

# Cisco cEdge هجوم ىل ع SNMPv3 خف نيوكت

## تايوت حمل

[عمدق مل](#)

[ةيساس الابلط مل](#)

[تابلط مل](#)

[عمدختس مل تانوك مل](#)

[نيوكت مل](#)

[تاننيوكت مل](#)

[حصلا نم ققحت مل](#)

[اهالص او اعاطخ ال افاشكتسا](#)

[قلص تاذا تامول عم](#)

## عمدق مل

ةكبشلا ةراد لوكوتورب نم 3 رادصل ا تارابتخ نيكم تل نيوكتلا دننتم مل اذه فصبي  
cEdge هجوم ىل ع vManage ةزيم بلق مادختسا ب (SNMP) طيسبلا

## ةيساس الابلط مل

### تابلط مل

ةيلاتل عيضاوملاب ةفرعم كيدل نوكت نأب Cisco ي صوت:

- ج Cisco SDWAN
- لوكوتورب ل يساس ال مهفلا

### عمدختس مل تانوك مل

ةيلاتل ةيداملا تانوك مل او جماربلا تارادصل ىل دننتم مل اذه يف ةدراولا تامول عم مل دننتم:

- 16.12.3 لغشي Cisco نم (CSR1000V) ةباحسلا تامدخ هجوم
- 19.2.2 هليغشت متي يذلا vManage رادصل

ةصاخ ةيلمعم ةئيبي يف ةدوجوملا ةزهجال نم دننتم مل اذه يف ةدراولا تامول عملا عاشن امت  
تناك اذا (يضا رتفا) حوسمم نيوكتب دننتم مل اذه يف عمدختس مل ةزهجال عيمج تادب  
رما يال لمحتحمل ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تبش

نوكت InManage يف. ةمئالملا تا عومجم ىل ماع لكشب فاولحلا جاتحت ال: **ةظالم**  
دوجوب ةيعبتلا دعيمل، ةلصفنم vEdge و cEdge بلوق نم ثدجال و 20.x تارادصل ال  
ةدوجوم ةمئالملا عومجم.

## نيوكت مل

## تاني وكتال

vManage جمانرب ي ف:

SNMP > ةزيم بلق > بلاوق > ني وكتال ل لقتنا ، SNMP ةزيم بلق عاشنإل 1. ةوطخل

هذه ي ف حضورم وه امك ، SNMP لي غشت فاق ي مدع عم ناعبتمل فصولاو بلق ل مسا لخدأ ةروصل.

The screenshot shows the Cisco vManage interface for configuring a feature template. The breadcrumb is "Feature Template > SNMP". The template name and description are both "CSR1000v-SNMP". Under the "SNMP Version" section, there is a "Shutdown" label and a radio button selection for "Yes" and "No", with "No" selected.

3. رادصلال - ةلاجل هذه ي ف . SNMP رادصلال دح 2. ةوطخل

The screenshot shows the "SNMP VERSION" configuration page. The "SNMP Version" label is followed by two radio buttons: "v2" and "v3". The "v3" radio button is selected.

هذه ي ف حضورم وه امك ، ةمئالملا تادحو ةئبعو و SNMP ةمئالم ةومجم عاشنإل 3. ةوطخل ةروصل.

TRAP GROUP TRAP TARGET SERVER

New Trap Group

Trap Group Name

SNMP-TRAP-GRP\_VMANAGE

Update Trap Group

Group Name

Trap Type Modules [1 Trap Type Modules](#)

[Save Changes](#) [Cancel](#)

VIEW & GROUP

Trap Type Modules

Module Name	Severity Levels
<input type="text" value="all"/>	<input type="text" value="critical x major x minor x"/> <span style="float: right; color: red;">-</span>

[+ Add Trap Module](#)

[Save Changes](#) [Cancel](#)

SNMP عمالمة فده مءاخ عاشنإ. 4 ؤوطءال

SNMP ءارابءء رءصمل (VRF) یره اءلال هے ؤوءءال ؤءاع مءءءءس مءء انه

```
interface GigabitEthernet1 vrf forwarding Mgmt-intf ip dhcp client default-router distance 1 ip
address dhcp negotiation auto arp timeout 1200 no mop enabled no mop sysid end
```

