

SNMP op Firepower FDM configureren en problemen oplossen

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Configureren](#)

[SNMP v3](#)

[SNMP v2c](#)

[SNMP-configuratie verwijderen](#)

[Verifiëren](#)

[SNMP v3-verificatie](#)

[SNMP v2c-verificatie](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u Simple Network Management Protocol (SNMP) op Firepower Device Management kunt inschakelen op versie 6.7 met REST API.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Firepower Threat Defence (FTD), beheerd door Firepower Device Management (FDM) op versie 6.7
- Kennis van REST API
- Kennis van SNMP

Gebruikte componenten

Firepower Threat Defence (FTD), beheerd door Firepower Device Management (FDM) op versie 6.7.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

Nieuwe functies op 6.7

FTD Device REST API ondersteunt configuratie en beheer van SNMP-server, gebruikers, host en hostgroepen. Met de ondersteuning van SNMP FTD Device REST API in FP 6.7:

- Een gebruiker kan SNMP configureren via FTD Device REST API om het netwerk te beheren
- SNMP-server, -gebruikers en host/host-groepen kunnen worden toegevoegd/bijgewerkt of beheerd via FTD Device REST API.

De voorbeelden in het document beschrijven de configuratiestappen die door FDM API Explorer zijn genomen.

Opmerking: SNMP kan alleen worden geconfigureerd via REST API als FTD versie 6.7 uitvoert en wordt beheerd door FDM

Overzicht van functies - Ondersteuning van SNMP FTD Device REST API

- Deze eigenschap voegt nieuwe FDM URL-endpoints toe die specifiek zijn voor SNMP.
- Deze nieuwe API's kunnen worden gebruikt om SNMP te configureren voor opiniepeilingen en vallen om systemen te bewaken.
- Na SNMP-configuratie via API's zijn de Management Information Bases (MIB's) op de FirePOWER-apparaten beschikbaar voor opiniepeilingen of voor meldingen in de trap op NMS/SNMP-client.

SNMP API/URL-endpoints

URL	Methoden	Models
/devicesettings/default/snmpservers	KRIJGEN	SNMP-server
/apparaten/standaard/servers/{objId}	PUT, GET	SNMP-server
/object/snmphosts	POST, GET	SNMPPost
/object/snmphosts/{objId}	PLAATSEN, VERWIJDEREN, VERKRIJGEN	SNMPPost
/object/snmpusergroups	POST, GET	SNMP-gebruikersgroep
/object/snmpusergroups/{objId}	PLAATSEN, VERWIJDEREN, VERKRIJGEN	SNMP-gebruikersgroep
/object/snmpusers	POST, GET	SNMP-gebruiker
/object/snmpusers/{objId}	PLAATSEN, VERWIJDEREN,	SNMP-gebruiker

VERKRIJGEN

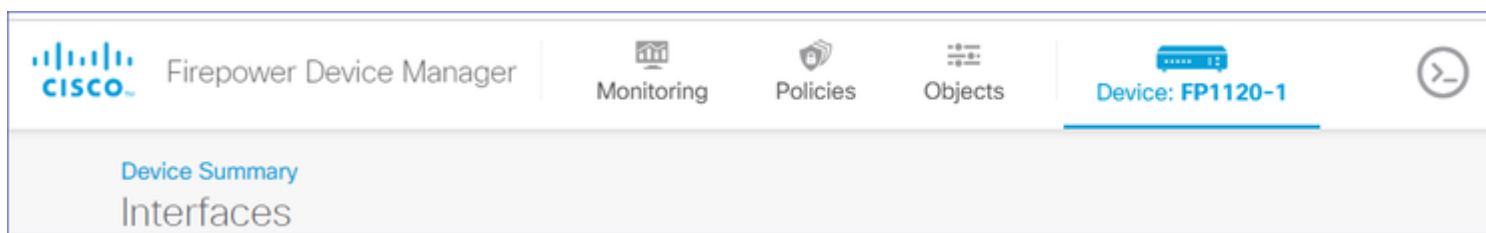
Configureren

- De SNMP-host heeft 3 primaire versies
- SNMP V1
 - SNMP V2C
 - SNMP V3
- Elk van deze heeft een specifiek formaat voor "securityConfiguration".
 - Voor V1 en V2C: Het bevat een "Community String" en een "type" veld dat de configuratie identificeert als V1 of V2C.
 - Voor SNMP V3: Het bevat een geldige SNMP V3-gebruiker en een veld "type" dat de configuratie identificeert als V3.

