

# اهحالص او هئا طخأ فاشك ت ساو SNMP نيوك ت FirePOWER FDM لى

## تايوت حمل

---

[عمدق مل](#)

[قيساس الابل ط مل](#)

[تابل ط مل](#)

[عمدخت س مل تانوك مل](#)

[قيساس ا تامول عم](#)

[6.7 لى ع دي دل ا وش](#)

[نيوك ت مل](#)

[SNMP v3](#)

[SNMP v2c](#)

[SNMP نيوك ت قلازا](#)

[فحص مل نم قق ح ت مل](#)

[SNMP v3 نم قق ح ت مل](#)

[SNMP v2c نم قق ح ت مل](#)

[اهحالص او عا ط خ ال فاشك ت سا](#)

[قبو ج او قلى س ا](#)

[قلى ص تا ذ تامول عم](#)

---

## عمدق مل

رادص ال لى ع (SNMP) طيس بل ا ك ب ش ل ا ة راد ا لوكوت و ر ب ني ك م ت ة ي ف ي ك دن ت س مل ا اذ ه ح ض و ي REST تاق ي ب ط ت ة ج م ر ب ة ه ج او مادخت سا ب FirePOWER زا ه ج ة راد ا نم 6.7.

## ة ي س اس ال ا تابل ط مل

### تابل ط مل

ة ي ل ل ا ل ع ي ض او م ل ا ب ة فر عم ك ي دل نو ك ت ن ا ب Cisco ي ص و ت:

- FirePOWER Device Management ل ب ق نم راد مل (FTD) Firepower دي ه ت دض ع ا ف دل ا (FDM)، 6.7 رادص ال ا
- REST API ة فر عم
- SNMP ة فر عم

### عمدخت س مل تانوك مل

رادص ال ا ، FirePOWER Device Management ة ط سا و ب ه ت راد ا م ت ت Firepower دي ه ت دض ع ا ف دل ا 6.7.

ةصاخ ةي لمعم ةئيب يف ةدوجوملا ةزهجال نم دنتسملا اذه يف ةدراول تامولعمل اءاشنم ت تناك اذا .(يضا رتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسمل ةزهجال عيمج ت ادب رما يال لم تحملا ريثاتلل كمهف نم دكأتف ، ليغشتلا ديقتك ت كبتش


## ةيساسا تامولعم

### 6.7 ىلع ديوجل وش

تاعومجمو ني فيضملا او ني مدختسمل او SNMP م داخ ةرادا و نيوكت REST API FTD Device م عدي 6.7 رادصلا ، FP يف SNMP FTD زاوجل تاقيبطتلا ةجمرب ةهجاو معد عم . ةفيضملا ةزهجال

- ةرادا REST API FTD تاقيبطت ةجمرب ةهجاو لالخ نم SNMP نيوكت مدختسمل نكمي ةكبشلا .
- تاعومجمو ني مدختسمل او SNMP م داخ ةرادا و ا ثي دحت/ ةفاضلا نكمي FTD زاوجل REST تاقيبطت ةجمرب ةهجاو لالخ نم ني فيضملا/ ني فيضملا

ةطساوب اهذاختا مت يتي ل نيوكتلا تاوطخ دنتسملا يف ةنمضملا ةلثملا فصت FDM ل (API) تاقيبطتلا ةجمرب ةهجاو فشكتسم

 REST تاقيبطت ةجمرب ةهجاو لالخ نم ال SNMP لوكوتورب نيوكت نكمي ال : ةظالم FDM ةطساوب هترادا متتو 6.7 رادصلا ليغشتب FTD موقوي ام دنع

تاقيبطتلا ةجمرب ةهجاو (API) تاقيبطتلا ةجمرب ةهجاو معد - تازيمل ىلع ةماع ةرطن SNMP FTD زاوجل (REST)

- SNMP ب ةصاخ FDM ل ديجل URL ناو نع ةياهن طاقن ةزيمل هذه فيضت .
- تاعالطتسال SNMP نيوكتل هذه ةديجل تاقيبطتلا ةجمرب تاهجاو مادختسا نكمي ةمظنالا ةبقارمل خاخ فل او يارلا .
- (API) تاقيبطتلا ةجمرب تاهجاو ربع SNMP لوكوتورب دع ب ام نيوكت ريفوت متي صحفلا راطخال و اعارتقال تاي لمعل ، FirePOWER ةزهجا ىلع (MIB) ةرادا تامولعم دع او قو NMS/SNMP لي مع ىلع

طاقن SNMP API/URL ةياهن

URL	بي لاسالا	زطلال
/devicesettings/default/snmpservers	راضا	SNMPServer
/devicesettings/default/snmpservers/{objId}	ذخ ، عض	SNMPServer
/object/snmphosts	ىلع لوصحلا ، لاسرا	SNMPHost
/object/snmphosts/{objId}	لوصحلا ، فذح ، عضو	SNMPHost

	ىلع	
/object/snmpusergroups	ىلع لوصحلا ، لاسرا	SNMPUserGroup
/object/snmpuserGroups/{objId}	لوصحلا ، فذح ، عضو ىلع	SNMPUserGroup
/object/snmpusers	ىلع لوصحلا ، لاسرا	SNMPUser
/object/snmpusers/{objId}	لوصحلا ، فذح ، عضو ىلع	SNMPUser

## نيوكتلا

ةيساسأ تارادصا 3 ىلع SNMP فيضم يوتحي:

1. SNMP v1
2. SNMP v2C
3. SNMP v3

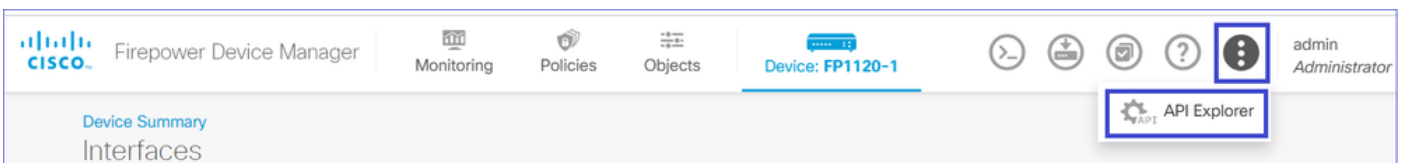
V1 و V2C: ني رادصا ل ةبسنلاب securityConfiguration ل صاخ قي سنت هذه نم دحاو لك ل V2C و V1 ه ناب نيوكتلا فرعي عون لقح و عم ةلس لس ىلع يوتحي

ىلع نيوكتلا فرعي عون لقح و حلاص SNMP v3 م دختسم ىلع يوتحي: SNMP v3 ل ةبسنلاب 3. ه ناب

