

FTD و ASA ل Syslog SNMP تام ئالم نيوكت

تايوت حمل

[قمدق مل](#)

[قسس اسأل تابلط مل](#)

[تابلط مل](#)

[قمدختس مل تانوك مل](#)

[قسس اسأل تامول عم](#)

[نيوكت مل](#)

[ASA نيوكت](#)

[FDM لبق نم رادمل FTD نيوكت](#)

[FMC لبق نم رادمل FTD نيوكت](#)

[قحص مل نم ققحت مل](#)

[SNMP مداخ تايئ اصح راظا](#)

[لجس مل دادع راظا](#)

[قلس تاذ تامول عم](#)

قمدق مل

(SNMP) طيس بل لك بش لة راد لوكوتورب تارابتخ نيوكت قف قك دنتس مل اذ قصي ديدت ن ع افدل او Cisco نم (ASA) قف كتل ل لبق ل نامأل زا ق ل ع syslog لئس ر لاس رال FirePOWER (FTD).

قسس اسأل تابلط مل

تابلط مل

قيلال عيضاوم لاب قفر عم كيدل نوكت نأ Cisco قيصوت:

- Cisco ASA ب قسس اسأل قفر عم
- Cisco FTD ب قسس اسأل قفر عم
- SNMP لوكوتورب قسس اسأل قفر عم

قمدختس مل تانوك مل

قيلال جم انربل رادص ل دنتس مل اذ ق ف قراول تامول عم ل دنتس ت:

- Cisco Firepower ل AWS 6.6.0 ديدت دص ع افدل
- Firepower Management Center، رادص ل 6.6.0
- Cisco، رادص ل 9.12(3)9 نم قف كتل ل لبق ل نامأل زا ق جم انرب

قصاخ قلم عم قئ ب قف قدو و مل قزه جأل نم دنتس مل اذ ق ف قراول تامول عم ل عاشن ا م تناك اذ (قصار قف) حوس مم نيوكت ب دنتس مل اذ ق ف قمدختس مل قزه جأل ع قمج تاد ب رمأ ق ل مل تح مل ر قثا ل ل كم هف نم دكأت ف، ل قغش تال د ق ك تك بش

ةيساسا تامولعم

كانه ،كلذ عمو .لجستل تامولعم ريفوتل ةددعتم تاناكلم |لج Cisco نم FTD و ASA يوتحي مداخ كانه ناك اذا اليدب SNMP تارابتخ| مدقت .ارايخ syslog مداخ نوكي ال ثيح ةددم عوام ريفوتم SNMP .

لج .ةبقارملا واهال صاوا عاطخال فاشكتسا ضارغال ةصاخ لئاسر لاسرل ةديفم ةادأ هذه زواجت تاهويرانيس ءانثا اهبقت مزلي ةلص تاذ ةلكشم كانه تناك اذا ،لاثملا ليبس لج زيكرتلل ASA و FTD نم لك لج HA ةئفلل SNMP تارابتخ| مادختسا| نكمي ،لشلال طاقف لئاسرلا هذه .

دنتسمل اذه |ف Syslog تائفب ةقلعتملا تامولعملا نم ديزم لج روثل نكمي .

(CLI) رماولا رطس ةهجاو مادختسا اب ASA ل نيوكت ةلثمأ ريفوت وه ةلاقملا هذه نم ضرغل ،ةطساوب اهترادا| متت يتل FTD ةزيمو ،FMC ةطساوب اهترادا| متت يتل FTD ةزيمو و FirePOWER Device Manager (FDM).

ةهجاو ل نيوكتلا اذه ةفاض| بجي ف ،FTD ل Cisco Defense Orchestrator (CDO) مادختسا| مت اذا FDM.

لئاسر لج لدمم دح نيوكتب صوي ،ةعفترملا syslog تالدمم ةبسنلاب :ريذحت
سرخال تالدمم لاي ريثاتلا عنم syslog .

دنتسمل اذه في ةدراولا ةلثمأ اعيمجل ةمدختسملا تامولعملا يه هذه .

