Cisco SD-WAN SNMP Configuration Guide

First Published: 2019-04-25

Last Modified: 2021-06-22

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED “AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

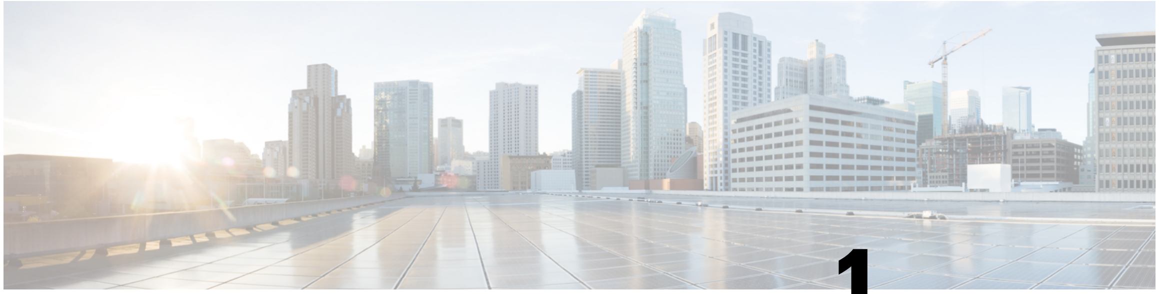
All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

CONTENTS

CHAPTER 1



CHAPTER 1

Cisco SD-WAN SNMP Configuration Guide

Read Me First

Related References

- Release Notes
- Cisco SD-WAN Controller Compatibility Matrix and Server Recommendations

User Documentation

- Cisco SD-WAN Command Reference

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: Cisco Profile Manager.
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit Cisco Services.
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit Cisco Devnet.

- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit Cisco Press.
- To find warranty information for a specific product or product family, visit Cisco Warranty Finder.
- To view open and resolved bugs for a release, access the Cisco Bug Search Tool.
- To submit a service request, visit Cisco Support.

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.

Note The documentation set for this product strives to use bias-free language. For purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Support for SMNP Traps on Cisco SD-WAN Devices

Table 1: Feature History

Feature Name	Release Information	Description
Support for Cisco SD-WAN Traps	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1 Cisco SD-WAN Release 20.6.1	This feature supports the receipt of the following SNMP trap notifications: • Certificate expiration notification on Cisco IOS XE SD-WAN devices and Cisco vEdge devices. • Health-monitoring notifications on Cisco vEdge devices, Cisco vBond Orchestrator, Cisco vSmart Controller, and Cisco vManage.

The SNMP agent on devices supports Cisco SD-WAN for generating and sending the SNMP traps to the SNMP manager.

The notifications that alert the SNMP manager are about the following issues:

- Enterprise certificate expiration notification for Cisco IOS XE SD-WAN devices and Cisco vEdge devices: The Certificate Authority (CA) server allows enrollment of certificates before a certificate expires to ensure the availability of certificates during authentication. However, network outages, clock update problems, and overloaded CAs can impede certificate renewal. The SNMP agent sends alert notifications using SNMP traps when certificates are on the verge of expiry.

  The SNMP agent sends traps or notifications at the following intervals:

  - First notification: This notification is sent 60 days before the expiry of the certificate.
  - Repeated notifications: After the first notification, subsequent notifications are sent every week until a week before the expiry of the certificate. In the last week, notifications are sent every day until the certificate expiry date.

  The notifications are in a *warning* mode when the certificate is valid for more than a week. The notifications are in an *alert* mode when the validity of a certificate is less than a week. The notifications include the following information:

  - Certificate type
  - Serial number of the certificate
  - Certificate issuer name
  - Number of days remaining for the certificate to expire

- Health monitoring notifications for Cisco vEdge devices and controllers: These notifications provide monitoring information for the set of objects such as file system or disk usage, CPU usage, and memory usage of Cisco SD-WAN controllers and Cisco vEdge devices.

  From Release 20.6.1, the traps are sent at the following levels of CPU usage:

  - Above 90 percent: Critical
  - Above 75 percent: Major
  - Below 75 percent: Minor

Configure SNMP using Cisco vManage

Use the SNMP template to configure SNMP parameters for all Cisco vEdge devices and Cisco IOS XE SD-WAN devices running the Cisco SD-WAN software.

Note A single device template can contain only one SNMP feature template. So in a single device template you can configure either SNMPv2 or SNMPv3, but not both.

Note All the SNMP versions are supported on Cisco IOS XE SD-WAN devices. However, SNMP v3 version is recommended because it is secure.

Note Viptela Management Information Base (MIBs) are not supported on Cisco IOS XE SD-WAN devices.

Note If your Network Management Stations (NMS) is reachable using a Cisco IOS XE SD-WAN device (for example, .biz internet or MPLS), ensure that the **allow-service snmp** command is enabled under the Transport VPN tunnel interface. This ensures that SNMP packets are not dropped.

The **allow-service snmp** command is specific for Cisco IOS XE SD-WAN devices. Ensure that the **allow-service snmp** command is enabled under the **sdwan > interface > tunnel-interface** configuration section as shown in the following example:

```
sdwan
 interface GigabitEthernet2
  tunnel-interface
   encapsulation ipsec
   color mpls
   allow-service all
   no allow-service bgp
   allow-service dhcp
   allow-service dns
   allow-service icmp
   allow-service sshd
   no allow-service netconf
   no allow-service ntp
   allow-service ospf
   no allow-service stun
   allow-service snmp
  exit
 exit
```

Navigate to the Template Screen and Name the Template

1. From the Cisco vManage menu, choose **Configuration** > **Templates** screen.
2. Click **Device**.
3. Click **Create Template**.
4. From the **Create Template** drop-down, select **From Feature Template**.
5. From the **Device Model** drop-down, select the type of device for which you are creating the template.
6. Click **Additional Templates** located directly beneath the Description field, or scroll to the **Additional Templates** section.
7. From the **SNMP** drop-down under Additional Templates, click **Create Template**.

   The SNMP template form is displayed. The top of the form contains fields for naming the template, and the bottom contains fields for defining SNMP parameters.
8. In the **Template Name** field, enter a name for the template. The name can be up to 128 characters and can contain only alphanumeric characters.
9. In the **Template Description** field, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

10. To save the SNMP feature template, click **Save**.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default or to enter a value, click the scope drop-down and select one of the following:

Table 2:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a Cisco IOS XE SD-WAN device or a Cisco vEdge device to a device template. When you click **Device Specific**, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a Cisco IOS XE SD-WAN device or a Cisco vEdge device to a device template. To change the default key, type a new string and move the cursor out of the Enter Key box. Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Attach the SNMP Feature Template to the Device Template

Once you have created the SNMP feature template, you need to attach the feature template to the device template.