## SNMP v3

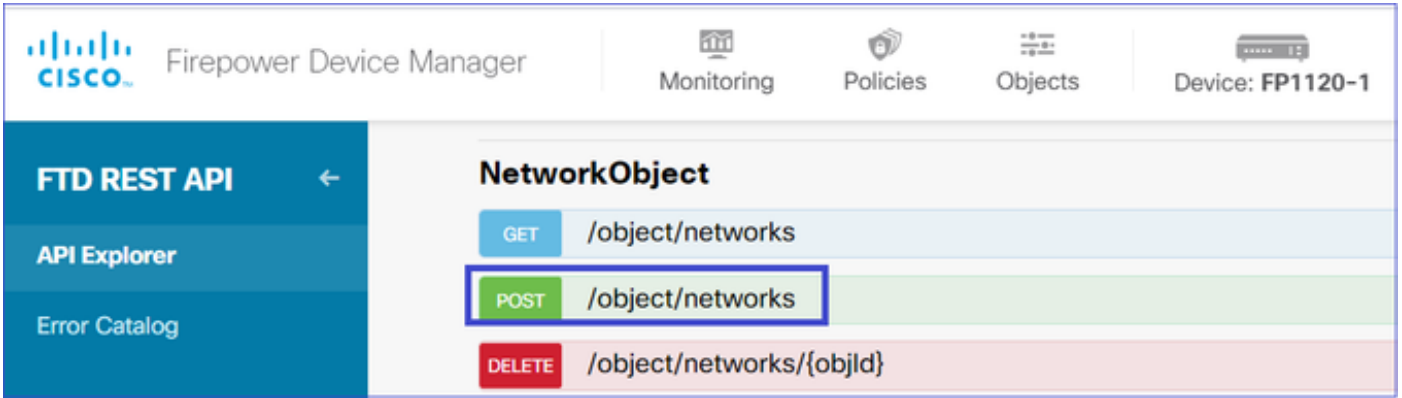
1. FDM ل (API) تاقىب طتلا ةجرمرب ةهجاو فشكتسم ىلا لوصولا.

م دختسم ل ةهجاو نم FDM REST ل (API) تاقىب طتلا ةجرمرب ةهجاو فشكتسم ىلا لوصولا (API) تاقىب طتلا ةجرمرب ةهجاو فشكتسم م ثا لثلا طاقنلا دح ، FDM ل (GUI) ةيموسرلا URL [تاقىب طت ةجرمرب ةهجاو فشكتسم](#) ىلا لقتنا ، كلذ نم ال دب



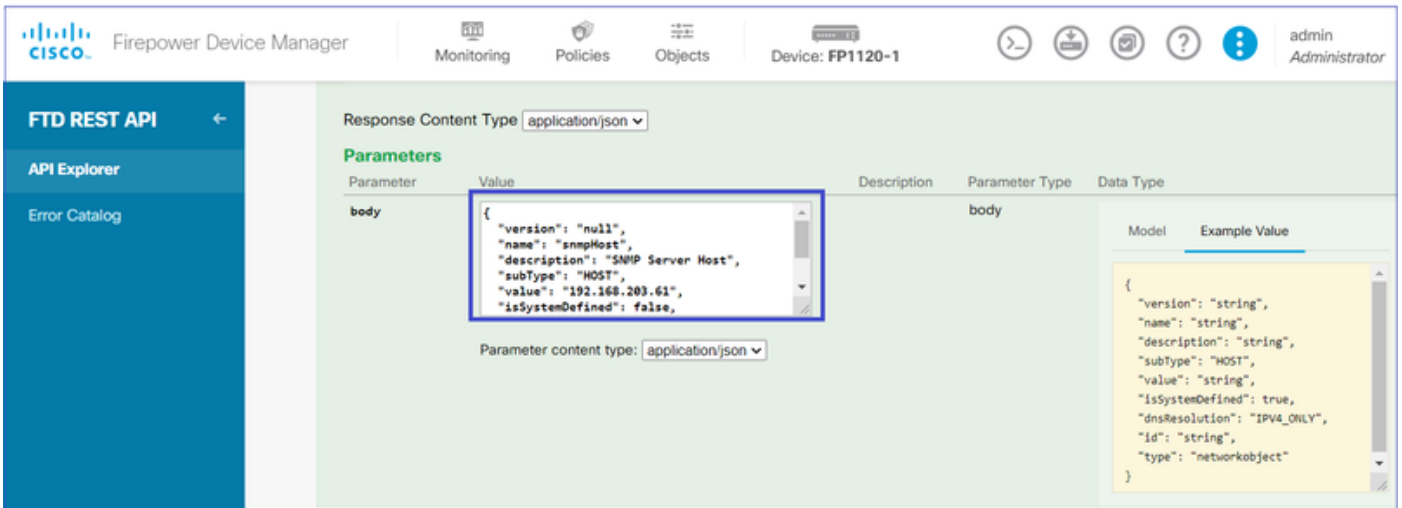
2. ةكبش ل نئاك نيوكت.

NetworkObject دح ، Explorer FDM API جمانرب في SNMP فيضم ل ديدج ةكبش نئاك عاشنا :  
تاكبش/نئاك/رشنب مق م ث



رېيغتو يې اساساً صرنا مسق يې اذه JSON قصلال. اذه وه SNMP فيضم ل JSON قيسنت  
 SNMP فيضم ل IP ناونع قوباطمل عميقلال ل IP ناونع

```
{
"version": "null",
"name": "snmpHost",
"description": "SNMP Server Host",
"subType": "HOST",
"value": "192.168.203.61",
"isSystemDefined": false,
"dnsResolution": "IPV4_ONLY",
"type": "networkobject"
}
```



(API) تاق يې بطتاللا عمرب هه جاو اء ادتس اذيفنتل! ءلوا حمال رزلل دحو لفسأ ل ريرمتلاب مق  
 200 ءباجتسالال زمر عا راب ءحجان عم لالم موقت

TRY IT OUT!

تمامولعملالعلمىلإجاحتحت، اقحال. تاطحالمرتفدىلإباجتسالالقهجمنJSONتانايبخسنا  
SNMP فيضم لوح.

The screenshot displays the FTD REST API Explorer interface. The left sidebar contains the following menu items: "FTD REST API", "API Explorer", and "Error Catalog". The main content area shows the URL `https://10.62.148.231/api/fdm/v6/object/networks` and the "Response Body" containing the following JSON data:

```
{
  "version": "bsha3bhghu3vm",
  "name": "snmpHost",
  "description": "SNMP Server Host",
  "subType": "HOST",
  "value": "192.168.203.61",
  "isSystemDefined": false,
  "dnsResolution": "IPV4_ONLY",
  "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
  "type": "networkobject",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/networks/1d10ce6d-49de-11eb-a432-e320cd56d5af"
  }
}
```

Below the response body, the "Response Code" is shown as 200.

3. (SNMP) طيسبلالأكبشلالةرادإلوكوتوربنم ثلاثلالرادصللديدمدختسمعاشنإ.  
FDM API Explorer، دح SNMP مق مئك/لجرتب مق مئك/snmpusers.