Update Trap Target

VPN ID   Mark as Optional Row i

IP Address

UDP Port

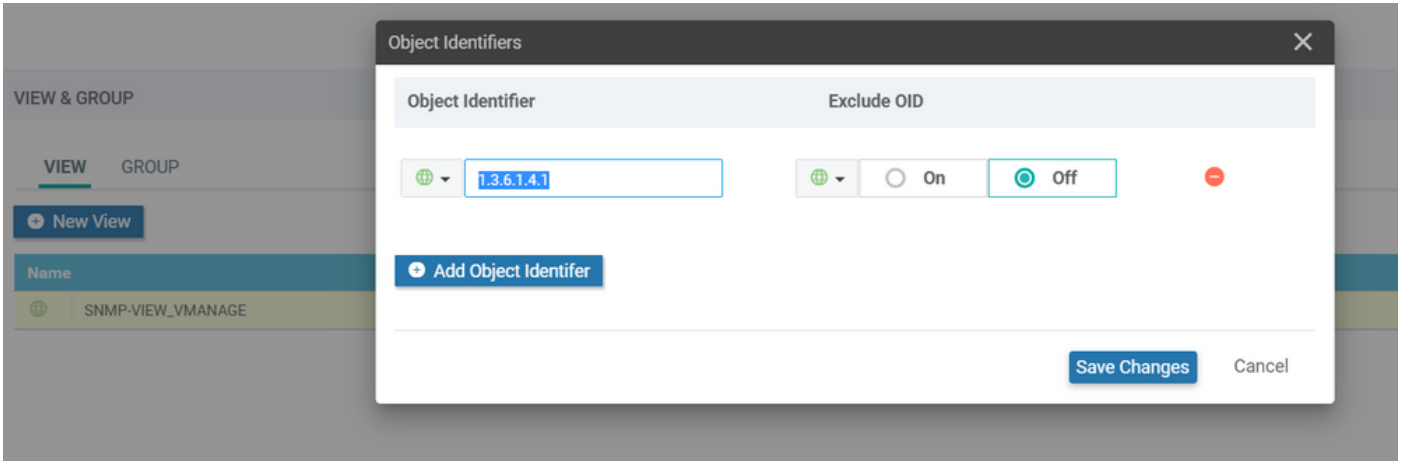
Trap Group Name

User Name

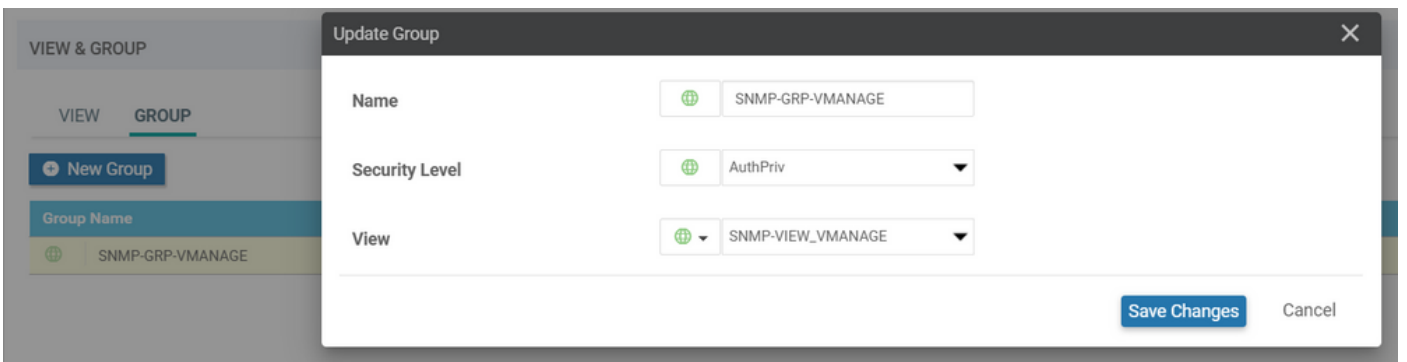
Source Interface

[Save Changes](#) [Cancel](#)

