

# Configurazione e risoluzione dei problemi di SNMP su Firepower FDM

## Sommario

---

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Configurazione](#)

[SNMP v3](#)

[SNMP v2c](#)

[Rimozione della configurazione SNMP](#)

[Verifica](#)

[Verifica SNMP v3](#)

[Verifica SNMP v2c](#)

[Risoluzione dei problemi](#)

[Informazioni correlate](#)

---

## Introduzione

In questo documento viene descritto come abilitare Simple Network Management Protocol (SNMP) su Firepower Device Management nella versione 6.7 con l'API REST.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Firepower Threat Defense (FTD) gestito da Firepower Device Management (FDM) sulla versione 6.7
- Conoscenza dell'API REST
- Conoscenza del protocollo SNMP

### Componenti usati

Firepower Threat Defense (FTD) gestito da Firepower Device Management (FDM) sulla versione 6.7.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico

ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Premesse


### Novità della versione 6.7

L'API REST del dispositivo FTD supporta la configurazione e la gestione di server SNMP, utenti, host e gruppi host. Con il supporto dell'API REST per il dispositivo FTD SNMP in FP 6.7:

- Un utente può configurare SNMP tramite l'API REST del dispositivo FTD per gestire la rete
- Server SNMP, utenti e gruppi host/host possono essere aggiunti/aggiornati o gestiti tramite l'API REST del dispositivo FTD.

Gli esempi inclusi nel documento descrivono i passaggi di configurazione eseguiti da FDM API Explorer.

---

 Nota: SNMP può essere configurato solo tramite l'API REST quando FTD esegue la versione 6.7 e gestito da FDM

---

### Panoramica delle funzionalità - Supporto API REST per dispositivo FTD SNMP

- Questa funzionalità aggiunge nuovi endpoint URL FDM specifici per SNMP.
- Queste nuove API possono essere utilizzate per configurare il protocollo SNMP per polling e trap per il monitoraggio dei sistemi.
- La configurazione post SNMP tramite API, i Management Information Base (MIB) sui dispositivi Firepower, sono disponibili per il polling o per la notifica trap su client NMS/SNMP.

### Endpoint SNMP API/URL

URL	Metodi	Modelli
/devicesettings/default/snmpservers	OTTIENI	Server SNMP
/devicesettings/default/snmpservers/{idbDispositivi}	PUT, GET	Server SNMP
/object/snmphosts	POST, LEGGI	SNMPPost
/object/snmphosts/{idobj}	PUT, DELETE, GET	SNMPPost

/object/snmpusergroups	POST, LEGGI	GruppoUtentiSNMP
/object/snmpusergroups/{idb}	PUT, DELETE, GET	GruppoUtentiSNMP
/object/snmpusers	POST, LEGGI	SNMPUser
/object/snmpusers/{idobj}	PUT, DELETE, GET	SNMPUser

## Configurazione

- L'host SNMP ha tre versioni principali

- SNMP V1

- SNMP V2C

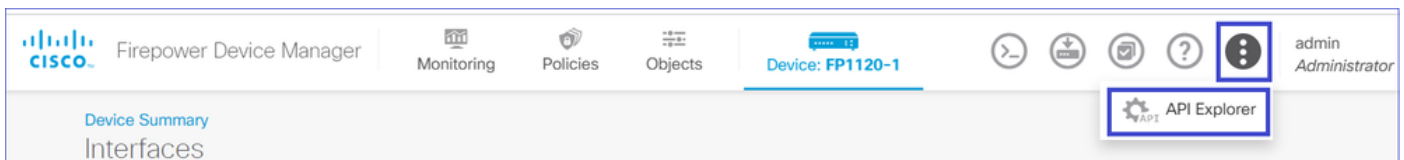
- SNMP V3

- Ognuno di questi elementi ha un formato specifico per "securityConfiguration".
- Per V1 e V2C: contiene una "stringa della community" e un campo "tipo" che identifica la configurazione come V1 o V2C.
- Per SNMP V3: contiene un utente SNMP V3 valido e un campo "tipo" che identifica la configurazione come V3.