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1

FTD REST API

API Explorer

Error Catalog

SNMP

- GET /devicesettings/default/snmpservers
- GET /devicesettings/default/snmpservers/{objId}
- PUT /devicesettings/default/snmpservers/{objId}
- GET /object/snmpusers
- POST /object/snmpusers

لثالث (لبيس لعل) كمه ي يتل ماسق الال ليدعتب مقو ةركفم لىل هذه JSON تانايب خسنال، authenticationPassword و encryptionPassword و (تايمزراوخل و):

```
{
"version": null,
"name": "snmpUser",
"description": "SNMP User",
"securityLevel": "PRIV",
"authenticationAlgorithm": "SHA",
"authenticationPassword": "cisco123",
"encryptionAlgorithm": "AES128",
"encryptionPassword": "cisco123",
"id": null,
"type": "snmpuser"
}
```

⚠ في .طقف يحيضوتللا ضرعلال ضارغال يه ةلثمالا يف ةمدختسملال رورملا تاملك ريذحت  
ةيوق رورم تاملك مادختسا نم دكأت ،جاتنا ةئييب

يساسال صنلال مسق لىل ةلدعملال JSON تانايب خسنال:

Firepower Device Manager

Monitoring Policies Objects Device: FP1120-1

admin Administrator

FTD REST API

API Explorer

Error Catalog

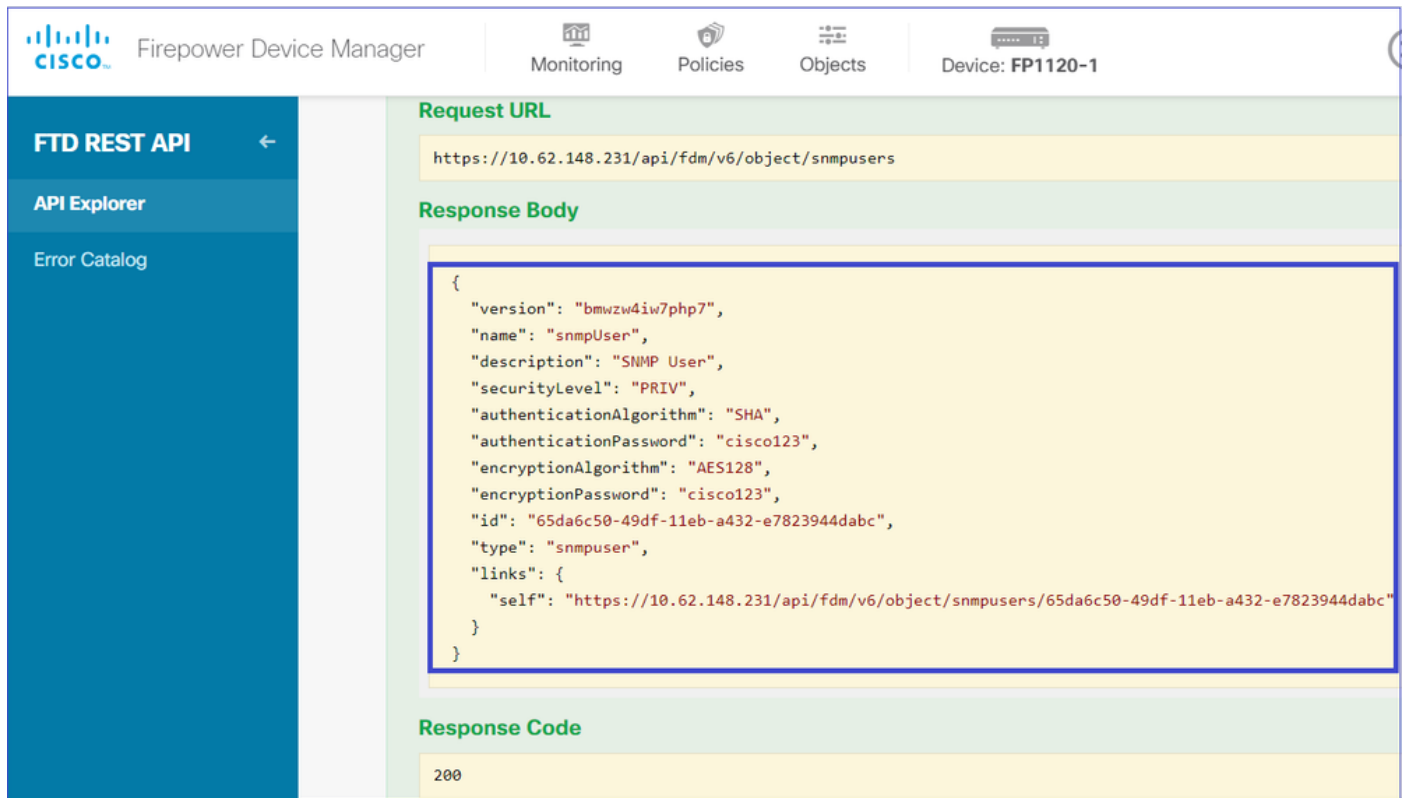
Response Content Type: application/json

Parameters

Parameter	Value	Description	Parameter Type	Data Type				
body	<pre>{ "version": null, "name": "snmpUser", "description": "SNMP User", "securityLevel": "PRIV", "authenticationAlgorithm": "SHA", "authenticationPassword": "cisco123", }</pre>		body	<table border="1"> <thead> <tr> <th>Model</th> <th>Example Value</th> </tr> </thead> <tbody> <tr> <td></td> <td> <pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre> </td> </tr> </tbody> </table>	Model	Example Value		<pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre>
Model	Example Value							
	<pre>{ "version": "string", "name": "string", "description": "string", "securityLevel": "AUTH", "authenticationAlgorithm": "SHA", "authenticationPassword": "string", "encryptionAlgorithm": "AES128", "encryptionPassword": "string", "id": "string", "type": "snmpuser" }</pre>							

Parameter content type: application/json

(API) تاقېب طتلا ةجمر ب ةهجاو ءاعدتسإ ذيفنتل !ةلواحمل رزلا ددحو لفسأ ىلإ ريرمتلاب مق ىلإ ةباجتسال ةهجاو نم JSON تانايب خسنا .200 ةباجتسالال زمرع اجراب ةحجان ةملاكم موقت SNMP مدختسم لوح تامولعملال علم ىلإ جاتحت ،اقحال .تاظحالم رتفد



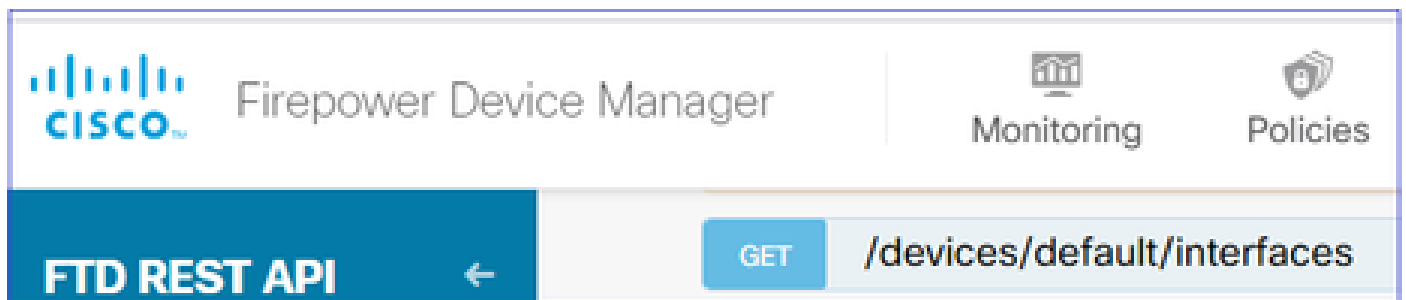
The screenshot displays the Firepower Device Manager interface. The top navigation bar includes the Cisco logo, 'Firepower Device Manager', and tabs for 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. On the left, a sidebar shows 'FTD REST API' with sub-items 'API Explorer' and 'Error Catalog'. The main content area shows a REST API call with the following details:

- Request URL:** `https://10.62.148.231/api/fdm/v6/object/snmpusers`
- Response Body:** A JSON object containing user details:

```
{
  "version": "bmwz4iw7php7",
  "name": "snmpUser",
  "description": "SNMP User",
  "securityLevel": "PRIV",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "cisco123",
  "encryptionAlgorithm": "AES128",
  "encryptionPassword": "cisco123",
  "id": "65da6c50-49df-11eb-a432-e7823944dabc",
  "type": "snmpuser",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpusers/65da6c50-49df-11eb-a432-e7823944dabc"
  }
}
```
- Response Code:** 200

4. ةهجاوولا تامولعمل ىلع لصحا.

