

Configuración y solución de problemas de SNMP en Firepower FDM

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[SNMP v3](#)

[SNMP v2c](#)

[Eliminación de configuración SNMP](#)

[Verificación](#)

[Verificación de SNMP v3](#)

[Verificación de SNMP v2c](#)

[Troubleshoot](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo habilitar el Protocolo simple de administración de red (SNMP) en Firepower Device Management en la versión 6.7 con la API REST.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Firepower Threat Defence (FTD) gestionado por Firepower Device Management (FDM) en la versión 6.7
- Conocimiento de API REST
- Conocimiento de SNMP

Componentes Utilizados

Firepower Threat Defence (FTD) gestionado por Firepower Device Management (FDM) en la versión 6.7.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

Novedades de 6.7

La API REST de dispositivos FTD admite la configuración y gestión de servidores, usuarios, hosts y grupos host SNMP. Con la compatibilidad con la API REST de dispositivos SNMP FTD en FP 6.7:

- Un usuario puede configurar SNMP a través de la API REST de dispositivo FTD para administrar la red
- El servidor SNMP, los usuarios y los grupos host/host se pueden agregar/actualizar o administrar a través de la API REST de dispositivo FTD.

Los ejemplos incluidos en el documento describen los pasos de configuración realizados por el Explorador de la API de FDM.

Nota: SNMP sólo se puede configurar mediante API REST cuando FTD ejecuta la versión 6.7 y FDM lo gestiona

Descripción general de la función: compatibilidad con API REST de dispositivo SNMP FTD

- Esta función añade nuevos terminales URL de FDM específicos de SNMP.
- Estas nuevas API se pueden utilizar para configurar SNMP para sondeos y trampas para monitorear sistemas.
- La configuración posterior a SNMP a través de API, las bases de información de administración (MIB) en los dispositivos Firepower, están disponibles para sondeos o para notificaciones de capturas en NMS/cliente SNMP.

Terminales URL/API SNMP

URL	Métodos	Modelos
/devicesettings/default/snmpservers	GET	servidorSNMP
/devicesettings/default/snmpservers/{objId}	PON, OBTÉN	servidorSNMP
/object/snmphosts	PUBLICAR, OBTENER	SNMPHost
/object/snmphosts/{objId}	PUT, DELETE, GET	SNMPHost
/object/snmpusergroups	PUBLICAR, OBTENER	SNMPUserGroup
/object/snmpusergroups/{objId}	PUT, DELETE, GET	SNMPUserGroup
/object/snmpusers	PUBLICAR, OBTENER	SNMPUser

/object/snmpusers/{objId}	PUT, DELETE, GET	SNMPUser
---------------------------	------------------	----------

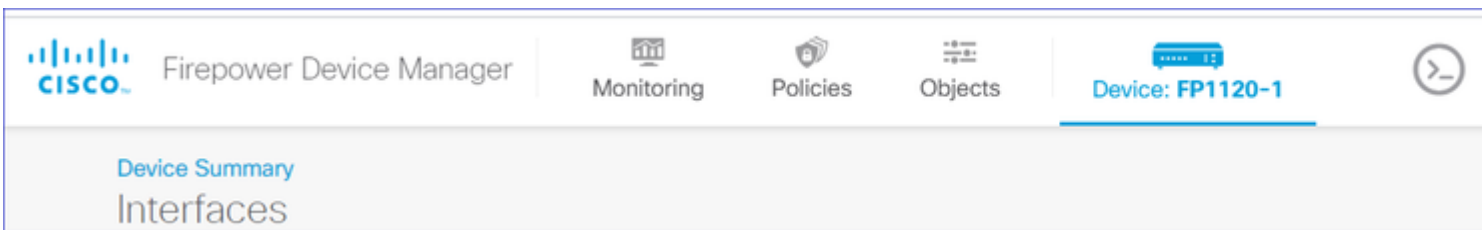
Configurar

- El host SNMP tiene 3 versiones principales
- SNMP V1
- SNMP V2C
- SNMP V3
 - Cada una de ellas tiene un formato específico para "securityConfiguration".
 - Para V1 y V2C: contiene una "cadena de comunidad" y un campo de "tipo" que identifica la configuración como V1 o V2C.
 - Para SNMP V3: contiene un usuario SNMP V3 válido y un campo de "tipo" que identifica la configuración como V3.