## SNMP v3

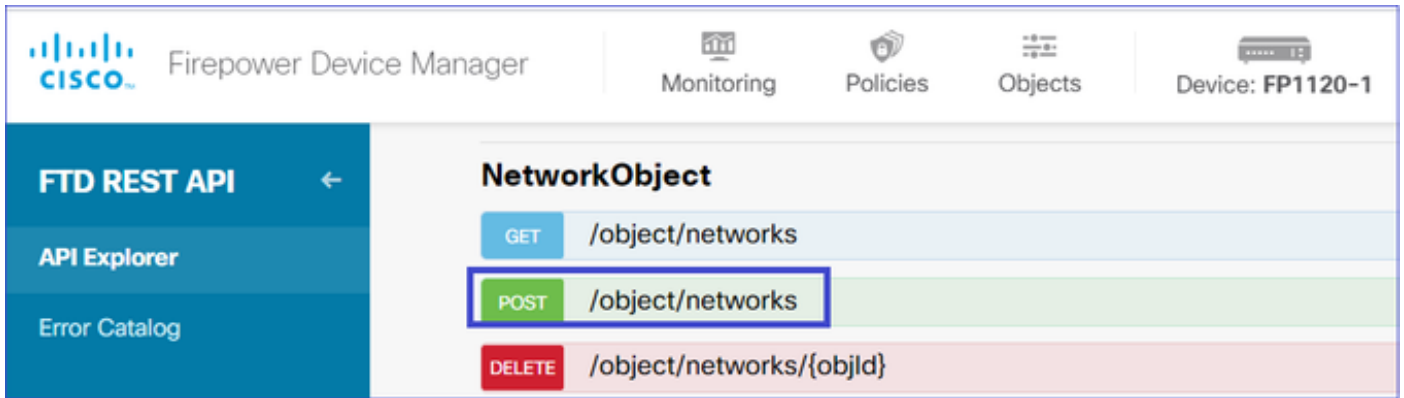
1. Accedere a FDM API Explorer

Per accedere a FDM REST API Explorer dalla GUI di FDM, selezionare i 3 punti e quindi API Explorer. In alternativa, selezionare l'URL [https://FDM\\_IP/#/api-explorer](https://FDM_IP/#/api-explorer):