ىلع لصحا مث ةهجاوولا ددح ،FDM ل (API) تاقېب طتلا ةجمر ب ةهجاو فشكلتسم ىلع SNMP مداخب لصتت يتلا ةهجاوولا نم تامولعملال عيمجت ىلإ جاتحت ./default/interfaces/ةزهجأل/



The screenshot shows the Firepower Device Manager interface with the REST API section active. The top navigation bar includes the Cisco logo, 'Firepower Device Manager', and tabs for 'Monitoring' and 'Policies'. The left sidebar shows 'FTD REST API'. The main content area displays the endpoint `/devices/default/interfaces` with a 'GET' button next to it.

(API) تاقېب طتلا ةجمر ب ةهجاو ءاعدتسإ ذيفنتل !ةلواحمل رزلا ددحو لفسأ ىلإ ريرمتلاب مق ىلإ ةباجتسال ةهجاو نم JSON تانايب خسنا .200 ةباجتسالال زمرع اجراب ةحجان ةملاكم موقت ةهجاوولا لوح تامولعمل ةئبعت ىلإ جاتحت ،اقحال .تاظحالم رتفد

**FTD REST API** ←

API Explorer

Error Catalog

https://10.62.148.231/api/fdm/v6/devices/default/interfaces

**Response Body**

```

"version": "kkpkibjlu6qro",
"name": "inside",
"description": null,
"hardwareName": "Ethernet1/2",
"monitorInterface": true,
"ipv4": {
  "ipType": "STATIC",
  "defaultRouteUsingDHCP": false,
  "dhcpRouteMetric": null,
  "ipAddress": {
    "ipAddress": "192.168.203.71",
    "netmask": "255.255.255.0",
    "standbyIpAddress": null,
    "type": "haipv4address"
  },
  "dhcp": false,
  "addressNull": false,
  "type": "interfaceipv4"
},
"ipv6": {
  "enabled": false,

```

**Response Code**

200

نم JSON تانايې ىل ع ل ا ث م . JSON تانايې نم عون ل ل او فر ع م ل او م س ا ل او ة ه ج ا و ل ا ر ا د ص ا ر ك ذ ت ة : ل خ ا د ل ا ة ه ج ا و ل ا

<#root>

```

{
"version": "kkpkibjlu6qro",
"name": "inside",
"description": null,
"hardwareName": "Ethernet1/2",
"monitorInterface": true,
"ipv4": {
"ipType": "STATIC",
"defaultRouteUsingDHCP": false,
"dhcpRouteMetric": null,
"ipAddress": {
"ipAddress": "192.168.203.71",
"netmask": "255.255.255.0",
"standbyIpAddress": null,
"type": "haipv4address"
},
"dhcp": false,
"addressNull": false,
"type": "interfaceipv4"
},
"ipv6": {

```



```
"enabled": false,
"autoConfig": false,
"dhcpForManagedConfig": false,
"dhcpForOtherConfig": false,
"enableRA": false,
"dadAttempts": 1,
"linkLocalAddress": {
"ipAddress": "",
"standbyIpAddress": "",
"type": "haipv6address"
},
"ipAddresses": [
{
"ipAddress": "",
"standbyIpAddress": "",
"type": "haipv6address"
}
],
"prefixes": null,
"type": "interfaceipv6"
},
"managementOnly": false,
"managementInterface": false,
"mode": "ROUTED",
"linkState": "UP",
"mtu": 1500,
"enabled": true,
"macAddress": null,
"standbyMacAddress": null,
"pppoe": null,
"speedType": "AUTO",
"duplexType": "AUTO",
"present": true,
"tenGigabitInterface": false,
"gigabitInterface": false,
```

```
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
```

```
"type": "physicalinterface",
```

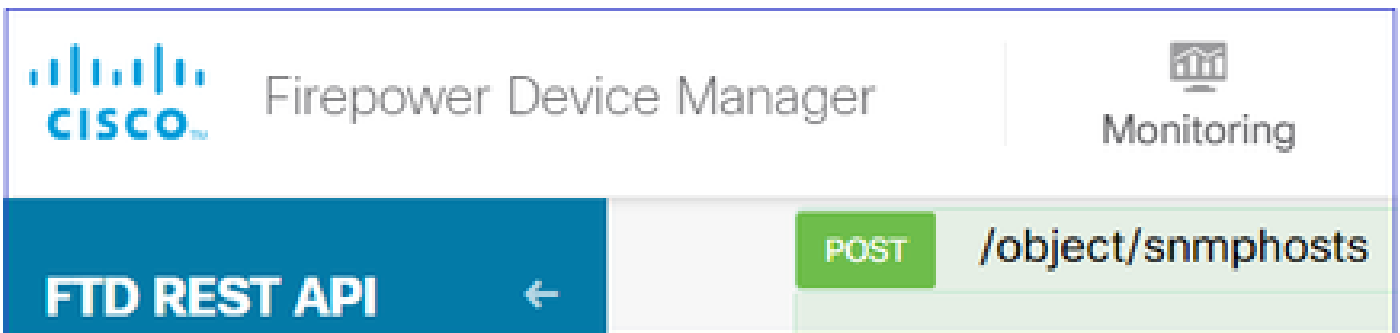
```
"links": {
"self": "https://10.62.148.231/api/fdm/v6/devices/default/interfaces/fc3d07d4-49d2-11eb-85a8-65aec636a0fc"
}
},
```

هنا رتقا مزلي يتل تانايبال لى ع يوتحت لخدال ي ف ةهجاو ل ةيؤر كنكمي JSON تانايب نم  
مداخ SNMP:

- رادصال: kkpki bju6qro
- لخد، iid: fc3d07d4-49d2-11eb-85a8-65aec636a0fc، مسال
- ةيؤر ل ةهجاو ل: عونل