SNMP v3

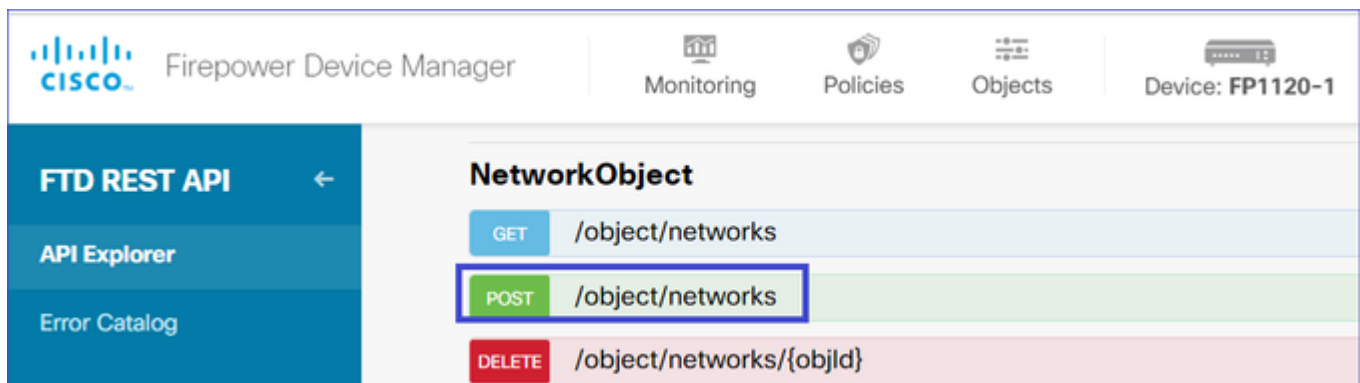
1. Open de FDM API Explorer

Om toegang te krijgen tot de FDM REST API Explorer vanuit de FDM GUI selecteert u de 3 punten en vervolgens **API Explorer**. U kunt ook naar URL https://FDM_IP/#/api-explorer navigeren:



2. Netwerkbobjectconfiguratie

Maak een nieuw netwerkbobject voor de SNMP-host: selecteer op FDM API Explorer NetworkObject en vervolgens **POST/object/netwerken**:



De SNMP Host JSON-indeling is als volgt. Plakt dit JSON in het hoofdgedeelte en wijzig het IP-adres op "waarde" zodat dit overeenkomt met het IP-adres van de SNMP-host:

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

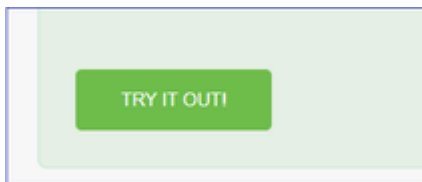
The screenshot shows the Cisco Firepower Device Manager (FDM) interface. The top navigation bar includes 'Monitoring', 'Policies', 'Objects', and 'Device: FP1120-1'. The left sidebar has 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area displays the 'Parameters' section for a parameter named 'body'. The 'Value' field contains a JSON object:

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

 The 'Parameter content type' is set to 'application/json'. On the right, a 'Model' section shows the schema for the parameter, with an 'Example Value' field containing a JSON object:

```
{
  "version": "string",
  "name": "string",
  "description": "string",
  "subType": "HOST",
  "value": "string",
  "isSystemDefined": true,
  "dnsResolution": "IPV4_O",
  "id": "string",
  "type": "networkobject"
}
```

Scroll naar beneden en selecteer de knop TRY IT OUT! om de API-oproep uit te voeren. Een succesvolle oproep retourneert Respons Code 200.