To attach the SNMP feature template:

1. In **Device**, select the SNMP template that you created.
2. Click **...** and choose **Attach Devices**. The Attach Devices dialog box opens with **Select Devices** selected.
3. In the Available Devices column, select a group and search for one or more devices, select a device from the list, or click **Select All**.
4. Click the arrow pointing right to move the device to the Selected Devices column on the right.
5. Click **Attach**.

Configuring Basic SNMP

To configure basic SNMP, select **SNMP** and configure the following parameters. All parameters are required.

Table 3:

Parameter Name	Description
Shutdown	Click **No** to enable SNMP. By default, SNMP is disabled.
Name of Device for SNMP	Enter device name to identify it in SNMP notifications.
Contact Person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE SD-WAN device or a Cisco vEdge device. It can be a maximum of 255 characters.
Location of Device	Enter a description of the location of the device. It can be a maximum of 255 characters.

To save the feature template, click **Save**.

```
snmp
   contact string location string name string
  [no]  shutdown
```

Configure SNMPv2

To configure SNMPv2, select **SNMP Version** and click **V2**. For SNMPv2, you can configure communities and trap information.

To configure SNMP views, in the **View & Community** section, select **View**. Then click **Add New View**, and configure the following parameters:

Table 4:

Parameter Name	Description
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 255 characters. You must add a view name for all views before adding a community.
Object Identifiers	Click **Add Object Identifiers** and configure the following parameters: • Exclude OID—Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the Viptela MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • On/Odd—Click Off to include the OID in the view or click On to exclude the OID from the view. To save the object identifiers, click **Save**. To remove an OID from the list, click the minus sign next to the entry.

To add the SNMP view, click **Add**.

To configure the SNMP community, select **Community**. Then click **Add New Community**, and configure the following parameters:

Table 5:

Parameter Name	Description
Name	Enter the name for the community. The name can be from 1 through 32 characters and can include angle brackets (< and >).
Authorization	Select read-only from the drop-down list. The MIBs supported by the Cisco SD-WAN software do not allow write operations, so you can configure only read-only authorization.
View	Select a view to apply to the community. The view specifies the portion of the MIB tree the community can access.

To add the SNMP community, click **Add**.

To configure trap, in the Trap section, select **Trap Group**. Then click **Add New Trap Group**, and configure the parameters below.

Note Note that an Cisco IOS XE SD-WAN device has no trap groups. As such, you must create a dummy trap group before you can configure the trap target server.

Table 6:

Parameter Name	Description
Group Name	Enter a name for the trap group. It can be from 1 to 32 characters long.

Parameter Name	Description
Trap Type Modules	Click **Add Trap Type Modules**, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap—critical, major, or minor. In **Module Name**, select the type of traps to include in the trap group: • all—All trap types. • app-route—Traps generated by application-aware routing. • bfd—Traps generated by BFD and BFD sessions. • control—Traps generated by DTLS and TLS sessions. • dhcp—Traps generated by DHCP. • hardware—Traps generated by Viptela hardware. • omp—Traps generated by OMP. • routing—Traps generated by BGP, OSPF, and PIM. • security—Trap generated by certificates, vSmart and vEdge serial number files, and IPsec. • system—Traps generated by system-wide functions. • vpn—Traps generated by VPN-specific functions, including interfaces and VRRP.

To save the trap type module, click **Save**.

To configure trap target servers, in the Trap section, select **Trap Target Server**. Then click **Add New Trap Group**, and configure the parameters below.

Note On a Cisco vEdge device, you can bind a different source interface to each trap target server. On a Cisco IOS XE SD-WAN device, however, the last occurrence of the source interface is chosen as the global source interface.

Table 7:

Parameter Name	Description
VPN ID	Enter the number of the VPN to use to reach the trap server.*Range:* 0 through 65530
IP Address	Enter the IP address of the SNMP server.
UDP Port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Group Name	Select the name of a trap group that was configured under Group.
Community Name	Select the name of a community that was configured under Community.

Parameter Name	Description
Source Interface	Enter the interface to use to send traps to the SNMP server that is receiving the trap information.

To save the trap target, click **Add**.

To save the feature template, click **Save**.

CLI Equivalent:

```
snmp
  community name
    authorization (read-only | read-write)
    view string
  contact string
  group group-name authentication
    view string
  location string
  name string
  [no] shutdown
  trap
    group group-name
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name group-name
      source-interface interface-name
  user username
    auth authentication
    auth-password password
    group group-name
    priv privacy
    priv-password password
```

Configure SNMPv3

Table 8: Feature History

Feature Name	Release Information	Description
Support for SNMPv3 AES-256 bit Authentication Protocol	Cisco SD-WAN Release 20.5.1	Support introduced for AES-256 bit Authentication Protocol called SHA-256.

To configure SNMPv3, in SNMP Version, click **V3**. For SNMPv3, you can configure groups, users, and trap information. Configure groups and trap information as described above.

To configure SNMPv3 users, in the User section, click **Add New User** and enter the following parameters:

Table 9:

Parameter Name	Description
User	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.

Parameter Name	Description
Authentication Protocol	Select the authentication mechanism for the user: • SHA-1 message digest. • SHA-256 message digest. **Note** Starting from Cisco SD-WAN Release 20.5.1, SHA-256 authentication protocol was introduced. When you choose SHA-256 as the authentication protocol, you must set the security level as `authPriv`. **Note** MD5 authentication protocol is deprecated for Cisco SD-WAN Release 20.3.2 and later releases.
Authentication Password	Enter the authentication password either in cleartext or as an AES-encrypted key.
Privacy Protocol	Select the privacy type for the user: • For SHA-1 authentication protocol: AES-CFB-128—Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. • Starting from Cisco SD-WAN Release 20.5.1, for SHA-256 authentication protocol: AES-256-CFB-128—Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 256-bit key.
Privacy Password	Enter the authentication password either in cleartext or as an AES-encrypted key.
Group	Select the name of a configure SNMPv3 group.

Note An SNMP trap message for an AES user has both **`msgAuthoritativeEngineBoots`** and **`msgAuthoritativeEngineTime`** set to a meaningful value. But the SNMP trap message for an AES256 user has **`msgAuthoritativeEngineBoots`** and **`msgAuthoritativeEngineTime`** set to 0. The trap receiver should ignore **`msgAuthoritativeEngineBoots`** and **`msgAuthoritativeEngineTime`** in the SNMP trap message.

To save the user, click **Add**.

To save the feature template, click **Save**.

