# SNMP Configuration

# Support for SNMP Traps on Cisco Catalyst SD-WAN Devices

*Table 1: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for Cisco Catalyst SD-WAN Traps | Cisco IOS XE Catalyst SD-WAN Release 17.6.1a<br>Cisco vManage Release 20.6.1<br>Cisco SD-WAN Release 20.6.1 | This feature supports the receipt of the following SNMP trap notifications:<br>• Enterprise certificate expiration notifications on Cisco IOS XE Catalyst SD-WAN devices, Cisco vEdge devices, Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controller, and Cisco SD-WAN Manager.<br>• Health-monitoring notifications on Cisco vEdge devices, and Controllers, Cisco Catalyst SD-WAN Validator, Cisco Catalyst SD-WAN Controller, and Cisco SD-WAN Manager. |
| Application Route SNMP Trap | Cisco IOS XE Catalyst SD-WAN Release 17.11.1a<br>Cisco vManage Release 20.11.1 | Any change in the SLA class triggers the **AppRouteSlaChange** SNMP trap for Cisco IOS XE Catalyst SD-WAN devices. |

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

**Note** The CPU usage spikes up during SNMP queries.

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

- Enterprise certificate expiration notifications for Cisco IOS XE Catalyst SD-WAN devices, Cisco vEdge devices, and controllers: 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 expiration.

  Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the SNMP agents send alert notifications for certificate expiration as follows:

  - First notification interval: Certificate expiration between 6 months and 1 year from the current date.

Interval: Monthly

- Second notification interval: Certificate expiration date between 60 to 180 days from the current date.

  Interval: Weekly

  Type: Major

- Third notification interval: Certificate expiration date between 30 and 60 days from the current date.

  Interval: Weekly

  Type: Critical

- Fourth notification: Certificate expiration date 7 to 30 days away from the current date.

  Interval: Every day

  Type: Critical

- Fifth notification: Certificate expiration date is less than a week away.

  Interval: Every 12 hours

  Type: Critical

- Expired notification: Certificate has expired.

  Interval: Immediate

  Type: Critical

In releases earlier than Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, The SNMP agent sends traps or notifications for certificate expiration in the following intervals as follows:

- 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 Catalyst 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 a Configuration Group

### Before you begin

On the **Configuration** > **Configuration Groups** page, choose **SD-WAN** as the solution type.

### Procedure

**Step 1** From the Cisco SD-WAN Manager menu, choose **Configuration** > **Configuration Groups**.

**Step 2** Create and configure a SNMP feature in a System profile.

**a.** Configure Basic settings.

*Table 2: SNMP Version*

| Field | Description |
|---|---|
| **SNMP Version** | Choose one of the following SNMP versions:<br>• **SNMP v2**<br>• **SNMP v3** |
| **SNMP v2: Add View** | |
| **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. |
| **Add OID** | Click this option to add object identifiers (OID) and configure the following parameters:<br>• **Id***: 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 Cisco Catalyst SD-WAN 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.<br>• **Exclude**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view. |
| **SNMP v2: Add Community** | |
| **Name*** | Enter a name for the community. The name can be from 1 through 32 characters and can include angle brackets (< and >). |

| Field | Description |
|---|---|
| **User Label*** | (Minimum release: Cisco vManage Release 20.9.2) Enter a label or identifier for the community name. It helps you distinguish or update a community name when there are multiple community names for an SNMP target. |
| **View*** | Choose a view to apply to the community. The view specifies the portion of the MIB tree that the community can access. |
| **Authorization*** | Choose **read-only** from the drop-down list. The MIBs supported by Cisco Catalyst SD-WAN do not allow write operations, so you can configure only read-only authorization. |
| **SNMP v2: Add Target** | |
| **VPN ID*** | Enter the number of the VPN to use to reach the trap server.<br>Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here. |
| **IPv4/IPv6 address of SNMP server*** | Enter the IP address of the SNMP server. |
| **UDP port number to connect to SNMP server*** | Enter the UDP port number for connecting to the SNMP server.<br>Range: 1 though 65535 |
| **Community Name*** | Choose the name of a community that was configured under **Add Community**.<br>This field is applicable only to Cisco vManage Release 20.9.1 and earlier releases. |
| **User Label*** | (Minimum release: Cisco vManage Release 20.9.2) Choose a user label that was configured under **Add Community**. |
| **Source interface for outgoing SNMP trap*** | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |
| **SNMP v3: Add View** | |
| **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. |
| **Add OID** | Click this option to add object identifiers (OID) and configure the following parameters:<br>• **Id***: 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 Cisco Catalyst SD-WAN 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.<br>• **Exclude**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view. |
| **SNMP v3: Add Group** | |