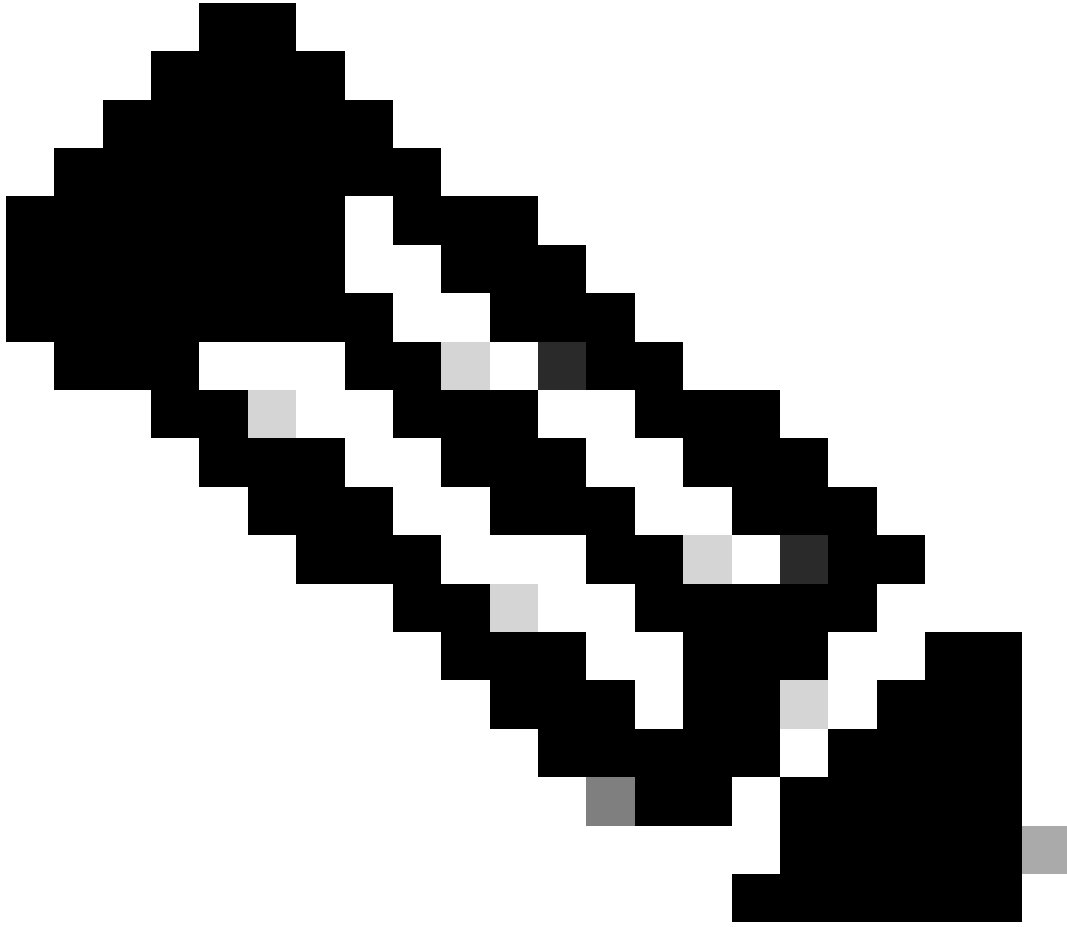
5. دي دج SNMPv3 فيضم عاشنإ.

م ت SNMP ددح ، "FDM ل API) تاقېب طتلا ةج مر ب ةه جاو ف شك تسم" ي ف  
SNMP ل فسأ /SNMPHosts/ نئاك/ ل حر ت



اق فو بل ا ق ل ا ل ا ة ق با س ل ا ت ا و ط خ ل ا ن م ت ا ن ا ي ب ل ا ق ص ل و خ س ن . ب ل ا ق ك ا ذ ه JSON م د خ ت س أ  
ك ل ذ ل :

```
{
  "version": null,
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwzw4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    },
    "type": "snmpv3securityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",
    "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
    "type": "physicalinterface"
  },
  "id": null,
  "type": "snmpHost"
}
```




ملاحظة:

- مرسال او رادصل او عونل او ManagerAddress فرعم يف ةميقلا لدبتسا  
1. ةوطخلال نم اهتملتسا يتلا تامولعملاب
- 2. ةوطخلال نم اهتملتسا يتلا تامولعملاب ةقداصلال يف ةميقلا لدبتسا
- 3. ةوطخلال نم اهتملتسا يتلا تانايبلااب ةهجاووال يف ةميقلا لدبتسا  
وه عونل او، ةقداصل م دجوت ال، SNMP2 لوكوتوربل ةبسنلاب  
snmpv3securityConfiguration نم ال دب snmpv2csecurityConfiguration.

---

يساسأل صنللا مسق ىلإ ةلدعملال JSON تانايب خسنال


Firepower Device Manager
Monitoring
Policies
Objects
Device: FP1120-1

---

**FTD REST API** ←

API Explorer

Error Catalog

Response Content Type application/json

**Parameters**

Parameter	Value	Description
body	<pre>{   "version": null,   "name": "snmpv3-host",   "description": null,   "managerAddress": {     "version": "bsha3bhghu3vmk",     "name": "snmpHost", </pre>	

Parameter content type: application/json

(API) تاقى بطلت الة حمر بة هجاو عاعدتس اذى فننتل !ةلوا حمر ل رزلا ددحو لفسأ ىل اذى رمرتلاب مق 200. ةباجتسالا زمرة اجراب ةحجان ةملاك موقت

**FTD REST API** ←

API Explorer

Error Catalog

**Request URL**

https://10.62.148.231/api/fdm/v6/object/snmphosts

**Response Body**

```
{
  "version": "gneswdadd3isp",
  "name": "snmpv3-host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vm",
    "name": "snmpHost",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "authentication": {
      "version": "bmwzw4iw7php7",
      "name": "snmpUser",
      "id": "65da6c50-49df-11eb-a432-e7823944dabc",
      "type": "snmpuser"
    }
  }
},
```

**Response Code**

200

ىل عالطالا كنكمى .تارىي غتلا رشنو FDM ل (GUI) ةىموسرلا مدختس ملة هجاو ىل لقتنا

مظعم SNMP نيوكت:

**Pending Changes**

✓ **Last Deployment Completed Successfully**  
29 Dec 2020 02:32 PM. [See Deployment History](#)

Deployed Version (29 Dec 2020 02:32 PM)	Pending Version
<b>+ Network Object Added: snmpHost</b>	
-	subType: Host
-	value: 192.168.203.61
-	isSystemDefined: false
-	dnsResolution: IPV4_ONLY
-	description: SNMP Server Host
-	name: snmpHost
<b>+ snmpHost Added: snmpv3-host</b>	
-	udpPort: 162
-	pollEnabled: true
-	trapEnabled: true
-	name: snmpv3-host
snmpInterface:	
-	inside
managerAddress:	
-	snmpHost
securityConfiguration.authentication:	
-	snmpUser

MORE ACTIONS ▾ CANCEL DEPLOY NOW ▾

## SNMP v2c

ىل ةجاحب لازت ال نكلو مدختسم عاشن ةل ةجاحت ال v2c ل ةبسنلاب:

1. SNMPv3 مسق ةف فوصوم ل لثم) ةكبش نئاك نيوكت عاشن ةل.
2. SNMPv3 مسق ةف فوصوم وه امك) ةهءاول تامولعم ةلع لوصحلا.
3. ةءء SNMPv2c ففضم نئاك عاشن ةل.