CLI Equivalent:

```
snmp group group-name authentication
 view string
!
user u1
 auth          sha
 auth-password $8$UZwdx9eu49iMElcJJINm0f202N8/+RGJvxO+e9h0Uzo=
 priv          aes-cfb-128
 priv-password $8$eB/I+VXrAWDw/yWmEqLMsgTcs0omxcHldkVN2ndU9QI=
 group         groupAuthPriv
 !
```

Note The SNMP walk application is blocked if you switch the SNMPv3 configuration to SNMPv2 configuration in the device template and apply this change through a template push. This is because the **snmp mib community-map** command for SNMPv3 is not removed during the configuration change. Hence, you cannot switch from SNMPv3 to SNMPv2 directly, when the SNMPv3 configuration template is active. To switch to SNMPv2, you must first remove the SNMPv3 configuration from the device and then push the SNMPv2 template through a separate commit.

Release Information

Introduced in Cisco vManage in Release 15.2. In Release 16.2, add support for SNMPv3. In Release 17.2, remove support for DES privacy for the SNMP user.

Configure SNMP with Encrypted Strings Using CLI Templates

Table 10: Feature History

Feature Name	Release Information	Description
Configure SNMP with Encrypted Strings Using CLI Templates	Cisco vManage Release 20.5.1	This feature enables you to configure SNMP using a CLI template or a CLI add-on feature template. You can also encrypt the supported variables in the CLI configuration.

Use the CLI template feature or CLI add-on feature template to configure SNMP and also encrypt supported variables on Cisco IOS XE SD-WAN devices. For more information on the encryption, see Type 6 Passwords on Cisco IOS XE SD-WAN Routers

Note If you encrypt plaintext strings using the CLI add on feature template, the strings are not encrypted in MIBs.

You cannot modify an existing SNMP community to convert it to encrypted strings. To encrypt the strings, you must delete and recreate the SNMP communities.

1. Navigate to **Configuration** > **Templates**
2. Use one of the following templates to add the CLI:
   - CLI add-on feature templates
     a. Click **Feature**.
     b. Click **Add Template**.
     c. Under the Select Devices pane, select the Cisco IOS XE SD-WAN device devices for which you are creating the template.
     d. Under the Select Template pane, scroll down to the Other Templates section.

e. Click **CLI Add-On Template**.

- CLI templates

a. In **Device**, click **Add Template**.

b. From the **Create Template** drop-down, select **CLI Template**.

c. Under the Select Devices pane, select the Cisco IOS XE SD-WAN device devices for which you are creating the template.

3. In the Template Name field, enter a name for the feature template. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (-), and underscores (_). It cannot contain spaces or any other characters.
4. In the Description field, enter a description for the device template. This field is mandatory, and it can contain any characters and spaces.
5. In the CLI Configuration box, enter the configuration either by typing it, cutting and pasting it, or uploading a file.
6. To encrypt plaintext values such as passwords or the SNMP community string, select the text and click **Encrypt Type6**.
7. To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**. You can also type the variable name directly, in the format `{{variable-name}}`. For example: `{{hostname}}`.
8. Click **Save**. The new feature template is displayed the Feature Template table.
9. To use the CLI add-on feature template, edit the device template as follows:

a. In the **Templates** page, click **Device**.

b. Select the device template for which you want to add the CLI add-on feature template.

c. Click **...** and choose **Edit**.

d. Scroll to the **Additional Templates** section.

e. In the CLI Add-On Template field, select the CLI add-on feature template that you previously created.

f. Click **Update**.

Configure SNMP on Cisco IOS XE SD-WAN Devices Using CLI

The following sections provide information about the various tasks that comprise the configuration of the SNMP on Cisco IOS XE SD-WAN devices.

Assign SNMP Agent System Information

Set the system contact and location of the SNMP agent.

1. Set the system contact string, which is the SNMP contact name:

```
Device# config-transaction
Device(config)# snmp-server contact text
```

2. Set the system location string, which is the SNMP location:

```
Device(config)# snmp-server location text
```

Configure Context-to-Network Entity Mapping

Configure an SNMP context-to-map to a logical network entity, such as a virtual routing and forwarding (VRF):

1. Map an SNMP context to a logical network, using the following command:

```
Device# config-transaction
Device(config)# snmp-server context context-name
```

2. Enable SNMP authorization failure (authFail) traps during an unknown SNMP context error:

```
Device(config)# snmp-server trap authentication unknown-context
```

Configure SNMPv1 and SNMPv2c

(Optional) When you configure SNMPv1 and SNMPv2c, you can optionally create or modify views for community strings to limit which MIB objects an SNMP manager can access using the following procedure:

1. Create or modify an SNMP view along with an Object Identifier (OID):

```
Device# config-transaction
Device(config)# snmp-server view view-name oid-tree included
```

2. Create or modify access control for an SNMP community:

```
Device(config)# snmp-server community string [view view-name][ro |rw
][access-list-number/name]
```

Configure SNMPv3

Ensure that you configure SNMP groups and users with passwords to configure SNMPv3 and to use the SNMPv3 security mechanism for handling SNMP packets.

1. Specify a new SNMPv3 server group or a table that maps SNMP users to SNMP views:

```
Device# config-transaction
Device(config)# snmp-server group [group-name{v1 |v2c |v3 |[auth |noauth |priv ]}][read
 readview][write writeview
][notify notifyview][access access-list]
```

2. Configure a new user to an SNMPv3 group:

```
Device(config)# snmp-server user username groupname [remote ip-address[udp-port port]]{v1
 |v2c |v3 [encrypted][auth {md5|sha} auth-password]}[access access-list]
```

Define the Maximum SNMP Agent Packet Size

Define the maximum packet size that is permitted when the SNMP agent is receiving a request or generating a reply:

```
Device# config-transaction
Device(config)# snmp-server packetsize byte-count
```

Configure SNMP Notifications

Configure a device to send SNMP traps.

1. Specify the recipient of an SNMP notification operation:

```
Device# config-transaction
Device(config)# snmp-server host {host-name|ip-address}[vrf
vrf-name|traps|version{1|2c|3[auth|noauth|priv]}]community-string
[udp-port port [notification-type]|notification-type]
```

2. Change SNMP notification operation values:

```
Device(config)# snmp-server  trap-source interface
```

Enable SNMP Notifications

Note that you can enable or disable SNMP notifications.

Use the following commands in configuration mode to enable the specified notification.

