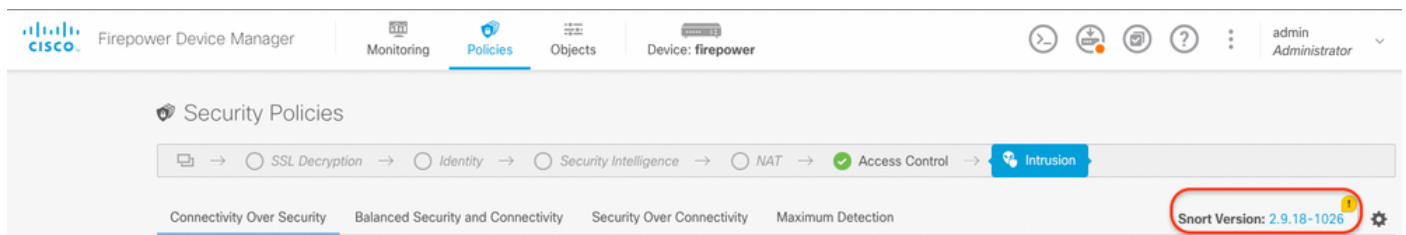
Currently running Snort 3

Cisco FDM ةطساوب FTD ةراد م مت

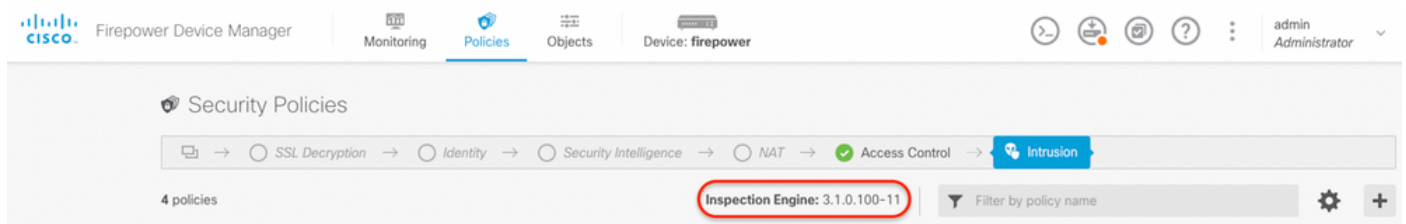
Cisco ةطساوب هتراد م مت يذال FTD يلع هليغش ت متي يذال طشننل اجم انربل رادصل دي دحتل فدي لاثم ل :
ةيلاتل تاوطخال لمك أ ، FDM

1. FDM بيولا ةهجاو لال خ نم Cisco FTD يلى لوخدلا ليحس ت ب مق .
2. تاسايس ددح ، ةيسيئرلا ةمئاق ل نم .
3. ماح تقا بيوبتلا ةمال ع ددح م ت .
4. FTD ي ف طشننل snort رادصل دي كاتل صحفلا كرحم مسق وا snort رادصل نع ثحبا .

snort نم 2 رادصلال FTD لغشي :1 لاثم



3. ةغيص snort ةغيص FTD لغشي :2 لاثم



Cisco FMC ةطساوب (FTD) ةعرسلال قئاف لاسرلال اجم انرب ةراد م مت

ةدحو ةطساوب هتراد م مت FTD يلع هليغش ت متي يذال طشننل لاثم ل رادصل دي دحتل فدي لاثم ل :
ةيلاتل تاوطخال لمك أ ، Cisco نم (FMC) ةيسيئال ةرادال ي ف مكحتل

1. Cisco FMC بيولا ةهجاو يلى لوخدلا ل حس .
2. زاهال ةراد ددح ، ةزهجال ةمئاق نم .
3. بس انم ل FTD زاهج ددح م ت .
4. صاصرلا ملقلا ريرحت ةنوقيا رقنا .

5. في طش نال snort رادص ا دي كاتل ص ح فال كرحم مسق نع ثح باو زا جال بي وب تال ةم ال ع دح فTD:

snort نم 2 رادص ا ل فTD ل غشي 1: لاثم

The screenshot shows the Cisco Firepower Management Center interface for device vFTD-1. The 'Inspection Engine' section is highlighted with a red box, indicating the current configuration is Snort 2. A 'NEW Upgrade' notification is present, stating that Snort 3 is the latest version and offers significant performance and security improvements. The notification includes a warning that switching snort versions requires a deployment to complete the process and that Snort must be stopped so that the new version can be started, resulting in momentary traffic loss. A 'Revert to Snort 2' button is visible in the highlighted section.