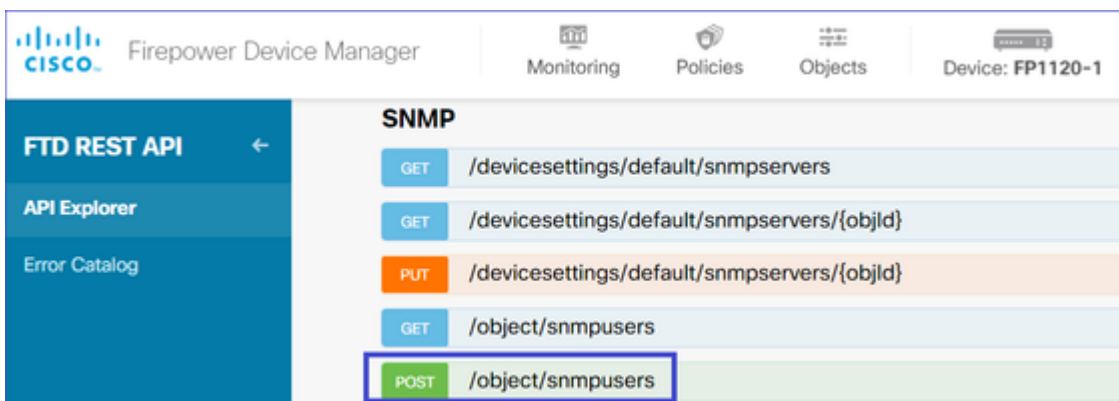


Kopieer de JSON-gegevens van de responsinstantie naar een kladblok. Later moet u de informatie over de SNMP-host invullen.



3. Een nieuwe SNMPv3-gebruiker maken

Selecteer op FDM API Explorer SNMP en vervolgens POST/object/snmpusers



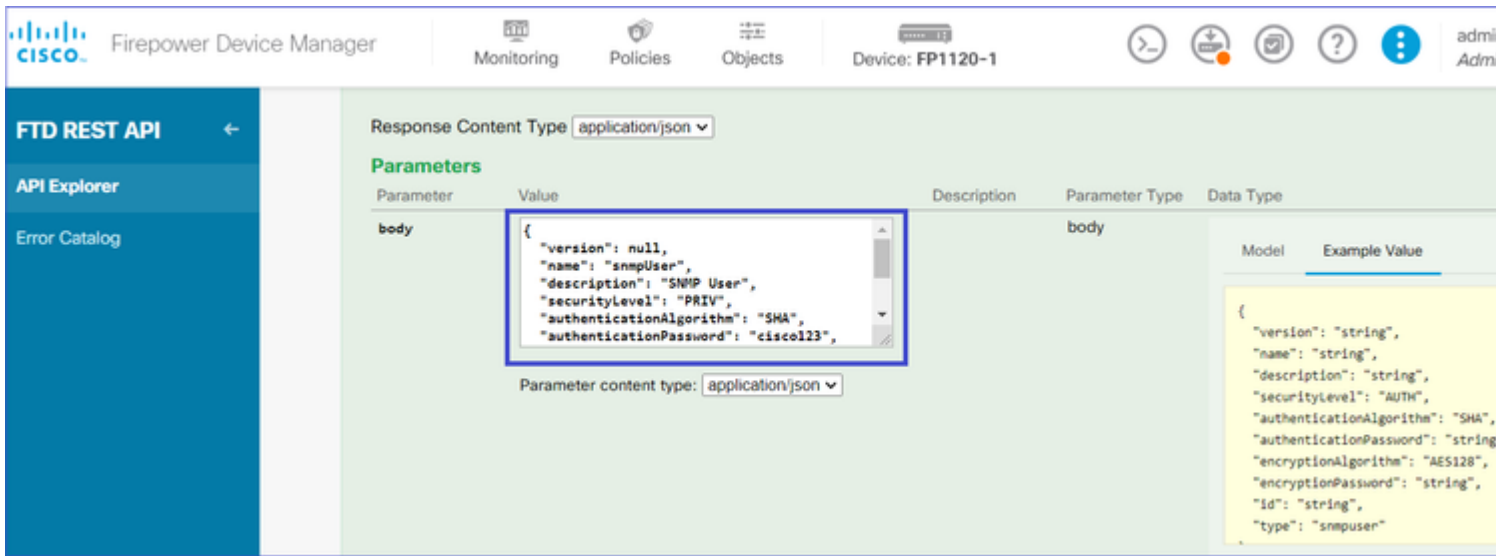
Kopieer deze JSON-gegevens naar een blocnote en wijzig de secties die u interesseert (bijvoorbeeld "authenticatiePassword", "encryptiePassword" of de algoritmen):