1. Enable all Cisco SD-WAN notifications:

```
Device# config-transaction
Device(config)# snmp-server enable traps sdwan
```

2. Enable SNMP notifications for rising alarm changes:

```
Device(config)# snmp-server enable traps alarms priority
```

3. Enable SNMP notifications for configuration changes:

```
Device(config)# snmp-server enable traps config
```

4. Send entity MIB notifications to a host:

```
Device(config)# snmp-server enable traps entity
```

5. Send information about the state of physical components such as disk, memory, and CPU utilization:

```
Device(config)# snmp-server enable traps entity-state
```

6. Enable SNMP notifications for OSPF transition state changes on a virtual or nonvirtual OSPF interface:

```
Device(config)# snmp-server enable traps ospf state-change
```

7. Enable SNMP notifications for OSPF errors (authentication failure, bad packet issues, and configuration errors):

```
Device(config)# snmp-server enable traps ospf errors
```

8. Enable SNMP notifications for OSFP link-state advertisements (LSAs):

```
Device(config)# snmp-server enable traps ospf lsa
```

9. Enable SNMP notifications for OSPF configuration mismatch errors on virtual or nonvirtual interfaces:

```
Device(config)# snmp-server enable traps ospf cisco-specific errors
```

10. Enable the authentication failure, linkup, linkdown, coldstart, or warmstart notifications:

```
Device(config)# snmp-server enable traps snmp
[authentication][linkup][linkdown][coldstart][warmstart]
```

Configure Interface Index Persistence

You can globally enable ifIndex values in the IF-MIB so that it persists across reboots. This configuration allows consistent identification of specific interfaces that use SNMP.

```
Device# config-transaction
Device(config)# snmp ifmib ifindex persist
```

To configure SNMP traps using Cisco vManage, use the information provided in CLI Add-on Feature templates to enter the configuration applicable to your environment. The following example shows how to configure SNMP to send traps to 172.16.1.111 and 172.16.1.27 using SNMPv2c, and to the host 172.16.1.33 using SNMPv3. The SNMP traps are sent by configuring a VRF routing table and address family submode.

```
config-transaction
!

       vrf definition 172
       address-family ipv4
       exit-address-family

       snmp-server contact Admin
       snmp-server location Lab-7

       snmp-server context CISCOCONTEXT
       no snmp-server trap authentication unknown-context
!
       snmp-server view v2 1.3.6.1.6.3.15 included
       snmp-server community public view v2 ro
       snmp-server view v3 1.3.6.1.6.3.18 included
!
       snmp-server community private view v3 ro 5
       snmp-server community public view v3 ro
       snmp-server group groupNoAuthNoPriv v3 noauth read v3

!
       snmp-server packetsize 1300
       snmp-server host 172.16.1.27 vrf 172 version 2c public udp-port 162
       snmp-server host 172.16.1.111 vrf 172 version 2c public udp-port 161
       snmp-server host 172.16.1.33 vrf 172 version 3 auth v3userAuthPriv udp-port 16664

       snmp-server trap-source Loopback0
!
       snmp-server enable traps sdwan
       snmp-server enable traps alarms informational
       snmp-server enable traps config
       snmp-server enable traps entity
       snmp-server enable traps entity-state
       snmp-server enable traps snmp authentication coldstart linkdown linkup warmstart
       snmp-server enable traps ospf state-change
       snmp-server enable traps ospf errors
       snmp-server enable traps ospf lsa
       snmp-server enable traps ospf cisco-specific errors!
       snmp-server enable traps ospf state-change
       snmp-server enable traps ospf errors
!
       snmp ifmib ifindex persist
!
```

Verify SNMP Traps on Cisco IOS XE SD-WAN Devices

The following is a sample output from the **show snmp user** command to show the user information configured for SNMPv3:

```
Device# show snmp user

User name: v3userAuthPriv
Engine ID: 800000090300000C88B487400
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: groupAuthPriv

User name: v3userNoAuthNoPriv
Engine ID: 800000090300000C88B487400
storage-type: nonvolatile active
Authentication Protocol: None
Privacy Protocol: None
Group-name: groupNoAuthNoPriv
```

The following example shows a trap notification that appears after uninstalling a root certificate for Cisco Catalyst 8000V using the **request platform software sdwan root-cert-chain uninstall** command:

```
2021-06-15 15:26:38 UDP: [198.51.100.1]:61114->[172.16.53.199]:162 [UDP:
[198.51.100.1]:61114->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (5155837) 14:19:18.37
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityRootCertChainUninstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

The following example shows a trap notification that appears after installing a root certificate for Cisco Catalyst 8000V using the **request platform software sdwan root-cert-chain install** command:

```
2021-06-15 01:16:55 UDP: [10.6.40.204]:50433->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50433->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (2143576) 5:57:15.76
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityRootCertChainInstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

The following example shows a trap notification that appears after removing installed certificates for Cisco Catalyst 8000V using the **clear sdwan installed-certificates** command:

```
2021-06-15 14:18:26 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (103213) 0:17:12.13
SNMPv2-MIB::snmpTrapOID.0 = OID:
```

```
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityClearInstalledCertificate
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

The following example shows a trap notification that appears after creating a certificate sign request certificate for Cisco Catalyst 8000V using the **request platform software sdwan csr upload flash** command:

```
Uploading CSR via VPN 0
Enter organization-unit name : CISCO
Re-enter organization-unit name : CISCO
Generating private/public pair and CSR for this "vedge" device
Generated CSR for vedge device
Copying /usr/share/viptela/server.csr to /bootflash/c8kv1.csr via VPN 0
CSR upload successful
c8kv1#

2021-06-15 14:20:14 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (114062) 0:19:00.62
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityNewCsrGenerated
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

The following example shows a trap notification that appears after installing a signed certificate for Cisco Catalyst 8000V using the **request platform software sdwan certificate install** command:

```
Installing certificate via VPN 0
Changing ownership of vedge_certs to binos...
Copying /bootflash/c8kv1.crt to /tmp/vconfd/server.crt.tmp via VPN 0
Got certificate_id 0123CF for /tmp/vconfd/server.crt.tmp vmanage_signed false
cp -f "/usr/share/viptela/tmp_csr/server.key" "/usr/share/viptela/server.key"
moving temp Cert "/tmp/vconfd/server.crt.tmp" to Cert
"/usr/share/viptela/vedge_certs/client_0123CF.crt"

Successfully installed the certificate 0

2021-06-15 14:24:02 UDP: [10.6.40.204]:50258->[172.16.53.199]:162 [UDP:
[10.6.40.204]:50258->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (136870) 0:22:48.70
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateInstalled
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: minor(3)
```

The following example shows a trap notification for a certificate that is expiring using the **show control local-properties** command. Here, a certificate of Cisco Catalyst 8000V is expiring today but it's not yet expired:

```
2021-07-06 21:04:17 UDP: [1.6.40.204]:53342->[172.27.53.199]:162 [UDP:
[1.6.40.204]:53342->[172.27.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (41478) 0:06:54.78
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateExpiring
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityCertificateType.0 = INTEGER: enterprise(2)
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityCertificateSerialNumber.0 = STRING: "01240F"
```

```
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityIssuer.0 = STRING: "XCA"
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecurityDaysToExpiry.0 = INTEGER: 1
```

The following example shows a trap notification for a certificate that has expired on Cisco Catalyst 8000V device using the **show control local-properties** command:

```
2021-06-15 15:59:16 UDP: [209.165.202.129]:49387->[172.16.0.199]:162 [UDP:
[209.165.202.129]:49387->[172.16.0.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (44510) 0:07:25.10
SNMPv2-MIB::snmpTrapOID.0 = OID:
CISCO-SDWAN-SECURITY-MIB::ciscoSdwanSecuritySecurityCertificateExpired
CISCO-SDWAN-SECURITY-MIB::netconfNotificationSeverity.0 = INTEGER: major(2)
```

Configure SNMP on Cisco vEdge Devices Using the CLI

Enabling SNMP

By default, SNMP is disabled on Cisco vEdge devices. To enable it and provide support for SNMP Versions 1, 2, and 3:

```
vEdge(config)# snmp
vEdge(config-snmp)# no shutdown
```

Enabling SNMP allows the device to use MIBs, generate traps, and respond to requests from an SNMP walk application.