هءه SNMPv2c نئاك ةشنت ةل JSON ةلومح نم ةنءع هءه:

```
{
  "version": null,
  "name": "snmpv2-Host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpv4hostgrp",
    "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
    "type": "networkobject"
  },
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
```

```

"community": "cisco123",
"type": "snmpv2securityconfiguration"
},
"interface": {
"version": "kkpkibjlu6qro",
"name": "inside",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmpv2host"
}

```

JSON رولومح رشنل POST بولسأ مدختسأ:

The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. The left sidebar shows 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main content area is titled 'Parameters' and shows a table with columns 'Parameter', 'Value', and 'Description'. A single parameter named 'body' is listed, with its value being a JSON object:
 

```

{
  "version": null,
  "name": "snmpv2-Host",
  "description": null,
  "managerAddress": {
    "version": "bsha3bhghu3vmk",
    "name": "snmpv4hostgrp",
  }
}

```

 The 'Response Content Type' dropdown is set to 'application/json', and the 'Parameter content type' dropdown is also set to 'application/json'.

ةجمر بةهجاو اءاعدتسإ ذيفننل "!جورخلال ةبرجت" رزلا ددحو لفسأ لىل ريرمتلاب مق ةباجتسالال زمر عاجراب ةحجان ةملاك م موقت (API) تاقىببطلال

**FTD REST API** ←

API Explorer

Error Catalog

**Request URL**

https://10.62.148.231/api/fdm/v6/object/snmphosts

**Response Body**

```

{
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "community": "*****",
    "type": "snmpv2csecurityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",
    "hardwareName": "Ethernet1/2",
    "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
    "type": "physicalinterface"
  },
  "id": "1bfbd1f0-4ac6-11eb-a432-e76cd376bca7",
  "type": "snmpHost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmphosts/1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
  }
}

```


**Response Code**

200


## SNMP نيوكت ةلازا

1. ةوطخلال

SNMP (SNMP > /object/snmpHost): فيضم تامولعم ىلع لوصحلل



Firepower Device Manager



Monitoring

**FTD REST API** ←

GET

**/object/snmphosts**

ةجمر ب ةهجاو ءاعدتسا ذيفنتل "جورخلال ةبرجت" رزلا ددحو لفسأ ىلإ ريرمتلاب مق ةباجتسالال زمر عاجراب ةحجان ةملاك موقت (API) تاقيبطتلال

هتلازا ديرت يذلا snmpHost نئلكال فرعم ظحال. تانئلكلاب ةمئاق ىلع لصحت

```

{
  "items": [
    {
      "version": "ofaasthu26u1x",
      "name": "snmpv2-Host",
      "description": null,
      "managerAddress": {

```

```

"version": "bsha3bhghu3vm",
"name": "snmpHost",
"id": "1d10ce6d-49de-11eb-a432-e320cd56d5af",
"type": "networkobject"
},
"udpPort": 162,
"pollEnabled": true,
"trapEnabled": true,
"securityConfiguration": {
"community": "*****",
"type": "snmpv2csecurityconfiguration"
},
"interface": {
"version": "kkpkibjlu6qro",
"name": "inside",
"hardwareName": "Ethernet1/2",
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": "1bfbd1f0-4ac6-11eb-a432-e76cd376bca7",
"type": "snmpHost",
"links": {
"self": "https://10.62.148.231/api/fdm/v6/object/snmpHosts/1bfbd1f0-4ac6-11eb-a432-e76cd376bca7"
}
},

```

## 2. عوطخل

1: عوطخل يف هتعمج يذلا فرع مالا قصل. `SNMP > /object/snmpHost{objId}` يف فذحل رايف رتخأ:

The screenshot shows the FTD REST API interface. On the left is a sidebar with 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main content area has a red 'DELETE' button and the endpoint `/object/snmpHosts/{objId}`. Below this, there are 'Implementation Notes' stating 'This API call is not allowed on the standby unit in an HA pair.' and a 'Parameters' table with one entry: `objId` with the value `1bfbd1f0-4ac6-11eb-a432-e76cd376bca7`.

عجم رب ههجاو اعادتس اذيفنتل! "جورخل ابرجت" رزلا ددحو لفسأ اى ايرم تلاب مق  
 400 اجاتسالا زمر عمالكمال عجت. (API) تاقىببطلال