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

Waarschuwing: de wachtwoorden in de voorbeelden zijn alleen voor demonstratiedoeleinden

gebruikt. Zorg er in een productieomgeving voor dat u sterke wachtwoorden gebruikt

Kopieer de aangepaste JSON-gegevens naar het hoofdgedeelte:



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 displays the 'Parameters' table for the REST API. The 'body' parameter is highlighted with a blue box, showing the following JSON value:

```
{
  "version": null,
  "name": "snmpUser",
  "description": "SNMP User",
  "securityLevel": "PRIV",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "cisco123",
}
```

The 'Parameter content type' is set to 'application/json'. On the right, the 'Model' section shows an 'Example Value' for the same parameter:

```
{
  "version": "string",
  "name": "string",
  "description": "string",
  "securityLevel": "AUTH",
  "authenticationAlgorithm": "SHA",
  "authenticationPassword": "string",
  "encryptionAlgorithm": "AES128",
  "encryptionPassword": "string",
  "id": "string",
  "type": "snmpuser"
}
```

Scroll naar beneden en selecteer de knop **IT OUT!** om de API-aanroep uit te voeren. Een succesvolle oproep retourneert Respons Code 200. Kopieer de JSON-gegevens van de responsinstantie naar een kladblok. Later moet u de informatie over de SNMP-gebruiker invullen.

The screenshot shows the Firepower Device Manager interface. On the left, the 'FTD REST API' menu is open, with 'API Explorer' selected. The main area displays the details of an API call:

- Request URL:** `https://10.62.148.231/api/fdm/v6/object/snmpusers`
- Response Body:**

```
{
  "version": "bmwzw4iw7php7",
  "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/"
  }
}
```
- Response Code:** 200

4. Krijg interfaceinformatie

Selecteer in FDM API Explorer de optie Interface en vervolgens **GET /devices/default/interfaces**. U moet informatie verzamelen via de interface die verbinding maakt met de SNMP-server.

The screenshot shows the Firepower Device Manager interface. The 'FTD REST API' menu is open, and the 'GET /devices/default/interfaces' endpoint is selected.

Scroll naar beneden en selecteer de knop **IT OUT!** om de API-aanroep uit te voeren. Een succesvolle oproep retourneert Respons Code 200. Kopieer de JSON-gegevens van de responsinstantie naar een kladblok. Later moet je informatie invullen over de interface.

The screenshot shows an API Explorer interface for the endpoint `https://10.62.148.231/api/fdm/v6/devices/default/interfaces`. The response body is a JSON object with the following structure:

```

{
  "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,
  }
}

```

The response code is 200.

Let op de interface "version", "name", "id" en "type" van de JSON-gegevens. Voorbeeld van een JSON-gegevens van de interface binnenin:

```

<#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"
}
},

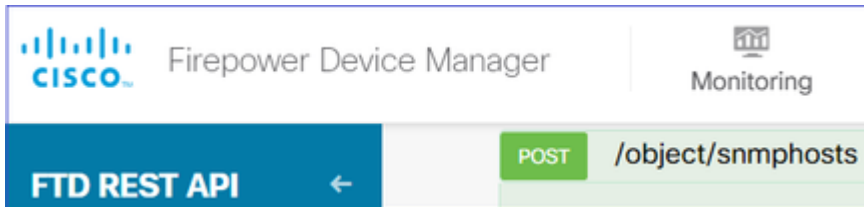
```

Op basis van de JSON-gegevens kunt u zien dat de interface 'inside' deze gegevens bevat die aan de SNMP-server moeten worden gekoppeld:

- "versie": "kkpkibjlu6qro"
- "naam": "binnenkant",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "type": "fysieke interface",

5. Een nieuwe SNMPv3-host maken

Selecteer op FDM API Explorer SNMP en vervolgens POST/**object/snmphosts/** onder SNMP



Gebruik deze JSON als sjabloon. Kopieer en plak gegevens uit vorige stappen naar de sjabloon als volgt:

```
{
"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"
}
```

Opmerking:

- Vervang de waarde in managerAddress-id, type, versie en naam door de informatie die u van Stap 1 hebt ontvangen
- Vervang de waarde in verificatie met de informatie die u van Stap 2 hebt ontvangen
- Vervang de waarde in interface met de gegevens die u van Stap 3 hebt ontvangen
- Voor SNMP2 is er geen verificatie en het type is snmpv2security configuratie in plaats van snmpv3security configuratie

Kopieert de gewijzigde JSON-gegevens naar het hoofdgedeelte.