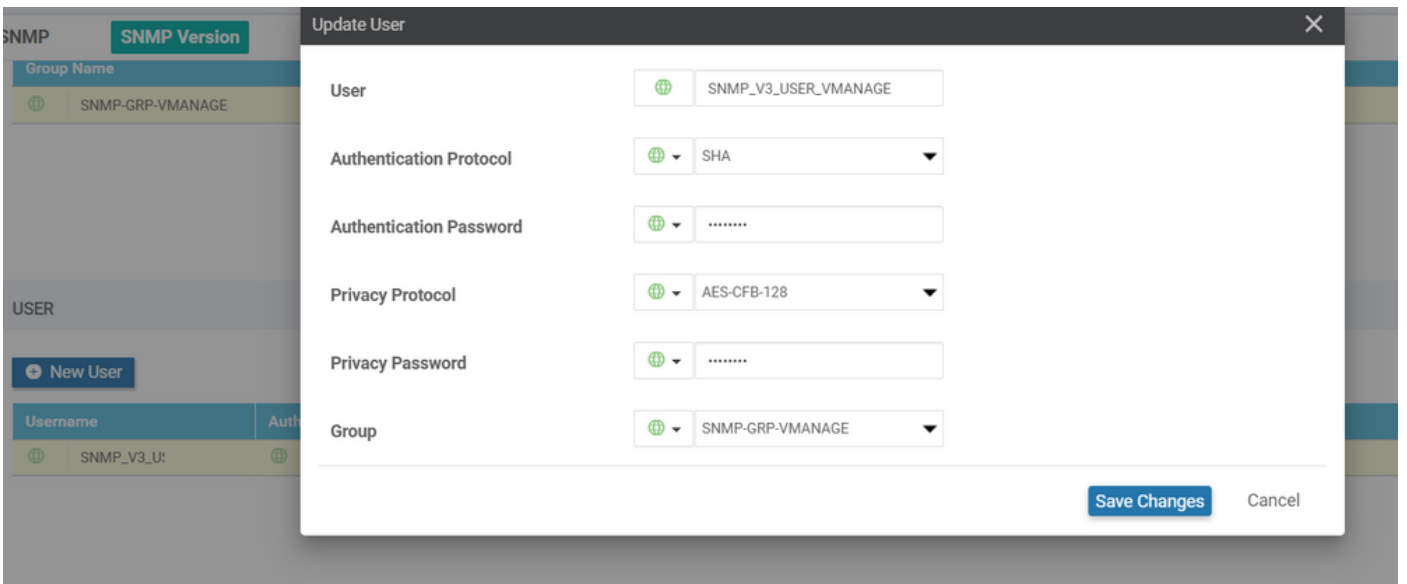
SNMP (OID) نئاك فرع ة فاضا و SNMP ضرع عاشن ا 5. ة و ط خ ل ا



اهب اق بس م اه و اشن ا م ت ي ت ل ا SNMP ضرع ة ق ي ر ط ق ف ر ا و SNMP ة و م ج م عاشن ا ب م ق 6. ة و ط خ ل ا



ة و ر و ص ل ا ه ذ ه ي ف ح ز و م و ه ا م ك ، SNMPv3 م د خ ت س م ة ف ا ض ا ا 7. ة و ط خ ل ا



ز ا ه ج ل ا ب ل ا ق ل ي ف ا ض ا ل ا ب ل ا ق ل ا م س ق ي ف SNMP ة ز ي م ب ل ا ق ق ا ف ر ا ب م ق 8. ة و ط خ ل ا



### Additional Templates

AppQoE	Choose...
Banner	Choose...
Global Template	Choose...
Policy	Choose...
Probes	Choose...
SNMP	CSR1000v-SNMP
Security Policy	test-1-sec



يُنعم ل زاهج ل اب زاهج ل بل اق ق اف ر اب مق 9. ة و ط خ ل ا

## ة ح ص ل ل ن م ق ق ح ت ل ل ا

ع ل ع Edge:

ي ل ل ا ل ا ع ا ط خ ا ل ا ح ي ح ص ت ن ي ك م ت

```
debug snmp packets debug snmp detail
```

snmp trap ر ا ب ت خ | ن ي و ك ت : SNMP ة م ئ ا ل م ا ش ن |

```
cEdge#test snmp trap config Generating CONFIG-MAN-MIB Trap cEdge# Aug 19 14:26:03.124: SNMP:
Queuing packet to 10.48.35.219 Aug 19 14:26:03.124: SNMP: V2 Trap, reqid 5563, errstat 0, erridx
0 sysUpTime.0 = 233535801 snmpTrapOID.0 = ciscoConfigManEvent ccmHistoryEventCommandSource.2 = 1
ccmHistoryEventConfigSource.2 = 2 ccmHistoryEventConfigDestination.2 = 2
ccmHistoryEventTerminalUser.2 = test Aug 19 14:26:03.374: SNMP: Packet sent via UDP to
10.48.35.219
```

10.48.35.219 م دا خ ل ا ل ا ل ا ه ل ا س ر ا م ت ي SNMP ة م ئ ا ل م ن ا ط ح ا ل ي ، ا ن ه