رادصا| SNMP: **SNMPv3**

ةعومجملا مسا :SNMPv3 ةعومجم

ةقداصملا ل HMAC SHA ةيمزراوخ عم **admin-user** SNMPv3 مدختسم

مداخ ل IP ناونع SNMP: **10.20.15.12**

جراخ :SNMP مداخ ب لاصلال اهمادختسا| بولطملا ASA/FTD ةهجاو

Syslog Message-id: **11009**

نيوكتلا

ASA نيوكت

ةيلال تامولعملا دعب ASA لج SNMP تامئالم نيوكتل تاوطخال هذه مادختسا| نكمي .

syslog ةئاق ل اةفاضل لئاسرلا نيوكتب مق .1 ةوطخال

```
logging list syslog-list message 111009
```

SNMPv3 مداخ تاملعم نيوكت .2 ةوطخال

```
snmp-server enable
```

```
snmp-server group group-name v3 auth
```

```
snmp-server user admin-user group-name v3 auth sha cisco123
```

SNMP تامئالم نيكمت 3. ةوطخال

```
snmp-server enable traps syslog
```

لجست ةهچوك SNMP تامئالم ةفاضل 4. ةوطخال

```
logging history syslog-list
```

FDM لبق نم رادملا FTD نيوكت

ةرادل دنع SNMP مداخلل اهل اسرلال ةنيعم syslog ةمئاق نيوكتل تاوطخال هذه مادختس لنكمي FDM ةطساوب FTD.

+ رزىلع ددحو شادحال ةمئاق تاحشرم > تانئاكل لىل لقتنا 1. ةوطخال

تاذلئ اسرلال تافرعم وائافل نيمصتب مقو ةيجوزلا ةمئاق ةيمصتب مق 2. ةوطخال قفاوم ددح مث. ةلصلل

Edit Event List Filter



Name

logging-list

Description

Logs to send through SNMP traps

Severity and Log Class

+

Syslog Range / Message ID

111009

100000 - 999999

[Add Another Syslog Range / Message ID](#)

CANCEL

OK

ةشاشلل نم FlexConfig تانئاك > FlexConfig > مدقتم نيوكت ىل لقتنا 3. ةوطخل
+ رزلا ددحو FDM ل ةسئزل

:ةردملا تامولعمل مادختساب ةللالت FlexConfig تانئاك ءاشناب مق

SNMP مداخ: مسالا

SNMP مداخ تامولعمل: (يرايخ) فصولا

بلال:

```
snmp-server enable
snmp-server group group-name v3 auth
snmp-server user admin-user group-name v3 auth sha cisco123
snmp-server host outside 10.20.15.12 version 3 admin-user
```

حل اص ريغ بلال:

```
no snmp-server host outside 10.20.15.12 version 3 admin-user
no snmp-server user admin-user group-name v3 auth sha cisco123
no snmp-server group group-name v3 auth
no snmp-server enable
```

Edit FlexConfig Object



Name

SNMP-Server

Description

SNMP Server Information

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable
2 snmp-server group group-name v3 auth
3 snmp-server user admin-user group-name v3 auth sha cisco123
4 snmp-server host outside 10.20.15.12 version 3 admin-user
```

Negate Template ⚠

Expand | Reset

```
1 no snmp-server host outside 10.20.15.12 version 3 admin-user
2 no snmp-server user admin-user group-name v3 auth sha cisco123
3 no snmp-server group group-name v3 auth
4 no snmp-server enable
```

CANCEL

OK

مسابلا: **SNMP-TRAPS**

SNMP تامئال م نيكمت : (يراي تخ) فصولا

بلاقلا:

```
snmp-server enable traps syslog
```

حل اص ريغ بلاق:

```
no snmp-server enable traps syslog
```

Edit FlexConfig Object



Name

SNMP-Traps

Description

Enable SNMP traps

Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 snmp-server enable traps syslog
```

Negate Template ⚠

Expand | Reset

```
1 no snmp-server enable traps syslog
```

CANCEL

OK

لېچستال تاطوفحم :مسالا

SNMP عقاومل syslog لئاسر نېيعتل نئاك : (پرايخا) فصولا

بلاقلا

```
logging history logging-list
```

حلاص ريغ بلاق

```
no logging history logging-list
```

Create FlexConfig Object



Name

Logging-List

Description

Syslog list to send through SNMP traps



Variables

There are no variables yet.
Start with adding a new variable.

+ ADD VARIABLE

Template

Expand | Reset

```
1 logging list syslog-list message 111009
2 logging trap syslog-list
```

Negate Template ⚠

Expand | Reset

```
1 no logging trap syslog-list
2 no logging list syslog-list message 111009
```

CANCEL

OK

تانيك ال عي مج فض أو FlexConfig جهن > FlexConfig > مدقتم نيوكت يلى لقتنا 4. ةوطخلال متي ةعباتال رماوالا نا شيح ةلص يذ ريغ رمالا. ةقبا سلال ةوطخلال ي ف اهواشنإ مت ي تلال كانه ةثالثل تانئكالل نوكت نا درجم ب ظفح دح. (SNMP مدإخ) نئكالل س فن ي ف اهني م ضت رمالا ةمئاق ةنياعمال مسق رهظي و.