Response Content Type: application/json

Parameters

Parameter	Value	Description
body	<pre>{ "version": null, "name": "snmpv3-host", "description": null, "managerAddress": { "version": "bsha3bhghu3vmk", "name": "snmpHost", "id": "1d10ce6d-49de-11eb-a432-e320cd56d5af", "type": "networkobject" } }</pre>	

Parameter content type: application/json

Scroll naar beneden en selecteer de knop **IT OUT!** om de API-aanroep uit te voeren. Een succesvolle oproep retourneert Respons Code 200.

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

Navigeer naar FDM GUI en implementeer de wijzigingen. U kunt de meeste SNMP-configuraties zien:

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																				
<p>Network Object Added: snmpHost</p> <table border="1"> <tr><td>-</td><td>subType: Host</td></tr> <tr><td>-</td><td>value: 192.168.203.61</td></tr> <tr><td>-</td><td>isSystemDefined: false</td></tr> <tr><td>-</td><td>dnsResolution: IPV4_ONLY</td></tr> <tr><td>-</td><td>description: SNMP Server Host</td></tr> <tr><td>-</td><td>name: snmpHost</td></tr> </table>		-	subType: Host	-	value: 192.168.203.61	-	isSystemDefined: false	-	dnsResolution: IPV4_ONLY	-	description: SNMP Server Host	-	name: snmpHost								
-	subType: Host																				
-	value: 192.168.203.61																				
-	isSystemDefined: false																				
-	dnsResolution: IPV4_ONLY																				
-	description: SNMP Server Host																				
-	name: snmpHost																				
<p>snmpHost Added: snmpv3-host</p> <table border="1"> <tr><td>-</td><td>udpPort: 162</td></tr> <tr><td>-</td><td>pollEnabled: true</td></tr> <tr><td>-</td><td>trapEnabled: true</td></tr> <tr><td>-</td><td>name: snmpv3-host</td></tr> <tr><td colspan="2">snmpInterface:</td></tr> <tr><td>-</td><td>inside</td></tr> <tr><td colspan="2">managerAddress:</td></tr> <tr><td>-</td><td>snmpHost</td></tr> <tr><td colspan="2">securityConfiguration.authentication:</td></tr> <tr><td>-</td><td>snmpUser</td></tr> </table>		-	udpPort: 162	-	pollEnabled: true	-	trapEnabled: true	-	name: snmpv3-host	snmpInterface:		-	inside	managerAddress:		-	snmpHost	securityConfiguration.authentication:		-	snmpUser
-	udpPort: 162																				
-	pollEnabled: true																				
-	trapEnabled: true																				
-	name: snmpv3-host																				
snmpInterface:																					
-	inside																				
managerAddress:																					
-	snmpHost																				
securityConfiguration.authentication:																					
-	snmpUser																				

MORE ACTIONS ▼ CANCEL DEPLOY NOW ▼

SNMP v2c

Voor v2c hoeft u geen gebruiker aan te maken, maar moet u toch:

1. Een netwerkobjectconfiguratie maken (zoals beschreven in het gedeelte SNMPv3)
2. Krijg interfaceinformatie (hetzelfde als beschreven in de SNMPv3-sectie)
3. Een nieuw SNMPv2c-hostobject maken