ة م ز ح ل ا ط ا ق ت ل ل ا

```

<
> Frame 2: 306 bytes on wire (2448 bits), 306 bytes captured (2448 bits)
> Ethernet II, Src: VMware_8d:61:ce (00:50:56:8d:61:ce), Dst: Cisco_5b:a6:1d (cc:7f:76:5b:a6:1d)
> Internet Protocol Version 4, Src: 10.48.62.184, Dst: 10.48.35.219
> User Datagram Protocol, Src Port: 49444, Dst Port: 161
> Simple Network Management Protocol
  msgVersion: snmpv3 (3)
  > msgGlobalData
  > msgAuthoritativeEngineID: 766d616e6167652d0a151515
  msgAuthoritativeEngineBoots: 1
  msgAuthoritativeEngineTime: 4490
  msgUserName: SNMP_V3_USER_VMANAGE
  msgAuthenticationParameters: ecb71af6d4616f7944426464
  msgPrivacyParameters: d2c8f7ee670781e2
  > msgData: encryptedPDU (1)

```

ءاطخأل احيحصت يف اطح "MIB. ضرع ةقيرط يف سيل OID CheckMIBView: OID ان اياحأ طحات دق  
 1.3.6.1.4.1). لاثملا لئبس ىلع) اهلا ل OID فضاو هالعأ SNMP ضرع ةقيرط نيوكت نم ققحت

## اهحالصإو ءاطخأل فاشكتسا

```

debug snmp detail debug snmp packets cEdge#test snmp trap config Generating CONFIG-MAN-MIB Trap
SPOKE-8#CheckMIBView: OID is in MIB view. CheckMIBView: OID is in MIB view. CheckMIBView: OID is
in MIB view. CheckMIBView: OID is in MIB view. CheckMIBView: OID is in MIB view. CheckMIBView:
OID is in MIB view. CheckMIBView: OID is in MIB view. SrCheckNotificationFilter: OID is
included. SrCheckNotificationFilter: OID is included. SrCheckNotificationFilter: OID is
included. SrCheckNotificationFilter: OID is included. SrCheckNotificationFilter: OID is
included. SrCheckNotificationFilter: OID is included. SrCheckNotificationFilter: OID is
included. Aug 19 14:30:16.527: SNMP: Queuing packet to 10.48.35.219Sr_send_trap: trap sent to
10.48.35.219:161:Mgmt-intf Aug 19 14:30:16.527: SNMP: V2 Trap, reqid 5564, errstat 0, erridx 0
sysUpTime.0 = 233561141 snmpTrapOID.0 = ciscoConfigManEvent ccmHistoryEventCommandSource.2 = 1
ccmHistoryEventConfigSource.2 = 2 ccmHistoryEventConfigDestination.2 = 2
ccmHistoryEventTerminalUser.2 = test SrV2GenerateNotification:Function has reached clean up
routine. Aug 19 14:30:16.777: SNMP: Packet sent via UDP to 10.48.35.219 cEdge#sh snmp | i sent
Logging to 10.48.35.219.161, 0/10, 3316 sent, 2039 dropped. cEdge#sh snmp user User name:
SNMP_V3_USER_VMANAGE Engine ID: 766D616E6167652D0A151515 storage-type: nonvolatile active
Authentication Protocol: SHA Privacy Protocol: AES128 Group-name: SNMP-GRP-VMANAGE cEdge#show
snmp group groupname: ILMI security model:v1 contextname:

```

## ةلص تاذا تاملعم

- [Cisco IOS و IOS-XE نيوكت لاثملا ةنمضم ةمزح طاقتل](#)
- [SNMP تامئالم مادختسا](#)
- [SNMP Object Navigator \(SNMP نئاك حفصتم\)](#)
- [Cisco Systems - تادنتس مل او ينقتل معدلا](#)

ةمچرتل هذه ل و ح

ةلأل تاي نقتل ن م ة و مچ م ادخت ساب دن ت س م ل ا اذ ه Cisco ت مچرت  
م ل ا ع ل ا اء ن ا ع مچ ي ف ن ي م د خ ت س م ل ل م ع د ي و ت ح م م ي د ق ت ل ة ي ر ش ب ل و  
ا م ك ة ق ي ق د ن و ك ت ن ل ة ل ا ة مچرت ل ض ف ا ن ا ة ظ ح ا ل م ي ج ر ي . ة ص ا خ ل ا م ه ت غ ل ب  
Cisco ي ل خ ت . ف ر ت ح م مچرت م ا ه م د ق ي ي ت ل ا ة ي ف ا ر ت ح ا ل ا ة مچرت ل ا ع م ل ا ح ل ا و ه  
ي ل ا م اء ا د ع و ج ر ل ا ب ي ص و ت و ت ا مچرت ل ا ه ذ ه ة ق د ن ع ا ه ت ي ل و ئ س م Cisco  
S y s t e m s ( ر ف و ت م ط ب ا ر ل ا ) ي ل ص ا ل ا ي ز ي ل ج ن ا ل ا د ن ت س م ل ا