## Response Code

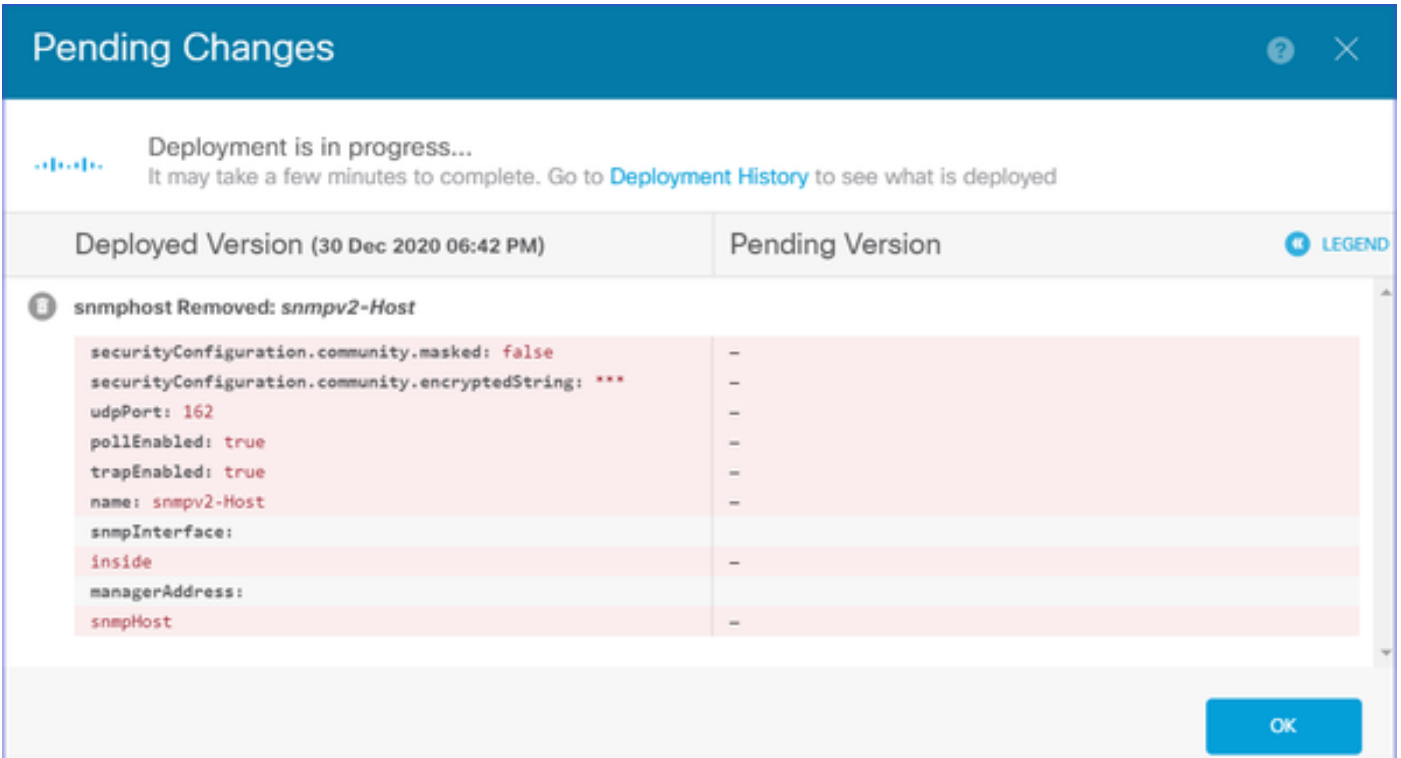
400

## Response Headers

```
{
  "accept-ranges": "bytes",
  "cache-control": "no-cache, no-store",
  "connection": "close",
  "content-type": "application/json;charset=UTF-8",
  "date": "Wed, 30 Dec 2020 18:00:41 GMT",
  "expires": "0",
  "pragma": "no-cache",
  "server": "Apache",
  "strict-transport-security": "max-age=63072000; includeSubdomains; preload, max-age=31536000 ; includeSubDomains",
  "transfer-encoding": "chunked",
  "x-content-type-options": "nosniff",
  "x-frame-options": "SAMEORIGIN, SAMEORIGIN",
  "x-xss-protection": "1; mode=block"
}
```

3. ةوطخل

رشي التل رشن:



**Pending Changes** [?] [X]

Deployment is in progress...  
It may take a few minutes to complete. Go to [Deployment History](#) to see what is deployed

Deployed Version (30 Dec 2020 06:42 PM)	Pending Version
<b>snmpHost Removed: snmpv2-Host</b>	
securityConfiguration.community.masked: false	-
securityConfiguration.community.encryptedString: ***	-
udpPort: 162	-
pollEnabled: true	-
trapEnabled: true	-
name: snmpv2-Host	-
snmpInterface:	-
inside	-
managerAddress:	-
snmpHost	-

OK

فيضم التل تام ولعم ةلازا يل ع رشن التل لمعي:

```
<#root>
```

```
FP1120-1#
```

```
show run snmp-server
```

```
snmp-server group AUTH v3 auth
snmp-server group PRIV v3 priv
snmp-server group NOAUTH v3 noauth
snmp-server location null
```

```
snmp-server contact null
snmp-server community *****
```

## سنمپ واک جی 2c ل ش ف

<#root>

root@kali2:~#

```
snmpwalk -v2c -c cisco123 -OS 192.168.203.71
```

Timeout: No Response from 192.168.203.71

بیت ترتل اذہب تانئ الکال فذح بجی، 3 رادصل لل ةبسن للاب.

1. (204 وه حجان لل عاجر لل زمر) SNMP فیضم.
2. (204 وه حجان لل عاجر لل زمر) SNMP لوكوت ورب مدخت سم.

أطخ لل اذہ یلع لصحت، ئطاخل بیت ترتل لاب تانئ الکال فذح تل واح اذہ:

```
{
  "error": {
    "severity": "ERROR",
    "key": "Validation",
    "messages": [
      {
        "description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmpv3-host1. You must remove the object from all parts of the configuration before you can delete it.",
        "code": "deleteObjWithRel",
        "location": ""
      }
    ]
  }
}
```

## ةحصل لل نم ققحت لل

### SNMP v3 نم ققحت لل

SNMP نیوكت نم ققحت لل FTD ب ةصاخل (CLI) رم او ال رطس ةه جاو یل لقت نا، رشن لل دع ب ائی اق لت engineID ةمیق ءاشن ا مت ه نا ظ حال.

<#root>

FP1120-1#

```
connect ftd
```

```
>
```

```
system support diagnostic-cli
```

```
Attaching to Diagnostic CLI ... Press 'Ctrl+a then d' to detach.  
Type help or '?' for a list of available commands.
```

```
FP1120-1>
```

```
enable
```

```
Password:
```

```
FP1120-1#
```

```
show run all snmp-server
```

```
snmp-server group AUTH v3 auth  
snmp-server group PRIV v3 priv  
snmp-server group NOAUTH v3 noauth  
snmp-server user snmpUser PRIV v3 engineID 80000009febdf0129a799ef469aba2d5fcf1bfd7e86135a1f8 encrypted  
snmp-server listen-port 161  
snmp-server host inside 192.168.203.61 version 3 snmpUser udp-port 162  
snmp-server location null  
snmp-server contact null  
snmp-server community *****  
snmp-server enable traps snmp authentication linkup linkdown coldstart warmstart  
no snmp-server enable traps syslog  
no snmp-server enable traps ipsec start stop  
no snmp-server enable traps entity config-change fru-insert fru-remove fan-failure power-supply power-s  
no snmp-server enable traps memory-threshold  
no snmp-server enable traps interface-threshold  
no snmp-server enable traps remote-access session-threshold-exceeded  
no snmp-server enable traps connection-limit-reached  
no snmp-server enable traps cpu threshold rising  
no snmp-server enable traps ikev2 start stop  
no snmp-server enable traps nat packet-discard  
no snmp-server enable traps config  
no snmp-server enable traps failover-state  
no snmp-server enable traps cluster-state  
snmp-server enable oid mempool  
snmp-server enable
```

## ي ع ا ر ش ر ي س ر ا ب ت خ |

```
root@kali2:~# snmpwalk -v3 -l authPriv -u snmpUser -a SHA -A cisco123 -x AES -X cisco123 192.168.203.71  
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.  
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663  
iso.3.6.1.2.1.1.3.0 = Timeticks: (1616700) 4:29:27.00  
iso.3.6.1.2.1.1.4.0 = STRING: "null"  
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"  
iso.3.6.1.2.1.1.6.0 = STRING: "null"  
iso.3.6.1.2.1.1.7.0 = INTEGER: 4  
...
```

## نم ققحتال SNMP v2c

```
FP1120-1# show run snmp-server
snmp-server host inside 192.168.203.61 community ***** version 2c
snmp-server location null
snmp-server contact null
snmp-server community *****
```

## SnmpWalk J v2c:

```
root@kali2:~# snmpwalk -v2c -c cisco123 -OS 192.168.203.71
iso.3.6.1.2.1.1.1.0 = STRING: "Cisco Firepower Threat Defense, Version 6.7.0 (Build 65), ASA Version 9.
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.9.1.2663
iso.3.6.1.2.1.1.3.0 = Timeticks: (10482200) 1 day, 5:07:02.00
iso.3.6.1.2.1.1.4.0 = STRING: "null"
iso.3.6.1.2.1.1.5.0 = STRING: "FP1120-1"
iso.3.6.1.2.1.1.6.0 = STRING: "null"
iso.3.6.1.2.1.1.7.0 = INTEGER: 4
```

## اهحالصإو ءاطخال فاشكتسا

ةياملال رادج لىل عبتتلاب طاقتلال نيكتمت:

```
<#root>
```

```
FP1120-1#
```

```
capture CAPI trace interface inside match udp any any eq snmp
```