Successfully saved.

Group List

+

1. Logging-history

2. SNMP-Server

3. SNMP-Traps

Preview

Expand

```
1 logging history logging-list
2 snmp-server enable
3 snmp-server group group-name v3 auth
4 snmp-server user admin-user group-name v3 auth sha cisco123
5 snmp-server host outside 10.20.15.12 version 3 admin-user
6 snmp-server enable traps syslog
```

SAVE

تاريغيغتلل قيبطتل عيزوت ةنوقيأ دح 5 ةوطخلل.

FMC لبق نم رادمل FTD نيوكت

قباسللا يف ةدوجوم تناك يتللا كلتل ةلثامم تاهوييرانيس هالعأ ةدراوللا ةلثمألل حضوت مت مث (FMC) ةيساسألل ةحوللل ةرادل يف مكحتلل ةدحو ىلع تاريغيغتلل هذه نيوكت مت نكلو SNMPv2 مادختسلا نكمي امك. هريدت يذلا " (FTD) ةعرسلل قئافل لاسرلال جم انرب" ىللا اهرشن مادختساب FTD ىلع رادصللا اذمه مادختساب SNMP مداخ دادع مادختسلا ةيفيك [لاقملا اذمه](#) حرشي ةرادل FMC.

ىللا نيعمللا جهنلا يف ريرحت ددحو ةيساسألل ماظنلل تادادع > ةزهجالا ىللا لقتنا 1. ةوطخلل هيلع نيوكتلل قيبطتل رادمل زاهجال.

SNMP مداوخ نيكم ت رايخ ددحو SNMP ىللا لقتنا 2. ةوطخلل

Overview Analysis Policies **Devices** Objects AMP Intelligence Deploy System Help

Device Management NAT VPN QoS **Platform Settings** FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

Hosts Users SNMP Traps

Add

Interface	Network	SNMP Version	Poll/Trap	Trap Port	Username
No records to display					

م دختس م لا تام ول عم أ ل ما . ة فاض ا رز لا د د ح و ن و م د خ ت س م ب ي و ب ت ل ا ة م ا ل ع د د ح . 3 ة و ط خ ل ا

Add Username

Security Level: Auth

Username*: user-admin

Encryption Password Type: Clear Text

Auth Algorithm Type: SHA

Authentication Password*:

Confirm*:

Encryption Type: []

Encryption Password: []

Confirm: []

OK Cancel

تمام عمل التهيئة بمتابعة مربع **إضافة اسم المستخدم** الذي يوافق الإعدادات في الخطوة 4. وخطوات
مضافة اسم المستخدم، ثم انقر فوق **إضافة** في مربع الحوار **إضافة اسم المستخدم**. إذا تم إدخال اسم المستخدم في مربع الحوار
تمام عمل التهيئة بمتابعة مربع **إضافة اسم المستخدم** الذي يوافق الإعدادات في الخطوة 4. وخطوات
مضافة اسم المستخدم، ثم انقر فوق **إضافة** في مربع الحوار **إضافة اسم المستخدم**. إذا تم إدخال اسم المستخدم في مربع الحوار
تمام عمل التهيئة بمتابعة مربع **إضافة اسم المستخدم** الذي يوافق الإعدادات في الخطوة 4. وخطوات
مضافة اسم المستخدم، ثم انقر فوق **إضافة** في مربع الحوار **إضافة اسم المستخدم**. إذا تم إدخال اسم المستخدم في مربع الحوار

Add SNMP Management Hosts



IP Address*

SNMP Version

Username

Community String

Confirm

Poll

Trap

Trap Port (1 - 65535)

Reachable By:

- Device Management Interface *(Applicable from v6.6.0 and above)*
- Security Zones or Named Interface

Available Zones

Add

Selected Zones/Interfaces

Add

OK

Cancel

تمام ال عي مج ة لازا نم دكأت syslog ع برم ددحو SNMP تامئالم بيوبتلا ةمال ع ددح 5 ة و طخل
ة بولطم نكت مل اذا ىرأل تامئالم رايتخ.