| Field | Description |
|---|---|
| **Name*** | Enter a name for the trap group. It can be from 1 to 32 characters long. |
| **Security Level*** | Choose the authentication to use for the group.<br>• **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials.<br>**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.<br>**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 and a privacy and privacy password. |
| **View*** | Choose an SNMP view that the trap group can access. |
| **SNMP v3: Add User** | |
| **Name*** | Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters. |
| **Authentication Protocol** | Choose the authentication mechanism for the user:<br>• **md5**<br>• **sha** |
| **Authentication Password** | Enter the authentication password either in cleartext or as an AES-encrypted key. |
| **Privacy Protocol** | Choose the privacy type for the user.<br>• **aes-cfb-128**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. This is a SHA-1 authentication protocol.<br>• **aes-256-cfb-258**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 256-bit key. This is a SHA-256 authentication protocol.<br>Starting from Cisco Catalyst SD-WAN Manager Release 20.15.4, only **aes-256-cfb-258** is supported. |
| **Privacy Password** | Enter the privacy password either in cleartext or as an AES-encrypted key. |
| **Group*** | Choose the name of an SNMPv3 group. |
| **SNMP v3: Add Target** | |
| **VPN ID*** | Enter the number of the VPN to use to reach the trap server.<br>Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here. |

| Field | Description |
|---|---|
| **IPv4/IPv6 address of SNMP server*** | Enter the IP address of the SNMP server. |
| **UDP port number to connect to SNMP server*** | Enter the UDP port number for connecting to the SNMP server.<br>Range: 1 though 65535 |
| **User*** | Choose the name of a user that was configured under **Add User**. |
| **Source interface for outgoing SNMP trap*** | Enter the interface to use to send traps to the SNMP server that is receiving the trap information. |

**b.** Configure Advanced settings.

***Table 3: Advanced Settings***

| Field | Description |
|---|---|
| **Shutdown** | By default, SNMP is enabled. |
| **Contact Person** | Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN 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. |

### What to do next

Also see Deploy a configuration group.

# Configure SNMP using Cisco SD-WAN Manager

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

**Note** If your Network Management Stations (NMS) are reachable using a Cisco IOS XE Catalyst 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 Catalyst 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 SD-WAN Manager menu, choose **Configuration** > **Templates**.
2. Click **Device Templates**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

3. From the **Create Template** drop-down, select **From Feature Template**.
4. From the **Device Model** drop-down, select the type of device for which you are creating the template.
5. Click **Additional Templates**, which scrolls the page to **Additional Templates** section.
6. From the **Cisco 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.
7. 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.

8. 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.
9. 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 4: Changing the Scope for a Parameter Value***

| 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 Catalyst SD-WAN device or a Cisco vEdge device to a device template.<br>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 Catalyst SD-WAN device or a Cisco vEdge device to a device template.<br>To change the default key, type a new string and move the cursor out of the Enter Key box.<br>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.<br>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.

**Note** You are required to recreate the SNMP feature templates as the templates created prior to Cisco vManage Release 20.5 fails when attached to the device.

To attach the SNMP feature template:

1. In **Device Templates**, 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**.

### Configure Basic SNMP

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

*Table 5: Basic SNMP Parameters*

| Parameter Name | Description |
|---|---|
| Shutdown | Click **No** to enable SNMP. By default, SNMP is disabled. |
| Contact Person | Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst 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**.

# Configure SNMPv2 on Cisco vEdge Device Using Cisco SD-WAN Manager

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 6: SNMPv2 View Parameters*

| 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. |

| Parameter Name | Description |
|---|---|
| Object Identifiers | Click **Add Object Identifiers** and configure the following parameters:<br>• 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.<br>• On/Odd—Click Off to include the OID in the view or click On to exclude the OID from the view.<br>To save the object identifiers, click **Save**.<br>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 7: SNMPv2 Community Parameters***

| 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 Catalyst 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.

***Table 8: Trap Group Parameters***

| 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:<br>In **Severity Levels**, select one or more severity levels for the trap—critical, major, or minor.<br>In **Module Name**, select the type of traps to include in the trap group:<br>• all: All trap types.<br>• app-route: Traps generated by application-aware routing.<br>• bfd: Traps generated by BFD and BFD sessions.<br>• control: Traps generated by DTLS and TLS sessions.<br>• dhcp: Traps generated by DHCP.<br>• hardware: Traps generated by Viptela hardware.<br>• omp: Traps generated by OMP.<br>• routing: Traps generated by BGP, OSPF, and PIM.<br>• security: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec.<br>• system: Traps generated by system-wide functions.<br>• 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.

***Table 9: Trap Target Server Parameters***

| 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. |
| 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**.

# Configure SNMPv3 on Cisco vEdge Devices Using Cisco SD-WAN Manager

*Table 10: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for SNMPv3 AES-256 bit Authentication Protocol | Cisco vManage Release 20.5.1<br>Cisco SD-WAN Release 20.5.1 | This feature allows you to configure SNMPv3 users in support with SHA-256 authentication protocol and AES-256 bit encryption on Cisco vEdge devices. |

To configure SNMPv3, in SNMP Version, navigate to template page and configure groups and trap information:

- From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.
- Click **Device Templates**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**

- From the **Create Template** drop-down, select **From Feature Template**.
- From the **Device Model** drop-down, select the type of device for which you are creating the template.
- Click **Additional Templates**, which scrolls the page to **Additional Templates** section.
- 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.
- 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.
- 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.
- In **SNMP Version** section, click **V3**. For SNMPv3, you can configure groups, users, and trap information.
- In the Trap section, select **Trap Group** to configure trap. Then click **Add New Trap Group**, and configure the parameters as listed below:

*Table 11: Trap Group Parameters for Cisco vEdge Devices*

| Parameter Name | Description |
|---|---|
| Group Name | Enter a name for the trap group. It can be from 1–32 characters long. |
| Trap Type Modules | Click **Add Trap Type Modules**, and configure the following parameters:<br>In **Severity Levels**, select one or more severity levels for the trap. Supported security levels for the trap are critical, major, and minor.<br>In **Module Name**, choose the type of traps to include in the trap group:<br>• all: All trap types.<br>• app-route: Traps generated by application-aware routing.<br>• bfd: Traps generated by BFD and BFD sessions.<br>• control: Traps generated by DTLS and TLS sessions.<br>• dhcp: Traps generated by DHCP.<br>• hardware: Traps generated by Viptela hardware.<br>• omp: Traps generated by OMP.<br>• routing: Traps generated by BGP, OSPF, and PIM.<br>• security: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec.<br>• system: Traps generated by system-wide functions.<br>• vpn: Traps generated by VPN-specific functions, including interfaces and VRRP. |

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

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

*Table 12: View and Groups Parameters*

| 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 group. |

| Parameter Name | Description |
|---|---|
| Object Identifiers (OID) | Click **Add Object Identifiers** and configure the following parameters:<br>• Object Identifier: 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 Cisco Catalyst SD-WAN 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.<br>**Note**<br>Starting from Cisco vManage Release 20.6.1, SNMPv3 configuration of user with auth "sha-256" and priv "aes-256-cfb-128" does not support oid with (*) wildcard.<br>• Exclude OID: Click **Off** to include the OID in the view or click **On** to exclude the OID from the view.<br>To remove an OID from the list, click the **Delete** icon for the entry.<br>To add the OIDs to the view list, click **Add**. |

To configure the SNMP group, click **New Group**, and configure the following parameters:

**Note** It's mandatory to create an SNMP view before you proceed with SNMP group configuration.

***Table 13: SNMP Group Parameters for Cisco vEdge Devices***

| Parameter Name | Description |
|---|---|
| Name | Enter the name for the group. The name can be from 1 through 32 characters and can include angle brackets (< and >). |
| Security Level | Choose the **Security Level** from the drop-down for the SNMPv3 security model:<br>SNMPv3 is a security model in which an authentication strategy for a user and the group in which the user resides are set up. A security level is the permitted level of security within a security model.<br>• noAuthNoPriv: Uses a username match for authentication.<br>• authNoPriv: Provides authentication based on the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) algorithms.<br>• authPriv: Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. |
| View | Choose the view from the drop-down to apply to the group. The view specifies the portion of the MIB tree the group can access. |

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

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

*Table 14: SNMPv3 User Parameters*

| Parameter Name | Description |
|---|---|
| User | Enter a name of the SNMP user. It can be 1–32 alphanumeric characters. |
| Authentication Protocol | Choose the authentication mechanism for the user:<br>• MD5 digest.<br>• SHA-1 message digest.<br>• SHA-256 message digest.<br>**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`.<br>**Note** MD5 authentication protocol is deprecated for Cisco Catalyst SD-WAN Release 20.3.2 and later releases.<br>**Note** From Cisco Catalyst SD-WAN Release 20.11.1, if you choose MD5 authentication, the console logs include a warning that MD5 has been deprecated. |
| Authentication Password | If you have the localized MD5 or SHA digest, you can specify the respective string as password. The digest is in the format aa:bb:cc:dd where aa, bb, cc, and dd are hexadecimal values. Also, the digest should be exactly 16 octets in length. |
| Privacy Protocol | Choose the privacy type for the user:<br>• For SHA-1 authentication protocol choose AES-CFB-128—Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 128-bit key.<br>• In Cisco SD-WAN Release 20.5.1, for SHA-256 authentication protocol choose AES-256-CFB-128—Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 256-bit key.<br>**Note** An authentication protocol SHA-1 is no longer supported and when a trap target is configured with SHA-1 for an SNMPv3 user, no SNMP trap is generated. You need to configure an SNMPv3 user with the SHA-256 authentication protocol. |
| Privacy Password | Enter the authentication password either in cleartext or as an AES-encrypted key. |
| Group | Choose the group name from the drop-down. All the configured SNMPv3 group names are listed in the drop-down. |

**Note** In Cisco vManage Release 20.6.x, if the SNMP user is configured with Auth-SHA-256 and Priv-AES-256, use a special port 1161 for SNMP queries.

**Note** Starting from Cisco SD-WAN Release 20.9.x, you cannot configure SNMP v3 users with the SHA authentication protocol and AES-CFB-128 privacy protocol. However, for existing users who upgrade, SNMP queries will be supported, but SNMP traps will not be supported.

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

**Note** It's mandatory to create User before creating Trap Target Server.

***Table 15: Trap Target Server Parameters***

| Parameter Name | Description |
|---|---|
| VPN ID | Enter the number of the VPN to use to reach the trap server. *Range:* 0–65530. |
| 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. |
| User Name | Choose the name of the user from the drop-down. |
| Source Interface | Enter the interface used to send traps to the remote SNMP server. |

To add the Trap Target Server, click **Add**.

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

**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 isn't 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.

# Configure SNMPv2 on Cisco IOS XE Catalyst SD-WAN Devices Using Cisco SD-WAN Manager

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 16: SNMPv2 View Parameters***

| 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:<br>• 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.<br>• On/Odd—Click Off to include the OID in the view or click On to exclude the OID from the view.<br>To save the object identifiers, click **Save**.<br>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 17: SNMPv2 Community Parameters***

| 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 Catalyst 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 target servers, in the Trap section, select **Trap Target Server**. Then click **New Trap Target**, and configure the parameters below.