Configuring an SNMP View

To create an SNMP view, along with an OID, so that SNMP information is available to the SNMP server, configure an SNMP view and its corresponding OID subtree:

```
vEdge(config-snmp)#  view string
vEdge(config-snmp)#  oid oid-subtree
```

In the OID subtree, you can use the wildcard * (asterisk) in any position to match any value at that position.

The following example creates a view of the Internet portion of the SNMP MIB:

```
vEdge(config)# snmp view v2 oid 1.3.6.1
```

The following example creates a view of the private portion of the Cisco SD-WAN MIB:

```
vEdge(config)# snmp view vEdge-private oid 1.3.6.1.4.1.41916
```

Configuring Access to an SNMP View

To require authentication privileges to access an SNMP view, configure SNMPv3. To do this, you configure authentication credentials for SNMPv3 users, and you configure groups of SNMP views and the authentication credentials required to access the views.

To configure authentication credentials for an SNMPv3 user, create a user and assign them an authentication level and a privacy level, depending on the authentication type you configure for the SNMP group (with the **snmp group** command, described below):

```
vEdge(config)# snmp user username
vEdge(config-user)# auth authentication
vEdge(config-user)# auth-password password
vEdge(config-user)# priv privacy
vEdge(config-user)# priv-password password
```

The username can be a string from 1 to 32 characters.

The authentication commands enable authentication privileges for the user. You can enter the password as a cleartext string or as an AES-encrypted key.

The privacy commands enable a privacy mechanism for the user. You can enter the password as a cleartext string or as an AES-encrypted key.

Then associate the SNMPv3 user with an SNMP group:

```
vEdge(config-user)# group group-name
```

group-name is the name of a group of views that you configure with the **snmp group** command.

To configure a group of views:

```
vEdge(config)# snmp group group-name authentication
vEdge(config-group)# view view-name
```

The group name can be a string from 1 to 32 characters.

The authentication to use for the group can be one of the following:

- **auth-no-priv**—Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password (with the **snmp user auth** and **auth-password** commands).
- **auth-priv**—Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password (with the **snmp user auth** and **auth-password** commands) and a privacy and privacy password (with the **snmp user priv** and **priv-password** commands).
- **no-auth-no-priv**—Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials.

Note Use two separate transactions to move an SNMP user to a new group and to delete the old group. Moving an SNMP user to a new group and deleting the old group in the same transaction is not supported.

The view name is the name of an SNMP view that you configure with the **snmp view** command.

Configuring Contact Parameters

For each Cisco vEdge device, you can configure its SNMP node name, physical location, and contact information for the person or entity responsible for the device:

```
vEdge(config)#  snmp
vEdge(config-snmp)#  name string
vEdge(config-snmp)#  location string
vEdge(config-snmp)#  contact string
```

If any of the strings include spaces, enclose the entire string in quotation marks (" ").

Configuring an SNMP Community

The SNMP community string defines the relationship between an SNMP server system and the client systems. This string acts like a password to control the clients' access to the server. To configure a community string, use the **community** command:

```
vEdge(config-snmp)#  community name
vEdge(config-community-name)# authorization read-only
vEdge(config-community-name)# view string
```

The community name can be 1 through 32 characters long. It can include angle brackets (< and >). If the name includes spaces, enclose the entire name in quotation marks (" ").

Use the **view** command to specify the portion of the MIB tree to view. *string* is the name of a view record configured with the **snmp view** command, as described below.

The Cisco SD-WAN software supports the standard interfaces, MIB, IF-MIB, and the system MIB (SNMPv2-MIB), which are automatically loaded onto the Cisco vEdge device when you install the Cisco SD-WAN software. For a list of enterprise MIBs, see Supported SNMP MIBs. The MIBs supported by the Cisco SD-WAN software do not allow write operations, so you can configure only read-only authorization (which is the default authorization).

Configuring View Records

To configure a portion of an SNMP MIB to view, use the **view** command:

```
vEdge(config-snmp)#  view string
vEdge(config-view)# oid oid-subtree [exclude]
```

For example, to view the internet portion of the SNMP MIB, configure the OID 1.3.6.1:

```
vEdge(config-snmp)# view v2 oid 1.3.6.1
```

To view the private portion of the Cisco SD-WAN MIB, configure the OID 1.3.6.1.4.1.41916.

SNMP Configuration Commands

Use the following commands to configure SNMP:

```
snmp
  community name
    authorization (read-only | read-write)
    view string
  contact string
  group group-name authentication
    view string
  location string
  name string
  [no] shutdown
  trap
    group group-name
      trap-type
        level severity
    target vpn vpn-id ip-address udp-port
      community-name community-name
      group-name group-name
      source-interface interface-name
  user username
    auth authentication
    auth-password password
    group group-name
    priv privacy
    priv-password password
```

SNMP Monitoring Commands

Use the following command to monitor SNMP:

Use the **show running-config snmp** command to monitor SNMP. The command output shows the active configuration that is running on the Cisco vEdge device.

Verify SNMP Traps on Cisco vEdge Devices

The following is a sample output of the **show full-configuration** command:

```
vEdge(config-snmp)# show full-configuration
snmp
 no shutdown
 view v2
  oid 1.3.6.1
 !
 group groupAuthPriv auth-priv
  view v2
 !
 user noc-staff
  auth          sha
  auth-password $8$UZwdx9eu49iMElcJJINm0f202N8/+RGJvxO+e9h0Uzo=
  priv          aes-cfb-128
  priv-password $8$eB/I+VXrAWDw/yWmEqLMsgTcs0omxcHldkVN2ndU9QI=
  group         groupAuthPriv
 !
!
```

The following is a sample output of the **show running-config snmp** command, introduced in Cisco SD-WAN Release 20.5.1:

```
vEdge(config-snmp)# show running-config snmp
snmp
 no shutdown
 view v3
  oid 1.3.6.1
!
 group groupAuthPriv auth-priv
  view v3
!
 user v3userAuthPriv-sha-aes
  auth          sha-256
  auth-password $8$QiM+RsTn8WBaufWNAPleqzhYtNSSQxtDPciQayxz73s=
  priv          aes-256-cfb-128
  priv-password $8$rsgqMKrWt4JwvBIrWW0gG/VH9tiMl7oAHjFbzrd818k=
  group         groupAuthPriv
 !
!
```