Device Management NAT VPN QoS Platform Settings FlexConfig Certificates

FTD-PS You have unsaved changes Save

Enter Description Policy A

- ARP Inspection
- Banner
- DNS
- External Authentication
- Fragment Settings
- HTTP
- ICMP
- Secure Shell
- SMTP Server
- ▶ **SNMP**
- SSL
- Syslog
- Timeouts
- Time Synchronization
- Time Zone
- UCAPL/CC Compliance

Enable SNMP Servers

Read Community String

Confirm

System Administrator Name

Location

Listen Port (1 - 65535)

SNMP Traps

Enable Traps All SNMP Syslog

Standard

Authentication

Link up

Link Down

Cold Start

Warm Start

Entity MIB

ةفاضاب مق ةفاضل رزلا دح .ثادجال مئوق بيوبتل ةمالع ددحو **syslog** لىل لقتنا 6 ةوطخل ةعباتملل قفاوم دح .ةمئاقلا يف اهنيمضت متيس يتلا لئاسرلاو مسا

Add Event List

Name*

?
X

Severity/EventClass

Message ID

+ Add

Message IDs	
111009	✎ 🗑

OK

Cancel

ةفاضل رزلا ددحو ليجستلا تاهجو بيوبتلا ةمالع دح. 7 ةوطخل

SNMP ةمئالم لىل ليجستلا ةهجو ربيغت

اهل ةرواجملا 6 ةوطخل لىف اهواشنم يتلا ثادحلأا ةمئاق رتخاو مدختسملا ثادحأ ةمئاق دح

عطقملا اذه ريرحت ءاهنال قفاوم دح.

Add Logging Filter

Logging Destination: SNMP Trap

Event Class: Use Event List

logging-list

Event Class	Syslog Severity
No records to display	

OK Cancel

هترادإ متت يذلا زاهجلا لىلع تاريخيغتلا رشنو ظفح رزلا دح. 8 ةوطخل

ةحصلال نم ققحتلا

ASA CLI و FTD CLISH نم لك لىف هاندأ رماوالا مادختسا نكمي

SNMP مداخ تايئاصح راهاظ

خف لاسرا اهيف مت يتلا تارملا ددع لوح تامولعم "show snmp-server statistics" رمال رفوي
ىرخأ تامئالم دادعلا اذه نمضتتي نأ نكمي

```
# show snmp-server statistics
0 SNMP packets input
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
0 Number of requested variables
0 Number of altered variables
0 Get-request PDUs
0 Get-next PDUs
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
```

2 SNMP packets output

```
0 Too big errors (Maximum packet size 1500)
0 No such name errors
0 Bad values errors
0 General errors
0 Response PDUs
```

2 Trap PDUs

رمأ ذيفنتب مدختسمل اهي ف موقوي ةرم لك لاثملا اذه في مدختسمل اةلاسرلا فرعم لغشي دادعلا ةدايز متت ، "show" رمأ رادصا متي ةرم لك في

ليجستلا دادعلا راهظا

ةهجو لك ةطساوب اهل اسرا متي يتلا لئاسرلا لوح تامولعم "show logging setting" رفوي ةمئالملا ليجست تايئاصح اطبترت . SNMP تارابتخا تادادعلا تاظوفحملا ليجست ريشي syslog تافيضم تادادع

```
# show logging setting
Syslog logging: enabled
Facility: 20
Timestamp logging: enabled
Hide Username logging: enabled
Standby logging: disabled
Debug-trace logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level debugging, 30 messages logged
Trap logging: level debugging, facility 20, 30 messages logged
Global TCP syslog stats::
NOT_PUTABLE: 0, ALL_CHANNEL_DOWN: 0
CHANNEL_FLAP_CNT: 0, SYSLOG_PKT_LOSS: 0
PARTIAL_REWRITE_CNT: 0
Permit-hostdown logging: disabled
History logging: list syslog-list, 14 messages logged
Device ID: disabled
Mail logging: disabled
ASDM logging: disabled
```

لئاسر ةيأ طاقسا مدع نامضل "show logging queue" رمألا رادصا ب مق

```
# show logging queue

Logging Queue length limit : 512 msg(s)
0 msg(s) discarded due to queue overflow
0 msg(s) discarded due to memory allocation failure
Current 0 msg on queue, 231 msgs most on queue
```

ةلص تاذا تامولعم

- [Cisco ASA Series Syslog لئاسر](#)
- [Cisco ASA Series تايلمعمل رمأوالا رطس ةهجاو نيوكت لئلد: 9.12 ةماعلا](#)
- [FirePOWER NGFW ةزهجا لئل ع SNMP نيوكت](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نمة دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةلخت. فرتمة مچرت مء دقء ةل ةل ةفارتحال ةمچرتل عم لاعل او
ىل إأمءءاد ءوچرلاب ةصوء و تامچرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزءل ءنل دن تسمل