**Note** On a Cisco IOS XE Catalyst SD-WAN device, however, the last occurrence of the source interface is chosen as the global source interface.

*Table 18: Trap Target Server Parameters*

| Parameter Name | Description |
|---|---|
| VPN ID | Enter the number of the VPN to use to reach the trap server.<br>Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here. |
| 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 |
| Community Name | Select the name of a community that was configured under Community. |
| 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**.

# Configure SNMPv3 on Cisco IOS XE Catalyst SD-WAN Devices Using Cisco SD-WAN Manager

*Table 19: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Support for SNMPv3 AES-128 and AES-256 bit Encryption Protocol | Cisco vManage Release 20.7.1<br>Cisco IOS XE Catalyst SD-WAN Release 17.7.1a | This feature allows you to configure SNMPv3 users with SHA-1 authentication protocol and AES-128 and AES-256 encryption on Cisco IOS XE Catalyst SD-WAN devices. |

To configure SNMPv3, in **SNMP Version**, navigate to **Template** page and configure groups and trap information:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Templates**.

2. Click **Device Templates**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose the type of device for which you are creating the template.
5. Click **Additional Templates**. This takes you to the **Additional Templates** section.
6. From the **Cisco SNMP** drop-down list, choose **Create Template**.

   The SNMP template form containing fields for naming the template and for defining SNMP parameters is displayed.
7. 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.
8. 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.
9. In **SNMP Version** section, click **V3**. For SNMPv3, you can configure groups and trap information.
10. In the **View & Groups** section, click **View**, choose **New View**, and configure the following fields:

***Table 20: View and Groups Parameters for Cisco IOS XE Catalyst SD-WAN Devices***

| Field 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 the views before adding a group. |
| **Object Identifiers (OID)** | Click **Add Object Identifiers** and configure the following parameters:<br>• Object Identifier: Enter the OID of the object. For example, to view the internet part of the SNMP MIB, enter the OID 1.3.6.1. To view the private part of the Cisco Catalyst SD-WAN MIB, enter the OID 1.3.6.1.4.1.9. 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.<br>• Exclude OID: Click **Off** to include the OID in the view or click **On** to exclude the OID from the view.<br>To remove an OID from the list, click **Delete** adjacent to the corresponding entry.<br>To add an OID to the view list, click **Add**. |

11. Click **Add**.

Click **Group**, choose **New Group**, and configure the following parameters.

**Note** It's mandatory to create an SNMP view before you proceed with SNMP group configuration.

*Table 21: Group Parameters*

| Field Name | Description |
|---|---|
| **Name** | Enter the name for the group. The name can be from 1 through 32 characters and can include angle brackets (< >). |
| **Security Level** | Choose the security level from the drop-down for the SNMPv3 security model:<br>SNMPv3 is a security model in which an authentication strategy for a user and the group in which the user resides are set up. A security level is the permitted level of security within a security model.<br>• noAuthNoPriv: Uses a username match for authentication.<br>• authNoPriv: Provides authentication based on the Message Digest 5 (MD5) or Secure Hash Algorithm (SHA) algorithms.<br>• authPriv: Provides authentication based on the HMAC-MD5 or HMAC-SHA algorithms. Provides DES 56-bit encryption in addition to authentication based on the CBC-DES (DES-56) standard. |
| **View** | Choose the view from the drop-down list to apply to the group. The view specifies the portion of the MIB tree that the group can access. |

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

To configure SNMPv3 users, in the **User** section, click **New User**, and provide information in the following fields. Note that it's mandatory to create an SNMP group before you proceed with SNMP user configuration.

*Table 22: SNMPv3 Users Parameters*

| Field Name | Description |
|---|---|
| **User** | Enter a unique name for the user. It can be 1 to 32 alphanumeric characters. |
| **Authentication Protocol** | Choose the authentication mechanism for the user:<br>• SHA-1 message digest.<br>• MD5 digest.<br>**Note**<br>Support for MD5 authentication protocol will be deprecated shortly.<br>**Note**<br>From Cisco IOS XE Catalyst SD-WAN Release 17.11.1a, if you choose MD5 authentication, the console logs include a warning that MD5 has been deprecated. |

| Field Name | Description |
|---|---|
| **Authentication Password** | If you have the localized MD5 or SHA digest, you can specify the respective string as password. The digest is in the format *aa:bb:cc:dd* where *aa*, *bb*, *cc*, and *dd* are hexadecimal values. Also, the digest should be exactly 16 octets in length. |
| **Privacy Protocol** | Choose the privacy type for the SHA-1 authentication protocol user:<br>AES-CFB-128: Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 128-bit key.<br>AES-256-CFB-128: Advanced Encryption Standard cipher algorithm is used in cipher feedback mode, with a 256-bit key. |
| **Privacy Password** | Enter the privacy password either in cleartext or as an AES-encrypted key. |
| **Group** | Choose the group name from the drop-down list. Configured SNMPv3 group names are displayed in the drop-down list. |

**Note** The SNMP authentication password supports all the special characters except exclamation (!) character. If you want to use the exclamation (!) in your password, you must use that password in double quotes. For example, "password!".