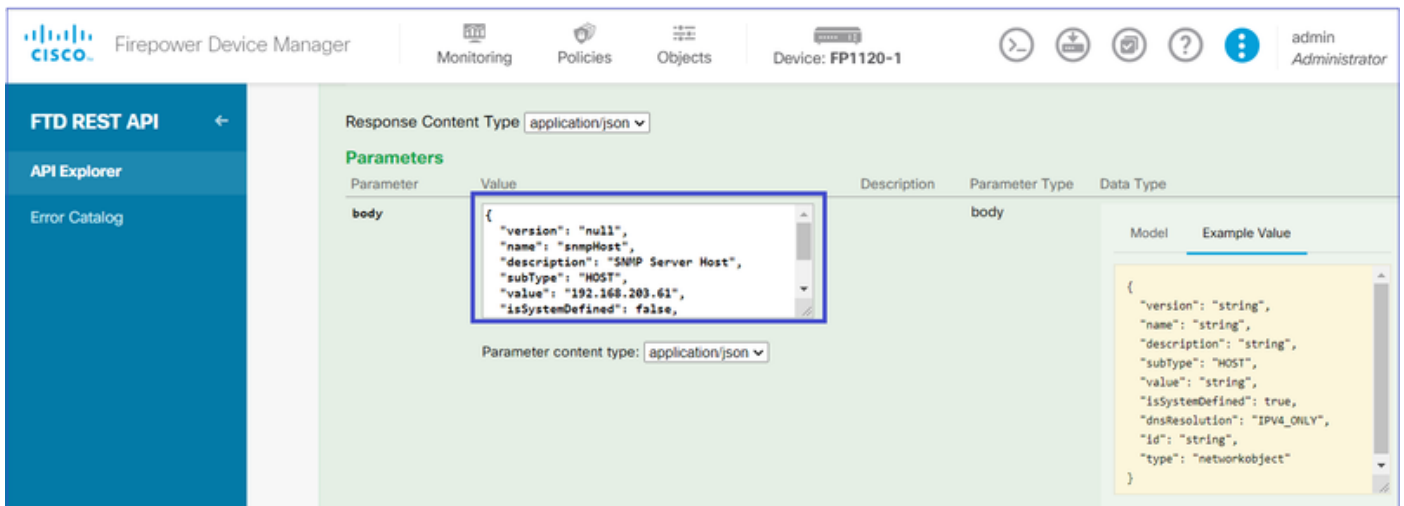
2. Configurazione oggetto di rete

Creare un nuovo oggetto di rete per l'host SNMP: in Esplora API di FDM selezionare NetworkObject, quindi POST/object/networks:



Il formato JSON dell'host SNMP è il seguente. Incollare il file JSON nella sezione body e modificare l'indirizzo IP in "value" in modo che corrisponda all'indirizzo IP dell'host SNMP:

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



Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 200.

TRY IT OUT!

Copiare i dati JSON dal corpo della risposta in un blocco note. In seguito, sarà necessario compilare le informazioni sull'host SNMP.

The screenshot displays the FTD REST API Explorer interface. On the left, a sidebar contains the text "FTD REST API", "API Explorer", and "Error Catalog". The main area shows the URL `https://10.62.148.231/api/fdm/v6/object/networks`. Below the URL, the "Response Body" section contains 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" section shows the value `200`.

### 3. Creare un nuovo utente SNMPv3

In FDM API Explorer selezionare SNMP, quindi POST/object/snmpusers

The screenshot shows the Cisco Firepower Device Manager interface for device FP1120-1. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area displays a list of REST API endpoints for SNMP configuration:

- GET /devicesettings/default/snmpservers
- GET /devicesettings/default/snmpservers/{objId}
- PUT /devicesettings/default/snmpservers/{objId}
- GET /object/snmpusers
- POST /object/snmpusers** (highlighted)

Copiare i dati JSON in un blocco note e modificare le sezioni desiderate (ad esempio, "authenticationPassword", "encryptionPassword" o gli algoritmi):

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

**⚠️ Attenzione:** le password utilizzate negli esempi sono solo a scopo dimostrativo. In un ambiente di produzione, assicurarsi di utilizzare password complesse

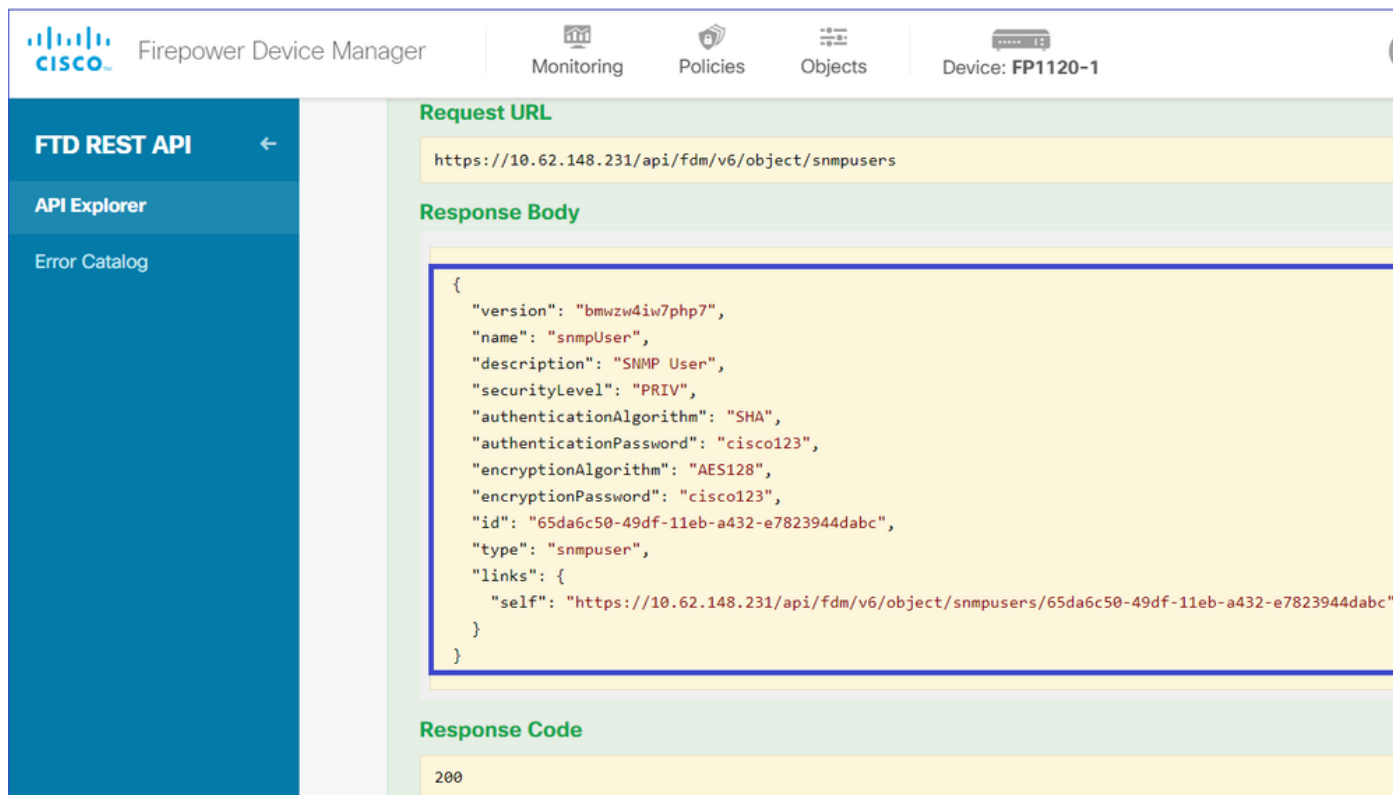
Copiare i dati JSON modificati nella sezione body:

The screenshot shows the REST API interface for the 'POST /object/snmpusers' endpoint. The 'Parameters' section is expanded to show the 'body' parameter. The JSON data is highlighted with a blue box:

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

The interface also shows a 'Model' section with an 'Example Value' field containing a JSON schema definition for the snmpuser object.

Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 200. Copiare i dati JSON dal corpo della risposta in un blocco note. In seguito, sarà necessario compilare le informazioni sull'utente SNMP.



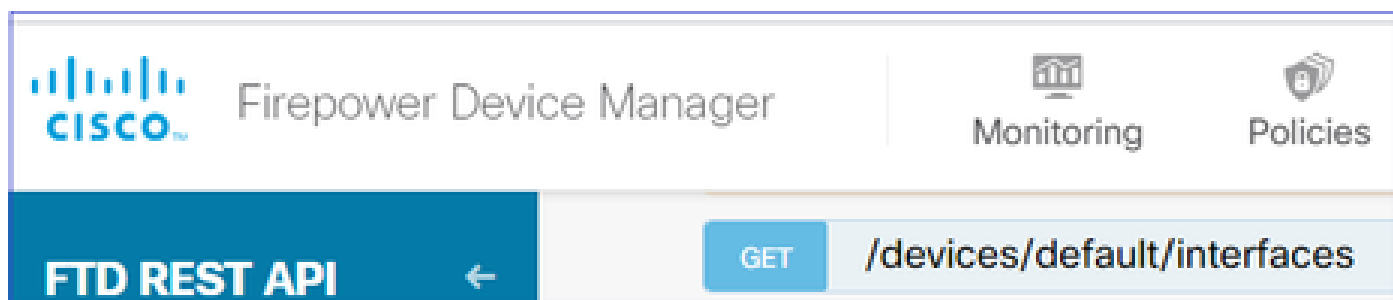
The screenshot shows the Firepower Device Manager interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring", "Policies", "Objects", and "Device: FP1120-1". On the left, a sidebar contains "FTD REST API" (selected), "API Explorer", and "Error Catalog". The main content area displays the results of an API call:

- 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. Ottieni informazioni sull'interfaccia

In FDM API Explorer selezionare Interface, quindi GET /devices/default/interfaces. È necessario raccogliere informazioni dall'interfaccia che si connette al server SNMP.