SNMP v3

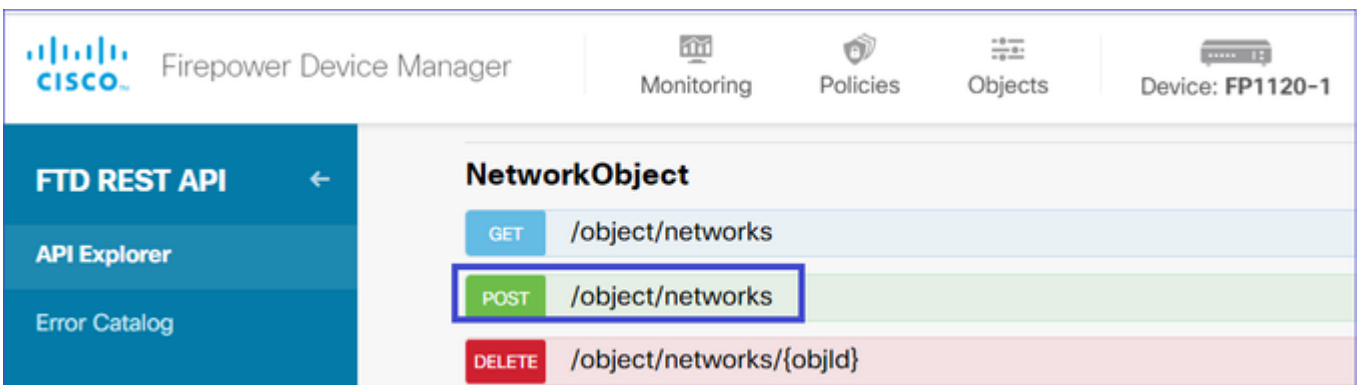
1. Acceder al Explorador de API de FDM

Para acceder al Explorador de API REST de FDM desde la GUI de FDM, seleccione los 3 puntos y, a continuación, **Explorador de API**. También puede navegar hasta la URL https://FDM_IP/#/api-explorer:



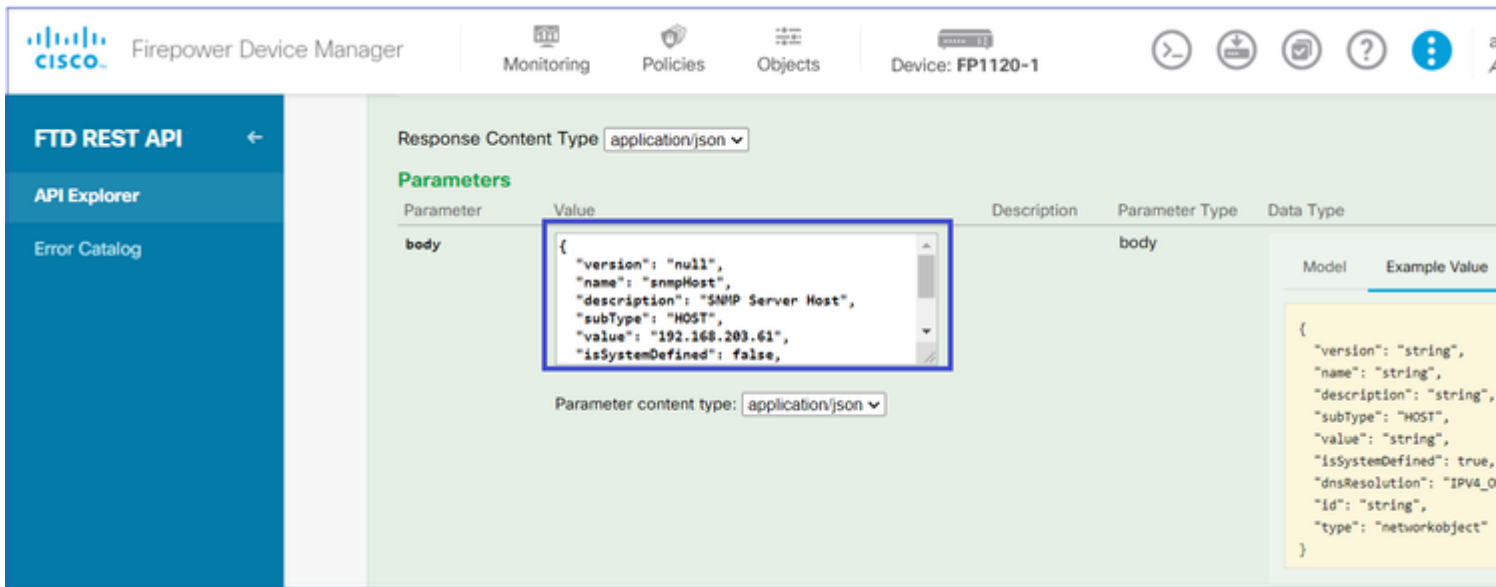
2. Configuración de objetos de red

Cree un nuevo objeto de red para el host SNMP: en el Explorador de API de FDM, seleccione NetworkObject y, a continuación, POST /object/networks:



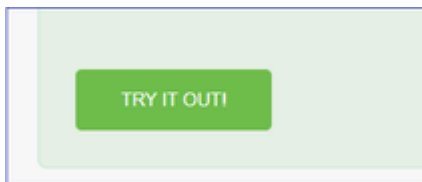
El formato SNMP Host JSON es este. Pegue este JSON en la sección body y cambie la dirección IP en "value" para que coincida con la dirección IP del host SNMP:

```
{
"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 REST API call. The 'Response Content Type' is set to 'application/json'. The 'Parameters' table has columns for 'Parameter', 'Value', 'Description', 'Parameter Type', and 'Data Type'. A parameter named 'body' is shown with a JSON value in the 'Value' column, which is highlighted with a blue box. The 'Parameter content type' is set to 'application/json'. The 'Example Value' column shows a JSON object with fields: 'version', 'name', 'description', 'subType', 'value', 'isSystemDefined', 'dnsResolution', 'id', and 'type'.

Desplácese hacia abajo y seleccione el botón TRY IT OUT! para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200.

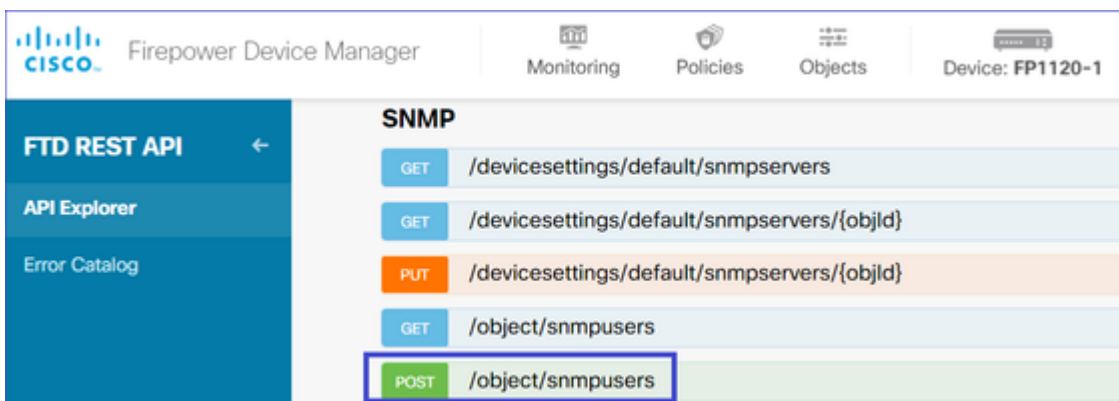


Copie los datos JSON del cuerpo de la respuesta en un bloc de notas. Más adelante, deberá completar la información sobre el host SNMP.



3. Crear un nuevo usuario SNMPv3

En el Explorador de API de FDM, seleccione SNMP y, a continuación, **usuarios POST/object/snmpus**



Copie estos datos JSON en un bloc de notas y modifique las secciones que le interesen (por ejemplo, "authenticationPassword", "encryptionPassword" o los algoritmos):

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

Precaución: las contraseñas utilizadas en los ejemplos se utilizan sólo con fines de demostración. En

un entorno de producción, asegúrese de utilizar contraseñas seguras

Copie los datos JSON modificados en la sección body:

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

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

 Below the table, the 'Parameter content type' is set to 'application/json'. On the right, the 'Model' section shows an 'Example Value' field with a JSON schema:

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

Desplácese hacia abajo y seleccione el botón **TRY IT OUT!** para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200. Copie los datos JSON del cuerpo de la respuesta en un bloc de notas. Más adelante, deberá completar la información sobre el usuario SNMP.

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. Obtener información de la interfaz

En el Explorador de API de FDM, seleccione Interfaz y, a continuación, GET `/devices/default/interfaces`. Necesita recopilar información de la interfaz que se conecta al servidor SNMP.

FTD REST API ← GET `/devices/default/interfaces`

Desplácese hacia abajo y seleccione el botón **TRY IT OUT!** para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200. Copie los datos JSON del cuerpo de la respuesta en un bloc de notas. Más adelante, tendrá que rellenar la información sobre la interfaz.

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.

Anote la "versión", "nombre", "id" y "tipo" de la interfaz en los datos JSON. Ejemplo de datos JSON de la interfaz interior:

```

<#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"
}
},

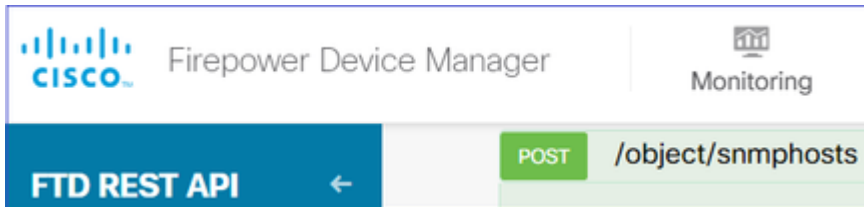
```

Desde los datos JSON, puede ver que la interfaz 'inside' tiene estos datos que deben asociarse con el servidor SNMP:

- "version": "kkpkibjlu6qro"
- "name": "inside",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "tipo": "interfaz física",

5. Crear un nuevo host SNMPv3

En el Explorador de API de FDM, seleccione SNMP y, a continuación, POST **/object/snmphosts/** en SNMP



Utilice este JSON como plantilla. Copie y pegue los datos de los pasos anteriores en la plantilla según corresponda:

```
{
"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"
}
```

Nota:

- Reemplace el valor de managerAddress id, type, version, and name con la información que recibió del Paso 1
- Reemplace el valor de autenticación con la información que recibió del Paso 2
- Reemplace el valor de la interfaz por los datos recibidos del paso 3
- Para SNMP2, no hay autenticación y el tipo es snmpv2csecurityconfiguration en lugar de snmpv3securityconfiguration

Copie los datos JSON modificados en la sección del cuerpo

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

Desplácese hacia abajo y seleccione el botón **TRY IT OUT!** para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200.

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

Vaya a la GUI de FDM e implemente los cambios. Puede ver la mayor parte de la configuración SNMP:

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>snmpInterface:</td><td></td></tr> <tr><td>-</td><td>inside</td></tr> <tr><td>managerAddress:</td><td></td></tr> <tr><td>-</td><td>snmpHost</td></tr> <tr><td>securityConfiguration.authentication:</td><td></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

Para v2c no es necesario crear un usuario, pero sigue siendo necesario:

1. Crear una configuración de objeto de red (igual que se describe en la sección SNMPv3)
2. Obtener información de la interfaz (la misma que se describe en la sección SNMPv3)
3. Crear un nuevo objeto de host SNMPv2c

Este es un ejemplo de una carga JSON que crea un objeto SNMPv2c:

```
{
  "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",

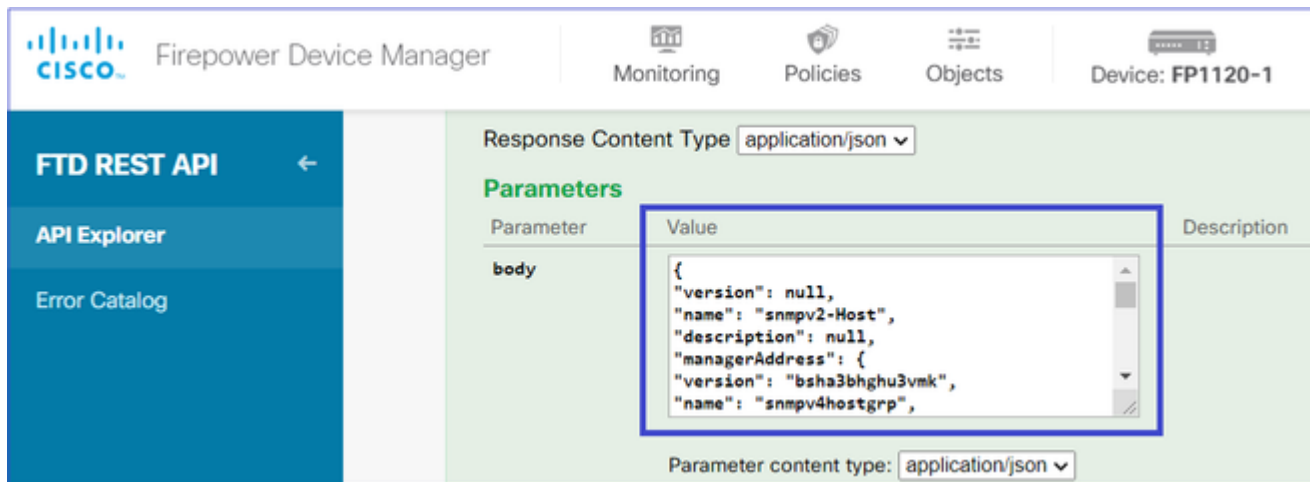
```

```

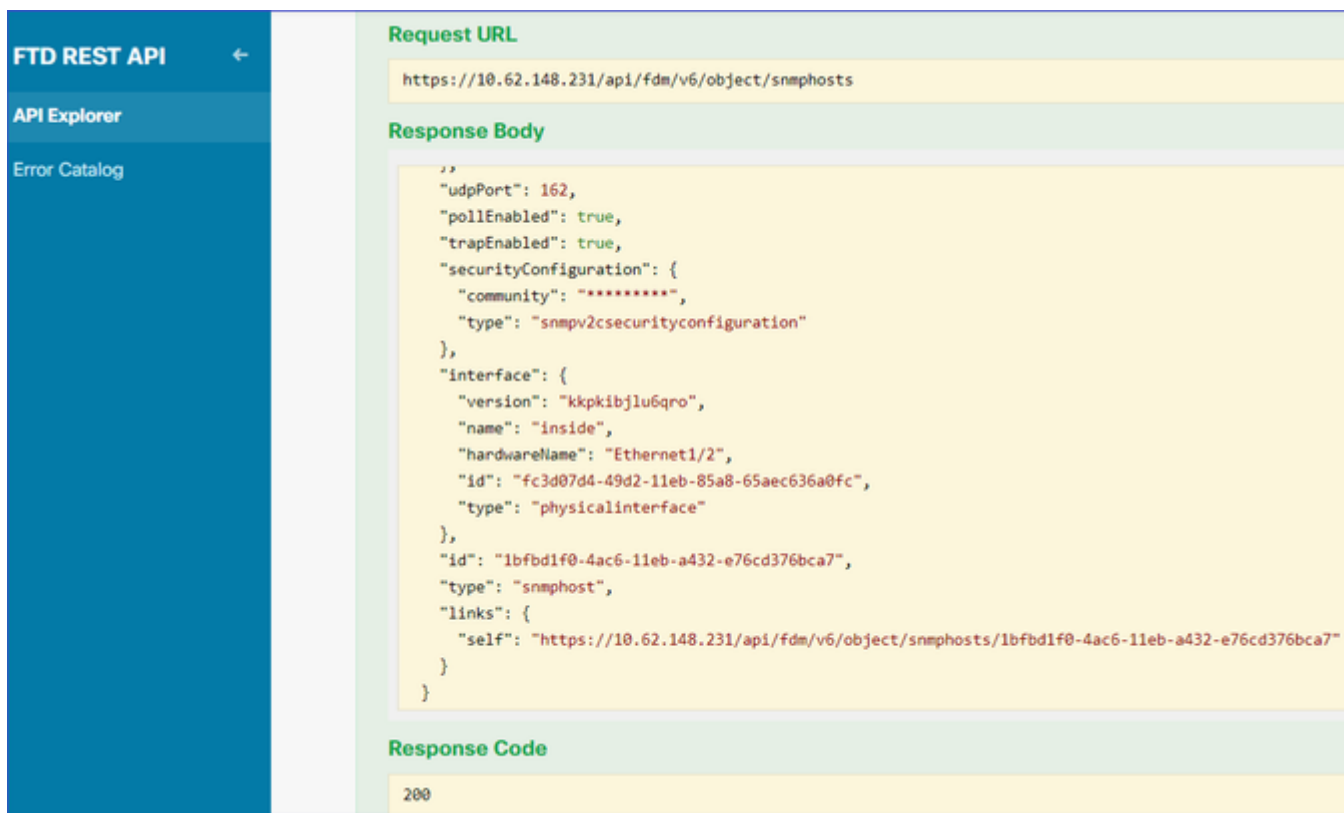
"id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
"type": "physicalinterface"
},
"id": null,
"type": "snmpghost"
}

```

Utilice el método POST para implementar la carga útil JSON:



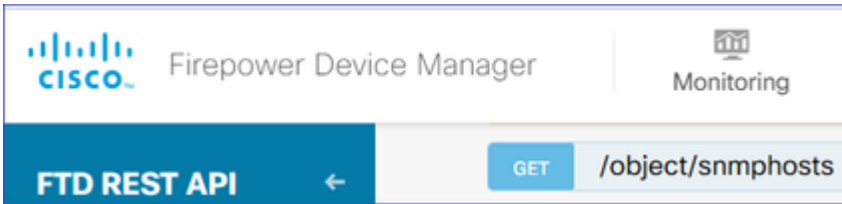
Desplácese hacia abajo y seleccione el botón TRY IT OUT! para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200.



Eliminación de configuración SNMP

Paso 1.

Obtenga la información del host SNMP (SNMP > /object/snmphosts):



Desplácese hacia abajo y seleccione el botón TRY IT OUT! para ejecutar la llamada API. Una llamada correcta devuelve el código de respuesta 200.

Se obtiene una lista de objetos. Anote el ID del objeto snmphost que desea eliminar:

```
<#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": "
1bfb1f0-4ac6-11eb-a432-e76cd376bca7
",
      "type": "snmphost",
      "links": {
        "self": "https://10.62.148.231/api/fdm/v6/object/snmphosts/1bfb1f0-4ac6-11eb-a432-e76cd376bca7"
      }
    },
  ],
}
```

Paso 2.

Elija la opción DELETE en **SNMP > /object/snmphosts{objId}**. Pegue la ID que recopiló en el paso 1:

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

Desplácese hacia abajo y seleccione el botón TRY IT OUT! para ejecutar la llamada API. La llamada devuelve el código de respuesta 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"
}
```

Paso 3.

Implemente el cambio:

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

OK

La implementación quita la información del host:

```
<#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 para v2c falla:

```
<#root>
```

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

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

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

Para la versión 3, debe eliminar los objetos en este orden.

1. Host SNMP (el código de retorno correcto es 204)
2. Usuario SNMP (el código de retorno correcto es 204)

Si intenta eliminar los objetos en el orden incorrecto, aparece este error:

```
<#root>
```

```
{
"error": {
"severity": "ERROR",
"key": "Validation",
"messages": [
{
"description": "You cannot delete the object because it contains SNMPHost: snmpv3-host2, SNMPHost: snmpv3-host1",
"code": "deleteObjWithRel",
"location": ""
}
]
}
}
```

Verificación

Verificación de SNMP v3

Después de la implementación, navegue hasta FTD CLI para verificar la configuración de SNMP. Tenga en cuenta que el valor engineID se genera automáticamente.

```
<#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
```

prueba snmpwalk

```
<#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
...
```

Verificación de SNMP v2c

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

snmpwalk para 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
```

Troubleshoot

Habilite la captura con seguimiento en el firewall:

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

Utilice la herramienta snmpwalk y verifique que pueda ver los paquetes:

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

El contenido de la captura:

```
<#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
```

Verifique que los contadores de estadísticas del servidor SNMP muestren las solicitudes y respuestas Get o Get-next de SNMP:

<#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

Rastrea un paquete de ingreso. El paquete es UN-NAT a la interfaz NLP interna:

<#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

La regla NAT se implementa automáticamente como parte de la configuración SNMP:

<#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
```

En el puerto backend, UDP 4161 escucha el tráfico SNMP:

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

En un caso de configuración incorrecta o incompleta, el paquete SNMP de ingreso se descarta porque no hay una fase UN-NAT:

```
<#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

Los syslogs de FTD LINA muestran que el paquete de ingreso es descartado:

<#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

Información Relacionada

- [Guía de configuración de Cisco Firepower Threat Defense para Firepower Device Manager, versión 6.7](#)
- [Guía API REST de Cisco Firepower Threat Defence](#)
- [Notas de la versión de Cisco Firepower, versión 6.7.0](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).