To add an SNMP user, click **Add**.

(Optional) To configure the Trap Target server, in the **Trap** section, click **New Trap Target**, and enter information in the following fields. Note that it's mandatory to create an SNMP user before you proceed with trap target server configuration.

***Table 23: Trap Target Server Parameters***

| Field Name | Description |
|---|---|
| **VPN ID** | Enter the number of the VPN to use to reach the trap server.<br>Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here. |
| **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 to 65535. |
| **User Name** | Choose the name of the configured user from the drop-down list. |
| **Source Interface** | Enter the interface used to send traps to the remote SNMP server. |

To add the Trap Target server, click **Add**.

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

**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 isn't removed during the configuration change. Hence, you can't 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.

# Configure SNMP with Encrypted Strings Using CLI Templates

*Table 24: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| Configure SNMP with Encrypted Strings Using CLI Templates | Cisco IOS XE Catalyst SD-WAN Release 17.5.1a<br>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 Catalyst 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 Templates**, and then click **Add Template**.

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Feature Templates** is titled as **Feature**.

     b. Under the Select Devices pane, select the Cisco IOS XE Catalyst SD-WAN device devices for which you are creating the template.
     c. Under the Select Template pane, scroll down to the Other Templates section.
     d. Click **CLI Add-On Template**.

- CLI templates

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

**Note** In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

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

  c. Under the Select Devices pane, select the Cisco IOS XE Catalyst 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 Catalyst 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 Catalyst 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 v3 {auth |noauth |priv}[read readview][write
 writeview
][notify notifyview][access [access-list-number | access-name][ipv6 named-access-list]
```

2. Configure a new user to an SNMPv3 group:

```
Device(config)# snmp-server user username group-name [remote ip-address[udp-port port][vrf
 vrf-name]]
v3 [encrypted][auth {md5|sha} auth-password][access [ipv6 nacl][priv {des|3des|aes|aes
{128|256}}privpassword]{acl-number|acl-name}]
```

**Note** For security reasons, the user command is not listed in the possible completions of the command line help. However, you can still use the user command when configuring a new user for an SNMPv3 group.

### 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 the possible traps (omp, policy, security, system) for Cisco Catalyst SD-WAN notification:

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

2. Enable SNMP notifications for rising alarm changes:

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

3. Enable SNMP notifications for configuration changes:

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

4. Send entity MIB notifications to a host:

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

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

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

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

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

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

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

11. Enable SNMP configuration copy notifications:

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

12. Enable SNMP configuration CTID notifications:

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

13. Enable SNMP Embedded Event Manager notifications:

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

14. Enable CPU thresholding violation notifications:

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

15. Enable Flash device insertion and removal SNMP notifications:

```
Device# config-transaction
Device(config)# snmp-server enable traps flash [insertion][removal]
```

16. Enable a device to send SNMP notifications when memory pool buffer usage reaches a new peak:

```
Device# config-transaction
Device(config)# snmp-server enable traps memory [bufferpeak]
```

17. Enable a device to send system logging message notifications:

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

### 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 SD-WAN Manager, 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 Catalyst 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: 80000009030000C88B487400
storage-type: nonvolatile active
Authentication Protocol: SHA
Privacy Protocol: AES128
Group-name: groupAuthPriv

User name: v3userNoAuthNoPriv
Engine ID: 80000009030000C88B487400
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 Catalyst 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:

```
Device(config)# snmp group group-name authentication
Device(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).

  From Cisco Catalyst SD-WAN Manager Release 20.12.1, the authentication method **auth-no-priv** is not supported.

- **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 Catalyst 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 Catalyst SD-WAN software. For a list of enterprise MIBs, see Supported SNMP MIBs. The MIBs supported by the Cisco Catalyst 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 Catalyst 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 Catalyst 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 Catalyst 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 25: SNMP Traps for Cisco IOS XE Catalyst SD-WAN Devices***