مزال ةيؤر لىل كتردق نم ققحتو طيسبال لقننل ةادأ مدختسأ:

```
<#root>
```

```
FP1120-1#
```

```
show capture
```

```
capture CAPI type raw-data trace interface inside
```

```
[Capturing - 3137 bytes]
```

```
match udp any any eq snmp
```

طاقات لال تايوت حم:

<#root>

FP1120-1#

show capture CAPI

154 packets captured

```
1: 17:04:16.720131      192.168.203.61.51308 > 192.168.203.71.161:  udp 39
2: 17:04:16.722252      192.168.203.71.161 > 192.168.203.61.51308:  udp 119
3: 17:04:16.722679      192.168.203.61.51308 > 192.168.203.71.161:  udp 42
4: 17:04:16.756400      192.168.203.71.161 > 192.168.203.61.51308:  udp 51
5: 17:04:16.756918      192.168.203.61.51308 > 192.168.203.71.161:  udp 42
```

ىلع لوصحلل SNMP تابلط س او تابلط رهظت SNMP م داخ تايئاصح| تادادع نأ نم ققحت  
ي:يلات ىلع لوصحلل و SNMP تابلط س او تابلط

<#root>

FP1120-1#

show snmp-server statistics

62

SNMP packets input

```
0 Bad SNMP version errors
0 Unknown community name
0 Illegal operation for community name supplied
0 Encoding errors
```

58 Number of requested variables

```
0 Number of altered variables
0 Get-request PDUs
```

58 Get-next PDUs

```
0 Get-bulk PDUs
0 Set-request PDUs (Not supported)
```

58 SNMP packets output

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

58 Response PDUs

0 Trap PDUs

نراق NLP يـلـخـاـدـلـا يـلـا un-nat طـبـرـلـا .لـخـدم ةـمـزـح عـبـتـت

<#root>

FP1120-1#

show capture CAPI packet-number 1 trace

30 packets captured

1: 17:04:16.720131 192.168.203.61.51308 > 192.168.203.71.

161

: udp 39

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: UN-NAT

Subtype: static

Result: ALLOW

Config:

Additional Information:

NAT divert to egress interface nlp\_int\_tap(vrfid:0)

Untranslate 192.168.203.71/161 to 169.254.1.3/4161

Phase: 4

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

Phase: 5  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:

Phase: 6  
Type: IP-OPTIONS  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:

Phase: 7  
Type: NAT  
Subtype: rpf-check  
Result: ALLOW  
Config:  
Additional Information:

Phase: 8  
Type: NAT  
Subtype: per-session  
Result: ALLOW  
Config:  
Additional Information:

Phase: 9  
Type: FLOW-CREATION  
Subtype:  
Result: ALLOW  
Config:  
Additional Information:  
New flow created with id 1078, packet dispatched to next module

Phase: 10  
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP  
Subtype: Resolve Preferred Egress interface  
Result: ALLOW  
Config:  
Additional Information:  
**Found next-hop 169.254.1.3 using egress ifc nlp\_int\_tap(vrfid:0)**

Phase: 11  
Type: ADJACENCY-LOOKUP  
Subtype: Resolve Nexthop IP address to MAC  
Result: ALLOW  
Config:  
Additional Information:  
Found adjacency entry for Next-hop 169.254.1.3 on interface nlp\_int\_tap  
Adjacency :Active  
MAC address 3208.e2f2.b5f9 hits 0 reference 1

Result:  
**input-interface: inside(vrfid:0)**

```
input-status: up
input-line-status: up

output-interface: nlp_int_tap(vrfid:0)

output-status: up
output-line-status: up

Action: allow
```

SNMP نيوكت نم عزجك ايئاق لت NAT ةدعاق رشن متي

```
<#root>
```

```
FP1120-1#
```

```
show nat
```

```
Manual NAT Policies (Section 1)
```

```
1 (nlp_int_tap) to (inside) source dynamic nlp_client_0_192.168.203.61_intf4 interface destination stat
translate_hits = 0, untranslate_hits = 0
```

```
Auto NAT Policies (Section 2)
```

```
...
```

```
2 (nlp_int_tap) to (inside) source static nlp_server_0_snmp_intf4 interface service udp 4161 snmp
```

```
translate_hits = 0, untranslate_hits = 2
```

SNMP رورم ةكرحل UDP 4161 عم تسي، يف لخال ذفنم لاي

```
<#root>
```

```
>
```

```
expert
```

```
admin@FP1120-1:~$
```

```
sudo netstat -an | grep 4161
```

```
Password:
```

```
udp 0 0 169.254.1.3:4161 0.0.0.0:*
```

```
udp6 0 0 fd00:0:0:1::3:4161 :::*
```

ارظن لخدم لابة صخال SNMP ةمزح طاقسا متي، لمالك لريغ/ححصلا ريغ نيوكت لة لاي ف  
unnat: ةلحرم دوجو مدعل



<#root>

FP1120-1#

show cap CAPI packet-number 1 trace

6 packets captured

1: 18:36:35.868485 192.168.203.61.50105 > 192.168.203.71.

161

: udp 42

Phase: 1

Type: CAPTURE

Subtype:

Result: ALLOW

Config:

Additional Information:

MAC Access list

Phase: 2

Type: ACCESS-LIST

Subtype:

Result: ALLOW

Config:

Implicit Rule

Additional Information:

MAC Access list

Phase: 3

Type: ROUTE-LOOKUP

Subtype: No ECMP load balancing

Result: ALLOW

Config:

Additional Information:

Destination is locally connected. No ECMP load balancing.

Found next-hop 192.168.203.71 using egress ifc identity(vrfid:0)

Phase: 4

Type: NAT

Subtype: per-session

Result: ALLOW

Config:

Additional Information:

Phase: 5

Type: ACCESS-LIST

Subtype:

Result: DROP

Config:

Implicit Rule

Additional Information:

Result:

input-interface: inside(vrfid:0)

input-status: up

input-line-status: up

Action: drop

Drop-reason: (acl-drop) Flow is denied by configured rule, Drop-location: frame 0x0000557415b6347d flow

لمهم طبر لخدملا نأ FTDLINA syslogs رهظي:

<#root>

FP1120-1#

show log | include 161

Dec 30 2020 18:36:38: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.

Dec 30 2020 18:36:39: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.

## ةبوجأو ةلئسأ

SNMP لئاسر لاسرال FTD ةرادإ ةهجاو مادختسا يننكمي له .س

ايلاح موعدم ريغ اذه ،ال

ةجارل SNMP لوكوتوربل (API) تاقيبطتلا ةجرمرب ةهجاومعد :ةلصللا وذنيسحتلا بي ع  
[ةهجاول نيظوملا NGFW-MGMT](#)

## ةلص تاذا تامولعم

- [6.7 رادصلال ، Firepower ةزهجأ ةرادال Cisco نم Firepower Threat Defense نيوكت ليلد](#)
- [Cisco Firepower ديدته نعا فدللا تاقيبطت ةجرمرب ةهجاول ليلد](#)
- [6.7.0 رادصلال ، Cisco Firepower رادصلال تاظالم](#)

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 تامةرتل هذه ةقء نء اهءل وئس م Cisco  
Systems (رفوتم طبارل) ةلصلأل ةزءل ءن إل دن تسمل