The following example shows a trap notification for disk usage that is higher than 75 percent and sent to the Network Management Server (NMS):

```
2021-06-21 22:35:05 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53772780) 6 days, 5:22:07.80
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:7:3.0,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER:major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is above 75%." Please clean up
 unnecessary files. If disk usage grows beyond 90%, system will attempt to recover disk
space by deleting files"
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 1174
```

After the disk usage normalizes, the trap notification is sent to NMS:

```
2021-06-21 22:40:29 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53805175) 6 days, 5:27:31.75
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:12:27.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is below 60%."
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 7362
```

The following example shows a trap notification when disk usage is above 75 percent:

```
2021-06-21 22:35:05 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.27.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53772780) 6 days, 5:22:07.80
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:7:3.0,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is above 75%." Please clean up
 unnecessary files. If disk usage grows beyond 90%, system will attempt to recover disk
space by deleting files
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 1174
```

After disk usage drops to below 60 percent, the trap notification sent to NMS:

```
2021-06-21 22:40:29 UDP: [172.27.58.143]:54392->[172.27.53.199]:162 [UDP:
[172.27.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53805175) 6 days, 5:27:31.75
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemDiskUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:12:27.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "Disk usage is below 60%."
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 7985
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 7362
```

The following example shows the trap notifications when CPU usage increases to a high level and then returns to a normal level:

```
2021-06-21 22:53:49 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53885189) 6 days, 5:40:51.89
SNMPv2-MIB::snmpTrapOID.0 = OID:
```

```
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:47.2,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage is above 75%"
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.01"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "80.40"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "18.59"

2021-06-21 22:53:53 UDP: [172.16.58.143]:54392->[172.27.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.27.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53885589) 6 days, 5:40:55.89
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:51.2,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: critical(1)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage is above 90% (critically
 high)"
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.51"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "98.49"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "0.00"

2021-06-21 22:54:01 UDP: [172.16.58.143]:54392->[172.16.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.16.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (53886390) 6 days, 5:41:03.90
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemCpuUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:25:59.1,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: minor(3)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System cpu usage back to normal level"
VIPTELA-TRAPS::viptelaSystemCpuUserPercentage.0 = STRING: "1.52"
VIPTELA-TRAPS::viptelaSystemCpuSystemPercentage.0 = STRING: "1.52"
VIPTELA-TRAPS::viptelaSystemCpuIdlePercentage.0 = STRING: "96.97"
```

The following is a trap notification for system memory usage that is higher than 75 percent:

```
2021-06-21 23:15:22 UDP: [172.16.58.143]:54392->[172.16.53.190]:162 [UDP:
[172.16.58.143]:54392->[172.16.53.190]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (54014426) 6 days, 6:02:24.26
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSystemMemoryUsage
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-23,5:47:19.5,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSystemWarning.0 = STRING: "System memory usage is above 75%"
VIPTELA-TRAPS::viptelaSystemTotalMb.0 = Gauge32: 3902
VIPTELA-TRAPS::viptelaSystemFreeMb.0 = Gauge32: 965
```

The following is a trap notification for a certificate that is expiring. Here, a Cisco vEdge device certificate is expiring today, but is not yet expired:

```
2021-06-15 16:53:29 UDP: [172.16.58.43]:56734->[172.16.53.199]:162 [UDP:
[172.16.58.43]:56734->[172.16.53.199]:162]:
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (92594) 0:15:25.94
SNMPv2-MIB::snmpTrapOID.0 = OID:
VIPTELA-TRAPS::viptelaSecuritySecurityCertificateExpiring
VIPTELA-TRAPS::eventTime.0 = STRING: 2021-6-15,23:53:3.5,+0:0
VIPTELA-TRAPS::netconfNotificationSeverity.0 = INTEGER: major(2)
VIPTELA-TRAPS::viptelaSecurityCertificateType.0 = INTEGER: enterprise(2)
VIPTELA-TRAPS::viptelaSecurityCertificateSerialNumber.0 = STRING: "0123D1"
```

```
VIPTELA-TRAPS::viptelaSecurityIssuer.0 = STRING: "XCA"
VIPTELA-TRAPS::viptelaSecurityDaysToExpiry.0 = INTEGER: 0
```

Configure SNMP Traps on Cisco vEdge Devices

The SNMP traps are asynchronous notifications that a Cisco device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the device. By default, SNMP traps aren’t sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

To configure SNMP traps, define the traps and configure the SNMP server that receives the traps.

Note The **trap group** UI option isn’t supported from Cisco SD-WAN Release 20.1.1 and later.

To configure groups of traps to be collected on Cisco vEdge devices, use the **trap group** command:

Note You don't need to configure groups of traps on Cisco IOS XE SD-WAN devices.

```
vEdge(config-snmp)#  trap group group-name
vEdge(config-group)# trap-type level severity
```

A single trap group can contain multiple trap types. In the configuration, specify one trap type per line, and each trap type can have one, two, or three severity levels. See the following configuration example for an illustration of the configuration process.

To configure the SNMP server to receive the traps, use the **trap target** command on Cisco vEdge devices:

Note You don't need to configure the SNMP server to receive the traps on Cisco IOS XE SD-WAN devices.

```
vedge(config-snmp)#  trap target vpn  vpn-id ipv4-address udp-port
vedge(config-target)# group-name name
vedge(config-target)# community-name community-name
vedge(config-target)# source-interface interface-name
```

For each SNMP server, specify the identifier of VPN where the server is located, the server's IPv4 address, and the UDP port on the server to connect to. When configuring the trap server's address, you must use an IPv4 address. You can’t use an IPv6 address.

In the **group-name** command, associate a previously configured trap group with the server. The traps in that group are sent to the SNMP server.

In the **community-name** command, associate a previously configure SNMP community with the SNMP server.

In the **source-interface** command, configure the interface to use to send traps to the SNMP server that is receiving the trap information. This interface cannot be a subinterface.