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **app-route** | Major | AppRouteSlaChange | A change in the SLA class for a tunnel generates this SNMP trap. |
| **control** | Major | ciscoSdwanSecurityControlConnectionStateChange | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device control connections state is changed. For example, when the Cisco Catalyst SD-WAN router connections are established. |
| **BFD** | Major | ciscoSdwanBfdStateChange | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device BFD session state is changed.<br>The BFD traps are supported from Cisco IOS XE Release 17.8.1a. |
| **omp** | Major | ciscoSdwanOmpOmpNumberOfVsmartsChange | SNMP trap is generated when the number of Cisco SD-WAN Controllers is changed. |
| | | ciscoSdwanOmpOmpPeerStateChange | SNMP trap is generated when the peer state is changed. |
| | | ciscoSdwanOmpOmpStateChange | SNMP trap is generated when the OMP system operational state is changed. |
| | | ciscoSdwanOmpOmpPolicy | SNMP trap is generated when a forwarding policy is received from Cisco SD-WAN Controller (on Cisco IOS XE SD-WAN device only). |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **policy** | Major | ciscoSdwanPolicyAccessListAssociationStatus | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device access policy is configured from Cisco SD-WAN Manager. |
| | | ciscoSdwanPolicyDataPolicyAssociationStatus | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device data policy is configured from Cisco SD-WAN Manager. |
| | | ciscoSdwanPolicySlaViolationPktDrop | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device SLA policy is violated due to packet drop. |
| | Minor | ciscoSdwanPolicySlaViolation | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device SLA policy is violated. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **security** | Major | ciscoSdwanSecuritySecurityCertificateExpired | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device certificate is expired. |
| | | ciscoSdwanSecuritySecurityCertificateExpiring | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device certificate is about to expire (expiring) starting from 60 days before the expiration of the certificate. |
| | | ciscoSdwanSecuritySecurityRootCertChainUninstalled | SNMP trap is generated after successfully uninstalling root certificate. |
| | | ciscoSdwanSecuritySecurityClearInstalledCertificate | SNMP trap is generated when the Cisco Catalyst SD-WAN root certificate is uninstalled on Cisco IOS XE Catalyst SD-WAN device.<br>For information on certificate expiry, see Support for SNMP Traps on Cisco Catalyst SD-WAN Devices. |
| | | ciscoSdwanSecuritySecurityVsmartEntryAdded | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device is added to Cisco SD-WAN Controller. |
| | Minor | ciscoSdwanSecuritySecurityRootCertChainInstalled | SNMP trap is generated when the root certificate is installed. |
| | | ciscoSdwanSecuritySecurityCertificateInstalled | SNMP trap is generated when the security certificate is installed. |
| | | ciscoSdwanSecuritySecurityNewCsrGenerated | SNMP trap is generated when a new certificate sign request is generated. |
| | | ciscoSdwanSecurityTunnelIpsecRekey | SNMP trap is generated when the tunnel IPSec is rekeyed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **system** | Major | ciscoSdwanSystemPseudoCommitStatus | SNMP trap is generated when the Cisco SD-WAN Manager pushes a tentative configuration (pseudo commit) to the Cisco IOS XE Catalyst SD-WAN device. |
| | Minor | ciscoSdwanSystemDomainIdChange | SNMP trap is generated when the Cisco Catalyst SD-WAN domain ID is changed on the Cisco IOS XE Catalyst SD-WAN device. |
| | | ciscoSdwanSystemOrgNameChange | SNMP trap is generated when the Cisco Catalyst SD-WAN organization name is changed on the Cisco IOS XE Catalyst SD-WAN device. |
| | | ciscoSdwanSystemSiteIdChange | SNMP trap is generated when the Cisco Catalyst SD-WAN site ID is changed on the Cisco IOS XE Catalyst SD-WAN device. |
| | | ciscoSdwanSystemSystemCommit | SNMP trap is generated when the configurations on the Cisco IOS XE Catalyst SD-WAN device is changed and commited. |
| | | ciscoSdwanSystemSystemIpChange | SNMP trap is generated when the Cisco IOS XE Catalyst SD-WAN device system IP is changed. |