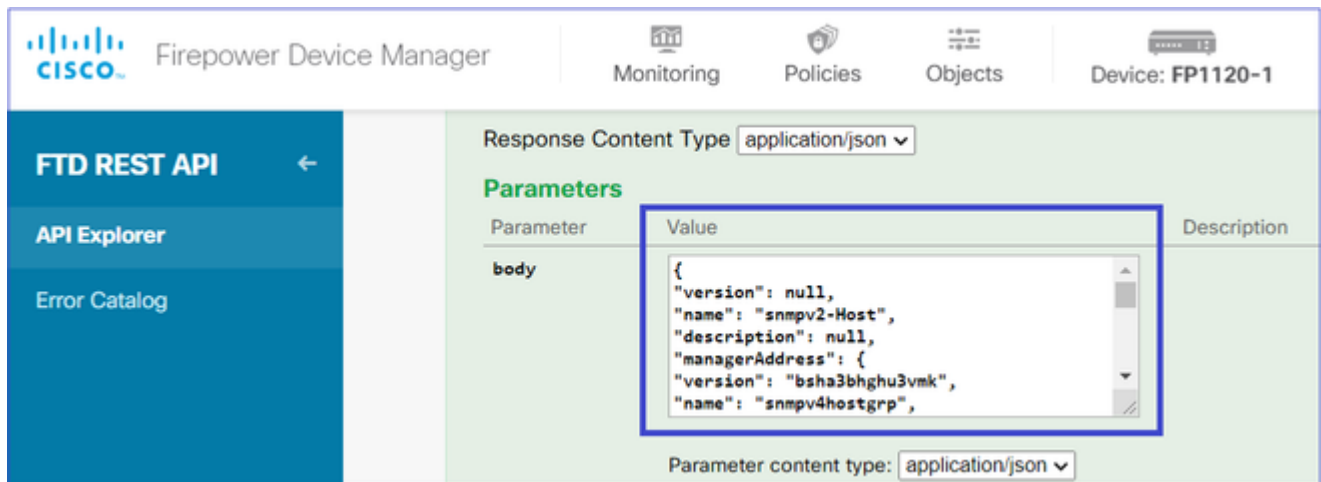
Dit is een voorbeeld van een JSON-payload die een SNMPv2c-object maakt:

```
{
  "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": "snmpv2csecurityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",

```

```
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmpghost"
}
```

Gebruik de POST-methode om de JSON-payload te implementeren:



The screenshot shows the Firepower Device Manager REST API interface. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area is titled 'Response Content Type' with a dropdown set to 'application/json'. Below this is a 'Parameters' table with a single row for 'body'. The value of 'body' is a JSON object:

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

. A 'Parameter content type' dropdown at the bottom is also set to 'application/json'.

Scroll naar beneden en selecteer de knop TRY IT OUT! om de API-oproep uit te voeren. Een succesvolle oproep retourneert Respons Code 200.



The screenshot shows the Firepower Device Manager REST API interface displaying the response of a POST request. The 'Request URL' is `https://10.62.148.231/api/fdm/v6/object/snmpghosts`. The 'Response Body' is a JSON object:

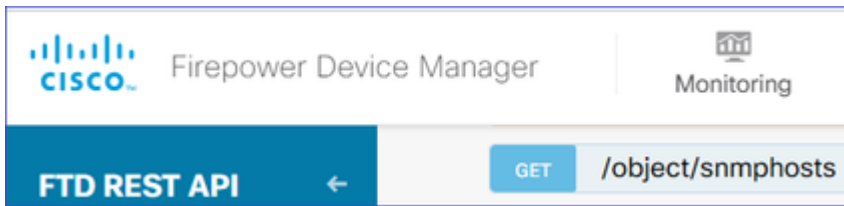
```
{
  "udpPort": 162,
  "pollEnabled": true,
  "trapEnabled": true,
  "securityConfiguration": {
    "community": "*****",
    "type": "snmpv2csecurityconfiguration"
  },
  "interface": {
    "version": "kkpkibjlu6qro",
    "name": "inside",
    "hardwareName": "Ethernet1/2",
    "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
    "type": "physicalinterface"
  },
  "id": "1bfd1f0-4ac6-11eb-a432-e76cd376bca7",
  "type": "snmpghost",
  "links": {
    "self": "https://10.62.148.231/api/fdm/v6/object/snmpghosts/1bfd1f0-4ac6-11eb-a432-e76cd376bca7"
  }
}
```

. The 'Response Code' is 200.

SNMP-configuratie verwijderen

Stap 1.

Ontvang de SNMP-hostinformatie (**SNMP** > /object/snmphosts):



Scroll naar beneden en selecteer de knop TRY IT OUT! om de API-oproep uit te voeren. Een succesvolle oproep retourneert Respons Code 200.