3. ة غشي snort ة غشي فTD ل غشي 2: لاثم

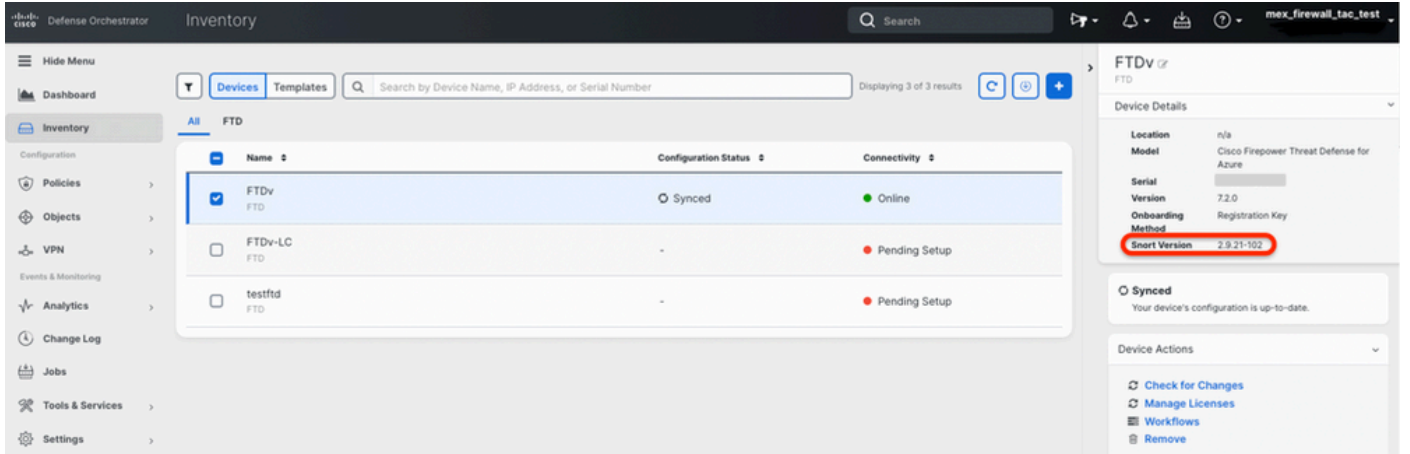
The screenshot shows the Cisco Firepower Management Center interface for device FTD1010-1. The 'Inspection Engine' section is highlighted with a red box, indicating the current configuration is Snort 3. A 'Revert to Snort 2' button is visible in the highlighted section. The notification area at the bottom of the page contains the same text as in the previous screenshot, detailing the benefits of Snort 3 and the requirements for upgrading.

Cisco CDO ةطس اوب (FTD) ةعرسلا قئاف لاسرالا ءمانرب ةرادإ متت

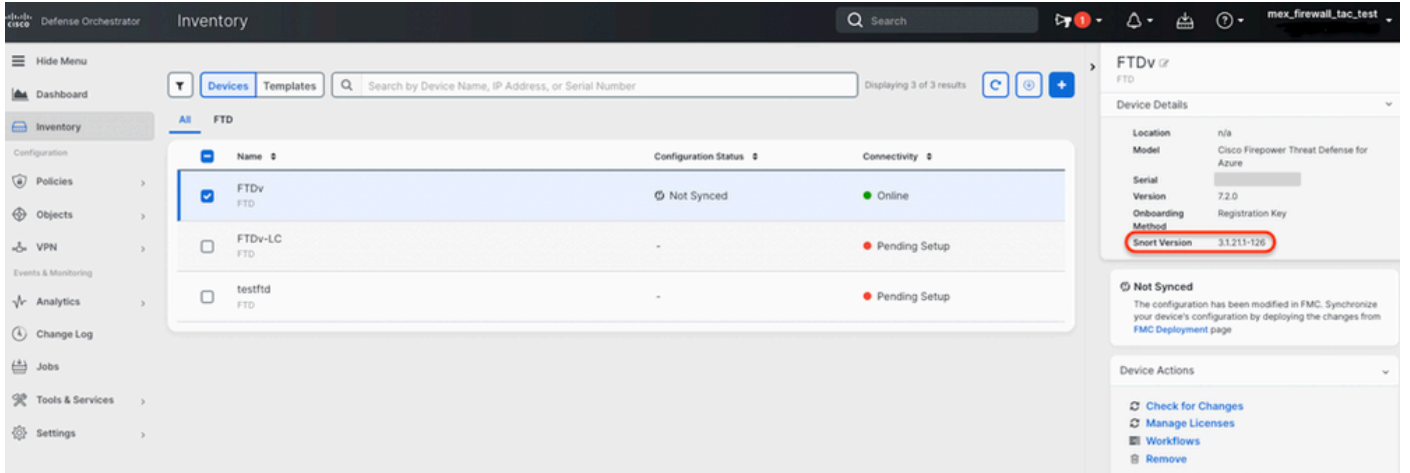
Cisco ةطس اوب ءترادإ متت FTD ىلع هلىغشت متي يذلا طشنلا ءمانربلا رادصا دي دحتل ةيلالاتا تاوطخلا لمكأ، Defense Orchestrator:

1. Cisco Defense Orchestrator بىولا ءهءاو ىلى لوخذلا لءس.
2. بسانملا FTD زاهء دء، نوزءملا ءمئاق نم.
3. snort رادصا نع ءءب، زاهءلا لىصافا مسق ي ف:

snort نم 2 رادصالا FTD لءش ي: 1 لائءم



3. ءغىص snort ءغىص FTD لءش ي: 2 لائءم



ءلص تا ءامول عم

- [Cisco Firepower، رادصالا 6.7.0](#)
- [Cisco Firepower، رادصالا 7.0](#)
- [Snort 3 عقوم](#)
- [Cisco Systems - ءادنءس مل او ىنءقءلا معءلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن مة و مچم مادختساب دن تسمل اذ ه Cisco ت مچرت
ملاعلاء ان ا عي مچ ي ف ني م دخت سمل ل معد ي و تح م مي دقت ل ق ي رش ب ل و
امك ق ي قد ن و ك ت ن ل ق ي ل أ مچرت ل ض ف أ ن أ ظ ح ال م ي ج ر ي . ص ا خ ل م ه ت غ ل ب
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ق ي ف ا ر ت ح ا ل ا مچرت ل ا ع م ل ا ح ل ا و ه
ي ل ا م ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ق د ن ع ا ه ت ي ل و ئ س م Cisco
Systems (رف و ت م ط ب ا ر ل ا) ي ل ص أ ل ا ي ز ي ل ج ن إ ل ا دن تسمل ا