The screenshot shows the Firepower Device Manager interface. The top navigation bar includes the Cisco logo, the text "Firepower Device Manager", and icons for "Monitoring" and "Policies". On the left, a sidebar contains "FTD REST API" (selected). The main content area displays the API endpoint:

- Method:** GET
- Endpoint:** /devices/default/interfaces

Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 200. Copiare i dati JSON dal corpo della risposta in un blocco note. In seguito, sarà necessario specificare le informazioni sull'interfaccia.

**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

Annotare l'interfaccia "version", "name", "id" e "type" dai dati JSON. Esempio di dati JSON dall'interfaccia interna:

<#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"
}
},

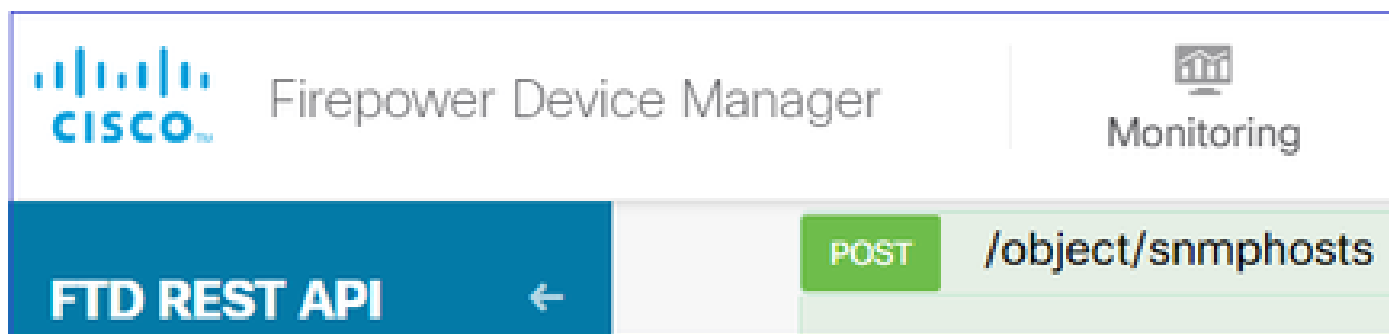
```

Dai dati JSON, si può vedere che l'interfaccia 'inside' ha questi dati che devono essere associati al server SNMP:

- "version": "kkpkibjlu6qro"
- "name": "inside",
- "id": "fc3d07d4-49d2-11eb-85a8-65aec636a0fc",
- "type": "physical interface",

## 5. Creare un nuovo host SNMPv3

In FDM API Explorer selezionare SNMP, quindi POST/object/snmphosts/ in SNMP



Utilizzare questo file JSON come modello. Copiare e incollare i dati dai passaggi precedenti nel modello di conseguenza:

```
{
  "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:

- Sostituire il valore in managerAddress id, type, version e name con le informazioni ricevute al punto 1
- Sostituire il valore nell'autenticazione con le informazioni ricevute dal passaggio 2

- Sostituire il valore nell'interfaccia con i dati ricevuti dal passaggio 3
- Per SNMP2 non è disponibile alcuna autenticazione e il tipo è snmpv2csecurityconfiguration anziché snmpv3securityconfiguration

Copiare i dati JSON modificati nella sezione body

The screenshot shows the Cisco Firepower Device Manager interface for device FP1120-1. The left sidebar contains 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area shows the 'Parameters' section for an API endpoint. The 'Response Content Type' is set to 'application/json'. A table lists parameters, with 'body' highlighted. The value for 'body' is a JSON object: { "version": null, "name": "snmpv3-host", "description": null, "managerAddress": { "version": "bsha3bhghu3vmk", "name": "snmpHost" } }. Below the table, the 'Parameter content type' is also set to 'application/json'.

Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 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

Passare alla GUI di FDM e distribuire le modifiche. È possibile visualizzare la maggior parte della configurazione 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
<span style="color: blue; font-weight: bold;">+</span> Network Object Added: <i>snmpHost</i>	
-	subType: Host
-	value: 192.168.203.61
-	isSystemDefined: false
-	dnsResolution: IPV4_ONLY
-	description: SNMP Server Host
-	name: snmpHost
<span style="color: blue; font-weight: bold;">+</span> snmpHost Added: <i>snmpv3-host</i>	
-	udpPort: 162
-	pollEnabled: true
-	trapEnabled: true
-	name: snmpv3-host
snmpInterface:	inside
managerAddress:	snmpHost
securityConfiguration.authentication:	snmpUser

MORE ACTIONS ▾
CANCEL
DEPLOY NOW ▾

## SNMP v2c

Per v2c non è necessario creare un utente, ma è comunque necessario:

1. Creare una configurazione oggetto di rete (come descritto nella sezione SNMPv3)
2. Ottenere le informazioni sull'interfaccia (come descritto nella sezione SNMPv3)
3. Creare un nuovo oggetto host SNMPv2c

Di seguito è riportato un esempio di payload JSON che crea un oggetto 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"
}

```

Utilizzare il metodo POST per distribuire il payload JSON:

The screenshot shows the Cisco Firepower Device Manager interface. On the left, there is a sidebar with 'FTD REST API', 'API Explorer', and 'Error Catalog'. The main area is titled 'FTD REST API' and shows a 'Parameters' table. The 'body' parameter is highlighted with a blue box and contains the following JSON payload:

```

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

```

Below the table, the 'Parameter content type' is set to 'application/json'.

Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 200.

The screenshot shows the results of the API call. 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": "1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7",
"type": "snmpghost",
"links": {
"self": "https://10.62.148.231/api/fdm/v6/object/snmpghosts/1bfbdf1f0-4ac6-11eb-a432-e76cd376bca7"
}
}

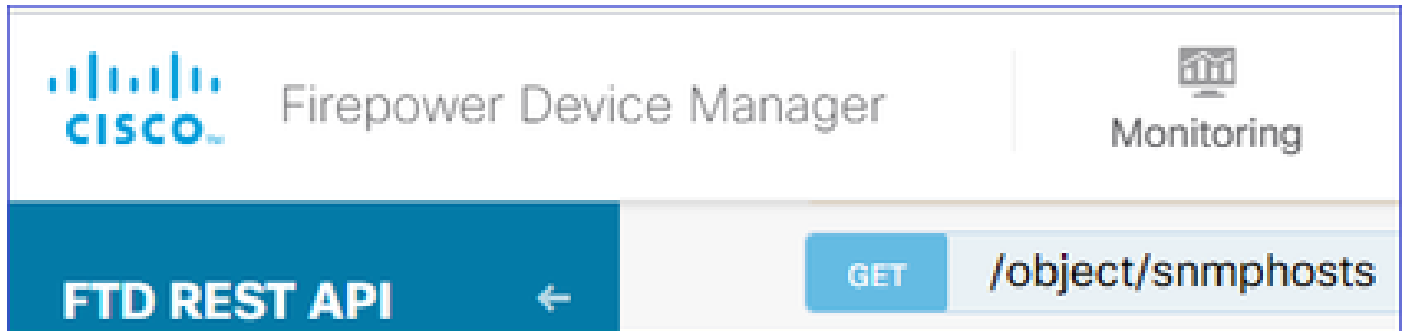
```

The 'Response Code' is 200.

## Rimozione della configurazione SNMP

Passaggio 1.

Ottenere le informazioni sull'host SNMP (SNMP > /object/snmphosts):



Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. Una chiamata riuscita restituisce il codice di risposta 200.

Ottenete un elenco di oggetti. Prendere nota dell'ID dell'oggetto snmphost che si desidera rimuovere:

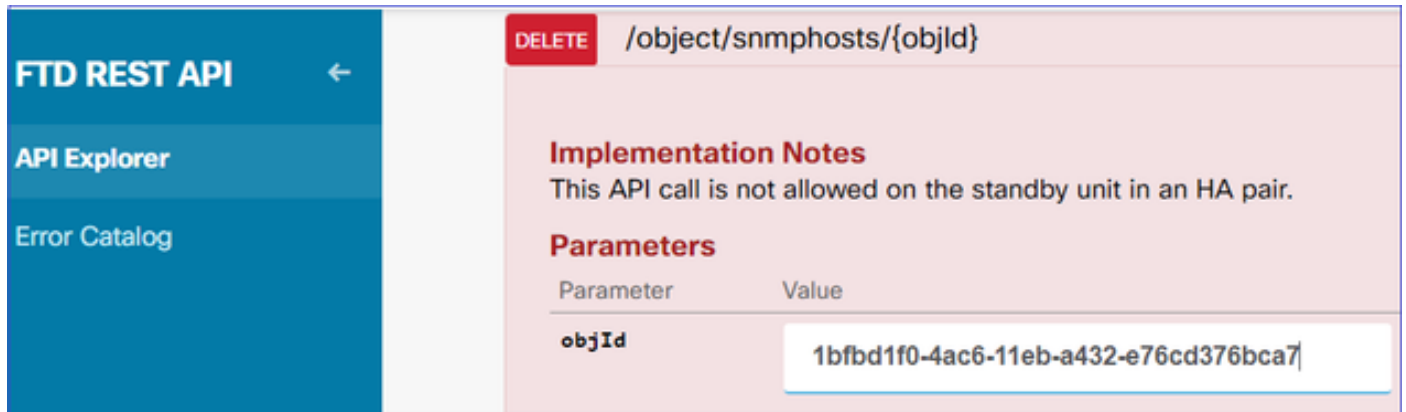
<#root>

```
{
  "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/1bfd1f0-4ac6-11eb-a432-e76cd376bca7"  
}  
},
```

Passaggio 2.

Scegliere l'opzione DELETE in SNMP > /object/snmphosts{objId}. Incollare l'ID raccolto nel passaggio 1:



The screenshot shows the FTD REST API interface. On the left, there is a navigation menu with 'API Explorer' and 'Error Catalog'. The main area displays the endpoint `/object/snmphosts/{objId}` with a red 'DELETE' button. Below the endpoint, there are sections for 'Implementation Notes' (stating the call is not allowed on the standby unit in an HA pair) and 'Parameters'. A table lists the parameter `objId` with its value `1bfd1f0-4ac6-11eb-a432-e76cd376bca7` entered in a text box.

Scorrere verso il basso e selezionare il pulsante TRY IT OUT! per eseguire la chiamata API. La chiamata restituisce il codice di risposta 400.