Je krijgt een lijst van objecten. Noteer de id van het snmhost-object dat u wilt verwijderen:

```
<#root>
{
  "items": [
    {
      "version": "ofaasthu26ulx",
      "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"
      }
    },
  ],
}
```

Stap 2.

Kies de optie VERWIJDEREN in **SNMP** > /object/snmphosts{objId}. Plakt het id dat u in stap 1 hebt verzameld:

FTD REST API ←

DELETE /object/snmphosts/{objId}

Implementation Notes
This API call is not allowed on the standby unit in an HA pair.

Parameters

Parameter	Value
objId	1bfbd1f0-4ac6-11eb-a432-e76cd376bca7

Scroll naar beneden en selecteer de knop TRY IT OUT! om de API-oproep uit te voeren. De oproep retourneert Respons code 400.

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"
}
```

Stap 3.

Voer de wijziging in:

Pending Changes ? ×

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
snmpv2-Host Removed: snmpv2-Host	
securityConfiguration.community.masked: false	-
securityConfiguration.community.encryptedString: ***	-
udpPort: 162	-
pollEnabled: true	-
trapEnabled: true	-
name: snmpv2-Host	-
snmpInterface:	-
inside	-
managerAddress:	-
snmpHost	-

OK

De implementatie verwijdert de hostinformatie:

```
<#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 *****
```

snmpwalk voor v2c mislukt:

```
<#root>
```

```
root@kali2:~#
```

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

```
Timeout: No Response from 192.168.203.71
```

Voor v3 moet u de objecten in deze volgorde verwijderen.

1. SNMP-host (de succesvolle retourcode is 204)
2. SNMP-gebruiker (de succesvolle retourcode is 204)

Als u probeert de objecten in de verkeerde volgorde te verwijderen, krijgt u deze fout:

```
<#root>
```

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

Verifiëren

SNMP v3-verificatie

Na de implementatie navigeer je naar de FTD CLI om de SNMP configuratie te controleren. Merk op dat de motor-ID waarde automatisch wordt gegenereerd.

```
<#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 auth sha ca:1b:18:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd priv aes 128 ca:1b:18:f3:62:b1:63:7e:92:34:92:b3:cf:54:86:f9:8e:2a:4c:fd
```

```
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-supply-failure  
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
```

snelwandeltest

<#root>

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 9.1
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
...
```

SNMP v2c-verificatie

<#root>

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 *****
```

momentopname voor v2c:

<#root>

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 9.1
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
```

Problemen oplossen

Opname met overtrekken op de firewall inschakelen:

```
<#root>  
  
FP1120-1#  
  
capture CAPI trace interface inside match udp any any eq snmp
```

Gebruik het hulpmiddel van de wandel en verifieer u de pakketten kunt zien:

```
<#root>  
  
FP1120-1#  
  
show capture  
  
capture CAPI type raw-data trace interface inside  
[Capturing - 3137 bytes]  
  
match udp any any eq snmp
```

De opnameinhoud:

```
<#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
```

Controleer of de SNMP-serverstatistiek tellers SNMP Get of Get-Next-verzoeken en antwoorden tonen:

```
<#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

Een toegangspakket overtrekken. Het pakket is UN-NAT naar de interne NLP-interface:

<#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

De NAT-regel wordt automatisch geïmplementeerd als deel van de SNMP-configuratie:

<#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 static
translate_hits = 0, untranslate_hits = 0
```

Auto NAT Policies (Section 2)

â€

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

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

In de backend poort UDP 4161 luistert naar SNMP-verkeer:

```
<#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 :::*
```

In een geval van onjuiste/onvolledige configuratie wordt het toegang SNMP-pakket verbroken omdat er geen UN-NAT fase is:

```
<#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

FTD LINA-syslogs tonen aan dat het ingangspakket wordt verworpen:

<#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:192.168.2
```

```
Dec 30 2020 18:36:39: %FTD-7-710005: UDP request discarded from 192.168.203.61/50105 to inside:192.168.2
```

Gerelateerde informatie

- [Cisco Firepower Threat Defence Configuration Guide voor Firepower Device Manager, versie 6.7](#)
- [Handleiding voor RUST API voor Cisco Firepower Threat Defence](#)
- [Cisco FirePOWER Releaseopmerkingen, versie 6.7.0](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.