In the following configuration example, all traps are sent to one SNMP server and only critical traps to another SNMP server. Two SNMP trap groups and the two target SNMP servers are configured:

```
vEdge# config
Entering configuration mode terminal
vEdge(config)# snmp
vEdge(config-snmp)# view community-view
vEdge(config-view-community-view)# exit
vEdge(config-snmp)# community public
vEdge(config-community-public)# authorization read-only
vEdge(config-community-public)# view community-view
vEdge(config-community-public)# exit
vEdge(config-snmp)# trap group all-traps
vEdge(config-group-all-traps)# all level critical major minor
vEdge(config-group-all)# exit
vEdge(config-group-all-traps)# exit
vEdge(config-snmp)# trap group critical-traps
vEdge(config-group-critical-traps)# control level critical
vEdge(config-group-control)# exit
vEdge(config-group-critical-traps)# exit
vEdge(config-snmp)# trap target vpn 0 10.0.0.1 162
vEdge(config-target-0/10.0.0.1/162)# group-name all-traps
vEdge(config-target-0/10.0.0.1/162)# community-name public
vEdge(config-target-0/10.0.0.1/162)# exit
vEdge(config-snmp)# trap target vpn 0 10.0.0.2 162
vEdge(config-target-0/10.0.0.2/162)# group-name critical-traps
vEdge(config-target-0/10.0.0.2/162)# community-name public
vEdge(config-target-0/10.0.0.2/162)# exit
vEdge(config-snmp)# show full-configuration
snmp
 view community-view
 !
 community public
  view          community-view
  authorization read-only
 !
 group groupAuthPriv auth-priv
  view v2
 !
 user u1
  auth          sha
  auth-password $8$UZwdx9eu49iMElcJJINm0f202N8/+RGJvxO+e9h0Uzo=
  priv          aes-cfb-128
  priv-password $8$eB/I+VXrAWDw/yWmEqLMsgTcs0omxcHldkVN2ndU9QI=
  group         groupAuthPriv
 !
 trap target vpn 0 10.0.0.1 162
  group-name     all-traps
  community-name public
 !
 trap target vpn 0 10.0.0.2 162
  group-name     critical-traps
  community-name public
 !
 trap group all-traps
  all
   level critical major minor
  !
 !
 trap group critical-traps
  bfd
   level critical
  !
  control
   level critical
  !
```

```
    hardware
     level critical
    !
    omp
     level critical
    !
  !
!
vEdge(config-snmp)#
```

Information About SNMP Traps and Notifications

SNMP trap supports multiple severity levels - critical, major, and minor.

The *trap-type* can be one of the variables listed in the following table:

Table 11: SNMP Traps for Cisco IOS XE SD-WAN Devices

Trap Type	Severity Level - Critical	Service Level - Major	Service Level - Minor
control	—	ciscoSdwanSecurityControlConnectionStateChange	—
policy	—	ciscoSdwanPolicyAccessListAssociationStatus ciscoSdwanPolicyDataPolicyAssociationStatus ciscoSdwanPolicySlaViolationPktDrop	ciscoSdwanPolicySlaViolation
security	—	ciscoSdwanSecuritySecurityCertificateExpired ciscoSdwanSecuritySecurityCertificateExpiring ciscoSdwanSecuritySecurityRootCertChainUninstalled ciscoSdwanSecuritySecurityClearInstalledCertificate ciscoSdwanSecuritySecurityVsmartEntryAdded	ciscoSdwanSecuritySecurityRootCertChainInstalled ciscoSdwanSecuritySecurityCertificateInstalled ciscoSdwanSecuritySecurityNewCsrGenerated ciscoSdwanSecurityTunnelIpsecRekey
system	—	ciscoSdwanSystemPseudoCommitStatus	ciscoSdwanSystemDomainIdChange ciscoSdwanSystemOrgNameChange ciscoSdwanSystemSiteIdChange ciscoSdwanSystemSystemCommit ciscoSdwanSystemSystemIpChange

Table 12: SNMP Traps for Cisco vEdge Devices

Trap Type	Severity Level - Critical	Service Level - Major	Service Level - Minor
all	All critical traps are listed in the following cells in this table.	All major traps are listed in the following cells in this table.	All minor traps are listed in the following cells in this table.

Trap Type	Severity Level - Critical	Service Level - Major	Service Level - Minor
app-route	—	SLA_Change	—
bfd	—	BFD_State_Change	—
bridge	—	—	Bridge_Creation Bridge_Deletion Max_MAC_Reached
control	No_Active_vBond No_Active_vSmart	Connection_Auth_Fail Connection_State_Change Connection_TLOC_IP_Change vBond_State_Change	—
dhcp	—	Server_State_Change	Address_Assigned Address_Released Address_Renewed Request_Rejected Server_State_Change
hardware	—	EMMC_Fault Fan_Fault FanTray_Fault Flash_Fault PEM_Fault PEM_State_Change PIM_Fault PIM_State_Change SDCard_Fault SFP_State_Change TempSensor_Fault TempSensor_State USB_State_Change	—
omp	—	Data_Policy Number_of_vSmarts_Change Peer_State_Change State_Change TLOC_State_Change	—

Trap Type	Severity Level - Critical	Service Level - Major	Service Level - Minor
policy	—	Access_List_Association_Status Data_Policy_Association_Status SLA_Violation_Pkt_Drop	SLA_Violation
routing	—	BGP_Peer_State_Change OSPF_Interface_State_Change OSPF_Neighbor_State_Change PIM_Interface_State_Change PIM_Neighbor_State_Change PIM_Tunnel_State_Change	—
security	—	Certificate_Expired Certificate_Expiring Clear_Installed_Certificate Root_Cert_Chain_Uninstalled vEdge_Entry_Added vEdge_Entry_Removed vEdge_Serial_File_Uploaded vSmart_Entry_Added vSmart_Entry_Removed vSmart_Serial_File_Uploaded	Certificate_Installed New_CSR_Generated Root_Cert_Chain_Installed Tunnel_IPSec_Manual_Rekey Tunnel_IPSec_Rekey
system	CPU_Usage Disk_Usage Memory_Usage	AAA_Admin_Pwd_Change CPU_Usage Disk_Usage Memory_Usage Process_Restart System_AAA_Login_Fail System_Pseudo_Commit_Status System_Reboot_Complete	CPU_Usage Disk_Usage Domain_ID_Change Memory_Usage Org_Name_Change Reboot_Issued Site_ID_Change Software_Install_Status System_Commit System_IP_Change System_Login_Change System_Logout_Change
vpn	—	Interface_State_Change VRRP_Group_State_Change	Route_Install_Fail Tunnel_Install_Fail

Trap Type	Severity Level - Critical	Service Level - Major	Service Level - Minor
wwan	—	Bearer_Change Domain_State_Change Reg_State_Change SIM_State_Change	—

Notification Messages for Cisco vEdge Devices

The following table lists the notifications generated when an SNMP trap is generated.