*Table 26: SNMP Traps for Cisco vEdge Devices*

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **all** | — | All critical traps are listed in the following cells in this table. | — |
| **app-route** | Major | viptelaAppRouteSlaChange | SNMP trap is generated when the SLA class(es) for a tunnel is changed. |
| **bfd** | Major | viptelaBfdBfdStateChange | SNMP trap is generated when a BFD session state is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **bridge** | Minor | viptelaBridgeCreation | SNMP trap is generated when a bridge is created via CLI. |
| | | viptelaBridgeDeletion | SNMP trap is generated when a bridge is deleted via CLI. |
| | | viptelaBridgeMaxMacReached | SNMP trap is generated when the threshold exceeds for DOT1X STA MACs. |
| **control** | Critical | viptelaSecurityControlNoActiveVbond | SNMP trap is generated when the DTLS peering with the Cisco SD-WAN Validator is removed. |
| | Major | viptelaSecurityControlConnectionAuthFail | SNMP trap is generated when the control connection authentication is failed. |
| | | viptelaSecurityControlConnectionStateChange | SNMP trap is generated when the peer is marked as up or down and the control connections state is changed. |
| | | viptelaSecurityControlConnectionTlocIpChange | SNMP trap is generated when the control connection tloc IP is changed. |
| | | viptelaSecurityControlVbondStateChange | SNMP trap is generated when the Cisco SD-WAN Validator sends the SNMP trap to indicate the admin status. |
| **dhcp** | Major | viptelaVpnDhcpServerStateChange | SNMP trap is generated when the state of a DHCP server is changed. |
| | Minor | viptelaVpnDhcpAddressAssigned | SNMP trap is generated when the DHCP address is assigned. |
| | | viptelaVpnDhcpAddressReleased | SNMP trap is generated when the DHCP address is released. |
| | | viptelaVpnDhcpAddressRenewed | SNMP trap is generated when the DHCP address is renewed. |
| | | viptelaVpnDhcpRequestRejected | SNMP trap is generated when the client's request to DHCP server is rejected. |
| | | viptelaVpnDhcpServerStateChange | SNMP trap is generated when the DHCP server state is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **hardware** | Major | viptelaHardwareEmmcFault | SNMP trap is generated when the eMMC fault is detected or cleared. |
| | | viptelaHardwareFanFault | SNMP trap is generated when the fan fault is detected or cleared. |
| | | viptelaHardwareFantrayFault | SNMP trap is generated when the fan tray fault is detected or cleared. |
| | | viptelaHardwareFlashFault | SNMP trap is generated when the flash fault is detected or cleared. |
| | | viptelaHardwarePemFault | SNMP trap is generated when the PEM fault is detected or cleared. |
| | | viptelaHardwarePemStateChange | SNMP trap is generated when the PEM state is changed. |
| | | viptelaHardwarePimFault | SNMP trap is generated when the PIM power fault is detected or cleared. |
| | | viptelaHardwarePimStateChange | SNMP trap is generated when the PIM module state is changed. |
| | | viptelaHardwareSdcardFault | SNMP trap is generated when the SD card fault is detected or cleared. |
| | | viptelaHardwareSfpStateChange | SNMP trap is generated when the SFP state is changed. |
| | | viptelaHardwareSfpSupportState | SNMP trap is generated when the SFP support state is changed. |
| | | viptelaHardwareTempsensorFault | SNMP trap is generated when the temperature sensor fault is detected or cleared. |
| | | viptelaHardwareTempsensorState | SNMP trap is generated when the temperature sensor state is changed. |
| | | viptelaHardwareUsbStateChange | SNMP trap is generated when the USB state is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **omp** | Major | viptelaOmpOmpNumberOfVsmartsChange | SNMP trap is generated when the number of Cisco SD-WAN Controllers is changed. |
| | | viptelaOmpOmpPeerStateChange | SNMP trap is generated when the peer state is changed. |
| | | viptelaOmpOmpStateChange | SNMP trap is generated when the OMP system operational state is changed. |
| | | viptelaOmpOmpPolicy | SNMP trap is generated when a forwarding policy is received from Cisco SD-WAN Controller (on Cisco vEdge routers only). |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **policy** | Major | viptelaPolicyAccessListAssociationStatus | SNMP trap is generated for the status of access list association. |
| | | viptelaPolicyDataPolicyAssociationStatus | SNMP trap is generated for the status of data policy association. |
| | | viptelaPolicySlaViolationPktDrop | SNMP trap is generated when a SLA class violation with packet is dropped. |
| | | viptelaPolicySlaConfig | SNMP trap is generated when a SLA class is added or modified or deleted. |
| | | viptelaPolicyZbfFlowTableFull | SNMP trap is generated when a flow table is full. |
| | | viptelaPolicyZbfClearFlowTableFull | SNMP trap is generated when a flow table drops back to low threshold value. |
| | | viptelaPolicyZbfHalfOpenHit | SNMP trap is generated when the max half open TCP connections (SYN flood) is reached. |
| | | viptelaPolicyZbfClearHalfOpenHit | SNMP trap is generated when the number of half open TCP connections (SYN flood) drops back. |
| | | viptelaPolicyAppListAppAliasesNotify | SNMP trap is generated when a list of application aliases (corresponding NBAR applications) are added or modified. |
| | | viptelaPolicyAppListUnsupportedAppNotify | SNMP trap is generated when a list of unsupported applications (no corresponding NBAR application) are added or modified |
| | Minor | viptelaPolicySlaViolation | SNMP trap is generated when a SLA class is violated. |
| | | viptelaPolicyZbfFlowCreation | SNMP trap is generated when a flow is created matching a zone-pair. |
| | | viptelaPolicyZbfFlowDeletion | SNMP trap is generated when a flow pertaining to a zone-pair is deleted due to timeouts or when zone-pair gets deleted. |
| | | viptelaPolicyZbfPktLog | SNMP trap is generated when a ZBFW packet log is received. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **routing** | Major | viptelaVpnBgpPeerStateChange | SNMP trap is generated when the state of a BGP peer is changed. |
| | | viptelaVpnOspfInterfaceStateChange | SNMP trap is generated when the state of an OSPF interface is changed. |
| | | viptelaVpnOspfNeighborStateChange | SNMP trap is generated when the state of an OSPF neighbor is changed. |
| | | viptelaVpnPimInterfaceStateChange | SNMP trap is generated when the state of a PIM interface is changed. |
| | | viptelaVpnPimNeighborStateChange | SNMP trap is generated when the state of the PIM neighbor is changed. |