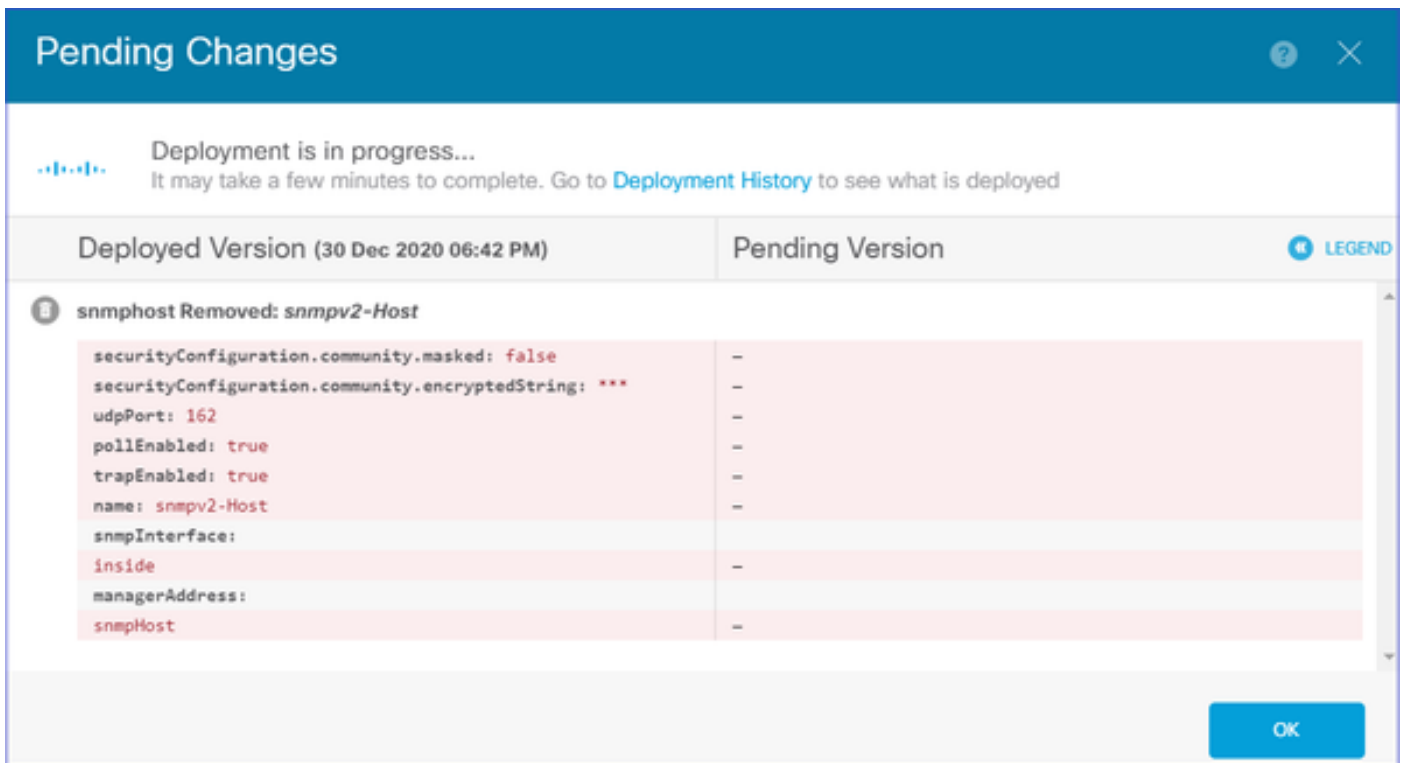
The screenshot shows the API response details. The 'Response Code' is 400. The 'Response Headers' are displayed as a JSON object:

```
{  
  "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"  
}
```

Passaggio 3.

Distribuire la modifica:





La distribuzione rimuove le informazioni sull'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 per v2c non riesce:

```
<#root>
```

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

```
snmpwalk -v2c -c cisco123 -Os 192.168.203.71
```

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

Per v3 è necessario eliminare gli oggetti nell'ordine indicato.

1. Host SNMP (il codice restituito è 204)

## 2. Utente SNMP (il codice restituito è 204)

Se si tenta di eliminare gli oggetti nell'ordine errato, viene visualizzato questo errore:

```
<#root>
{
  "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": ""
      }
    ]
  }
}
```

## Verifica

### Verifica SNMP v3

Dopo la distribuzione, passare alla CLI FTD per verificare la configurazione SNMP. Il valore engineID viene generato automaticamente.

```
<#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-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
```

test 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 9.8(2)K8"
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
...
```

## Verifica 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 per 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.
```

```
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
```

## Risoluzione dei problemi

Abilita acquisizione con traccia nel firewall:

```
<#root>
```

```
FP1120-1#
```

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

Utilizzare lo strumento snmpwalk e verificare che sia possibile visualizzare i pacchetti:

```
<#root>
```

```
FP1120-1#
```

```
show capture
```

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

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

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

Il contenuto dell'acquisizione:

```
<#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
```

Verificare che i contatori delle statistiche del server SNMP visualizzino le richieste e le risposte Get o Get-next di 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

Tracciare un pacchetto in entrata. Il pacchetto è UN-NAT per l'interfaccia 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 regola NAT viene distribuita automaticamente come parte della configurazione 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 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

Nella porta back-end UDP 4161 resta in ascolto del traffico 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 :::*
```

In caso di configurazione errata/incompleta, il pacchetto SNMP in entrata viene scartato in quanto non è presente 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

I syslog di FTD LINA mostrano che il pacchetto in entrata viene scartato:

<#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.

## Informazioni correlate

- [Guida alla configurazione di Cisco Firepower Threat Defense per Firepower Device Manager, versione 6.7](#)
- [Guida API REST Cisco Firepower Threat Defense](#)
- [Note sulla release di Cisco Firepower, versione 6.7.0](#)

## Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).