Table 13:

Notification	Corresponding SNMP Trap
aaa-admin-pwd-change	AAA_Admin_Pwd_Change
access-list-association-status	Policy_Access_List_Association_Status
app-dpi-flows-out-of-memory	System_App_DPI_Flow_Out_Of_Memory
app-dpi-flows-write-failed-vedge	System_App_DPI_Flow_Write_Failed_vEdge
bearer-change	WWAN_Bearer_Change
bfd-state-change	BFD_State_Change
bgp-peer-state-change	BGP_Peer_State_Change
bridge-creation	Bridge_Creation
bridge-deletion	Bridge_Deletion
bridge-interface-state-change	Bridge_Interface_State_Change
bridge-max-mac-reached	Bridge_Max_MAC_Reached
cloudexpress-application-change	VPN_CloudExpress_Application_Change
cloudexpress-max-local-exit-exceeded	VPN_CloudExpress_Max_Local_Exit_Exceeded
cloudexpress-score-change	VPN_CloudExpress_Score_Change
control-connection-auth-fail	Control_Connection_Auth_Fail
control-connection-state-change	Control_Connection_State_Change
control-connection-tloc-ip-change	COntrol_Connection_TLOC_IP_Change
control-no-active-vbond	Control_No_Active_vBond
control-no-active-vsmart	Control_No_Active_vSmart

Notification	Corresponding SNMP Trap
control-vbond-state-change	Control_vBond_State_Change
control-vedge-list-request	Control_vEdge_List_Request
cpu-usage	CPU_Usage
data-policy-association-status	Policy_Data_Policy_Association_Status
device-template-attached-during-ztp	Security_Device_Template_Attached_During_ZTP
device-template-missing	Security_Device_Template_Missing
dhcp-address-assigned	DHCP_Address_Assigned
dhcp-address-released	DHCP_Address_Released
dhcp-address-renewed	DHCP_Address_Renewed
dhcp-request-rejected	DHCP_Request_Rejected
dhcp-server-state-change	DHCP_Server_State_Change
disk-usage	Disk_Usage (Disk usage on the device exceeds the predefined threshold of 60%)
domain-id-change	Domain_ID_Change
domain-state-change	WWAN_ Domain_State_Change
emmc-fault	HW_EMMC_Fault
fan-fault	HW_Fan_Fault
fantray-fault	HW_FanTray_Fault
fib-update	VPN_FIB_Update
flash-fault	HW_Flash_Fault
interface-admin-state-change	Interface_Admin_State_Change
interface-bw	VPN_If_BW_Update
interface-pcs-fault-detected	Interface_PCS_Fault_Detected
interface-state-change	Interface_State_Change
memory-usage	Memory_Usage
omp-data-policy	Data_Policy
omp-number-of-vsmarts-change	OMP_Number_of_vSmarts_Change
omp-peer-state-change	OMP_Peer_State_Change

Notification	Corresponding SNMP Trap
omp-policy	OMP_Policy
omp-state-change	OMP_State_Change
omp-tloc-state-change	OMP_TLOC_State_Change
org-name-change	Org_Name_Change
ospf-interface-state-change	OSPF_Interface_State_Change
ospf-neighbor-state-change	OSPF_Neighbor_State_Change
pem-fault	HW_PEM_Fault
pem-state-change	PEM_State_Change
pim-fault	HW_PIM_Fault
pim-interface-state-change	PIM_Interface_State_Change
pim-neighbor-state-change	PIM_Neighbor_State_Change
pim-state-change	HW_PIM_State_Change
pim-tunnel-change	PIM_Tunnel_Change
pim-tunnel-state-change	PIM_Tunnel_State_Change
process-down	Process_Down
process-restart	Process_Restart
pseudo-commit-status	System_Pseudo_Commit_Status
reg-state-change	WWAN_Reg_State_Change
route-install-fail	Route_Install_Fail
sd-card-fault	HW_SDCard_Fault
security-certificate-expired	Security_Certificate_Expired
security-certificate-installed	Security_Certificate_Installed
security-clear-installed-certificate	Security_Clear_Installed_Certificate
security-new-csr-generated	Security_New_CSR_Generated
security-root-cert-chain-installed	Security_Root_Cert_Chain_Installed
security-root-cert-chain-uninstalled	Security_Root_Cert_Chain_Uninstalled
security-vedge-entry-added	Security_vEdge_Entry_Added
security-vedge-entry-removed	Security_vEdge_Entry_Removed

Notification	Corresponding SNMP Trap
security-vedge-serial-file-uploaded	Security_vEdge_Serial_File_Uploaded
security-vsmart-serial-file-uploaded	Security_vSmart_Serial_File_Uploaded
service-gre-state-update	Security_Service_GRE_State_Update
sfp-state-change	SFP_State_Change
sfp-support-state	SFP_Support_State
sim-state-change	WWAN_SIM_State_Change
site-id-change	Site_ID_Change
sla-change	SLA_Change
sla-violation	Policy_SLA_Violation
sla-violation-pkt-drop	Policy_SLA_Violation_Pkt_Drop
system-aaa-login-fail	System_AAA_Login_Fail
system-commit	System_Commit
system-ip-change	System_IP_Change
system-login-change	System_Login_Change
system-logout-change	System_Logout_Change
system-reboot-aborted	System_Reboot_Aborted
system-reboot-complete	System_Reboot_Complete
system-reboot-issued	Reboot_Issued
system-software-install-status	Software_Install_Status
tempsensor-fault	HW_TempSensor_Fault
tempsensor-state	HQ_TempSensor_State
tunnel-install-fail	Tunnel_Install_Fail
tunnel-ipsec-manual-rekey	Tunnel_IPSec_Manual_Rekey
tunnel-ipsec-rekey	Tunnel_IPSec_Rekey
usb-state-change	USB_State_Change
vbond-reject-vedge-connection	Security_Reject_vEdge_Connection
vmanage-connection-preference-changed	Security_vManage_Connection_Preference_Changed
vrrp-group-state-change	VRRP_Group_State_Change

Supported SNMP MIBs

Table 14: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN MIBs	Cisco IOS XE Release 17.6.1a Cisco vManage Release 20.6.1	The following Cisco SD-WAN MIBs are introduced on Cisco IOS XE SD-WAN devices: CISCO-SDWAN-APP-ROUTE-MIB.my CISCO-SDWAN-BFD-MIB.my CISCO-SDWAN-OPER-SYSTEM-MIB.my CISCO-SDWAN-POLICY-MIB.my CISCO-SDWAN-SECURITY-MIB.my

Cisco IOS XE SD-WAN Devices

You can download the MIBs supported on Cisco IOS XE SD-WAN devices from ftp://ftp.cisco.com/pub/mibs/v2/

Note For the CISCO-SDWAN-POLICY-MIB.my MIB, the Object Identifier (OID) value cannot exceed 128 sub-identifiers, as defined in RFC 2578. When the OID limit exceeds 128 sub-identifiers, we recommend you to use the **Real-Time Monitoring - Policy** Netconf or REST API on Cisco IOS XE SD-WAN devices as alternative APIs for monitoring and troubleshooting.

Cisco vEdge Devices

For supported Cisco vEdge MIBs, see ftp://ftp.cisco.com/pub/mibs/viptela-mibs.

For information about downloading these MIB files, see the Release Notes for your software release.