| | | viptelaVpnPimTunnelStateChange | SNMP trap is generated when the state of the tunnel of a PIM neighbor is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **security** | Major | viptelaSecuritySecurityCertificateExpired | SNMP trap is generated when the certificate is expired. |
| | | viptelaSecuritySecurityCertificateExpiring | SNMP trap is generated repeatedly from 60 days before the expiry of the certificate. |
| | | viptelaSecuritySecurityClearInstalledCertificate | SNMP trap is generated when all the certificates on a device, including the public and private keys and the root certificate, have been cleared, and the device has returned to the factory-default state. |
| | | viptelaSecuritySecurityRootCertChainUninstalled | SNMP trap is generated when the file containing the root certificate key chain is removed from a controller or a router. |
| | | viptelaSecuritySecurityVedgeEntryAdded | SNMP trap is generated on controllers when a new Cisco vEdge device entry is added via the csv or json file. |
| | | viptelaSecuritySecurityVedgeEntryRemoved | SNMP trap is generated on controllers when a Cisco vEdge device entry is deleted or removed via the csv or json file. |
| | | viptelaSecuritySecurityUnclaimedVedgeEntryAdded | SNMP trap is generated when an unclaimed Cisco vEdge device entry is added. |
| | | viptelaSecuritySecurityVedgeSerialFileUploaded | SNMP trap is generated when the WAN edge serial number file is uploaded to the Cisco SD-WAN Manager server. |
| | | viptelaSecurityVbondRejectVedgeConnection | SNMP trap is generated when a challenge ack is received on a controller and cannot be verified. |
| | | viptelaSecuritySecurityVsmartEntryAdded | SNMP trap is generated on all the devices when a new Cisco SD-WAN Controller serial num file is added. |
| | | viptelaSecuritySecurityVsmartEntryRemoved | SNMP trap is generated on all devices when a new Cisco SD-WAN Controller serial num file is removed or deleted. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| | | viptelaSecuritySecurityVsmartSerialFileUploaded | SNMP trap is generated when the Cisco SD-WAN Manager uploads the file containing certificate serial numbers for Cisco SD-WAN Controllers in the overlay network. |
| | | viptelaSecurityDeviceTemplateAttachedDuringZtp | SNMP trap is generated on a Cisco SD-WAN Manager, during the ZTP process, when the edge device has been registered with ZTP and the base template is pre-configured on a Cisco SD-WAN Manager. |
| | | viptelaSecurityDeviceTemplateMissing | SNMP trap is generated on a Cisco SD-WAN Manager, during ZTP process, when the edge device has been registered with ZTP and the base template is not pre-configured on a Cisco SD-WAN Manager. |
| | Minor | viptelaSecuritySecurityCertificateInstalled | SNMP trap is generated when a certificate is installed on the device. |
| | | viptelaSecuritySecurityNewCsrGenerated | SNMP trap is generated when a controller or router generates a signing request (CSR) certificate. |
| | | viptelaSecuritySecurityRootCertChainInstalled | SNMP trap is generated when the file containing the root certificate key chain is installed on a edge device. |
| | | viptelaSecurityTunnelIpsecManualRekey | SNMP trap is generated when a request security ipsec-rekey is performed on theCisco vEdge device. |
| | | viptelaSecurityTunnelIpsecRekey | SNMP trap is generated when the tunnel IPSec is re-keyed by timer. |
| | | viptelaSecurityVmanageConnectionPreferenceChanged | SNMP trap is generated on a device when the Cisco SD-WAN Manager-conn-preference on a tloc is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **system** | Critical | viptelaSystemCpuUsage | SNMP trap is generated when the system CPU usage goes above 90 percent. |
| | | viptelaSystemDiskUsage | SNMP trap is generated when the system disk usage goes above 90 percent. |
| | | viptelaSystemMemoryUsage | SNMP trap is geenrated when the system memory usage goes above 90 percent. |
| | Major | viptelaSystemAaaAdminPwdChange | SNMP trap is generated when the password for the AAA user admin is changed on a router or a controller. |
| | | viptelaSystemCpuUsage | SNMP trap is generated when the system CPU usage goes above 75 percent. |
| | | viptelaSystemDiskUsage | SNMP trap is generated when the system disk usage goes above 75 percent. |
| | | viptelaSystemMemoryUsage | SNMP trap is generated when the system memory usage goes above 75 percent. |
| | | viptelaSystemProcessRestart | SNMP trap is generated when a process (daemon) on a controller or a router is restarted. |
| | | viptelaSystemProcessDown | SNMP trap is generated when a process (daemon) on a device is exited. |
| | | viptelaSystemSystemAaaLoginFail | SNMP trap is generated when the AAA user SSH-based login fails. |
| | | viptelaSystemPseudoCommitStatus | SNMP trap is generation when the Cisco SD-WAN Manager pushes a tentative configuration (called the pseudo commit) to the device and starts the rollback timer. |
| | | viptelaActionsSystemRebootComplete | SNMP trap is generated when the device reboot procedure is completed. |
| | | viptelaActionsSystemRebootAborted | |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| | | | SNMP trap is generated when the device reboot is aborted. |
| | Minor | viptelaSystemCpuUsage | SNMP trap is generated when the system CPU usage -<br>• goes between 60 or 75 percent.<br>• goes below 60 percent. |
| | | viptelaSystemDiskUsage | SNMP trap is generated when the system disk usage -<br>• goes between 60 or 75 percent.<br>• goes below 60 percent. |
| | | viptelaSystemDomainIdChange | SNMP trap is generated when a domain identifier in the overlay network is changed. |
| | | viptelaSystemMemoryUsage | SNMP trap is generated when the system memory usage -<br>• goes between 60 or 75 percent.<br>• goes below 60 percent. |
| | | viptelaSystemOrgNameChange | SNMP trap is generated when the organization name used in the certificates for all overlay network devices is changed. |
| | | viptelaActionsSystemRebootIssued | SNMP trap is generated when a device is rebooted. |
| | | viptelaSystemSiteIdChange | SNMP trap is generated when a site identifier in the overlay network is changed. |
| | | viptelaActionsSystemSoftwareInstallStatus | SNMP trap is generated to notify the system software install status. |
| | | viptelaSystemSystemCommit | SNMP trap is generated when the user configuration is committed. |
| | | viptelaSystemSystemIpChange | SNMP trap is generated when the system IP address on a controller or a router is changed. |
| | | viptelaSystemSystemLoginChange | SNMP trap is generated when the system login for a user is changed. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| | | viptelaSystemSystemLogoutChange | SNMP trap is generated when a user logs out of the system. |
| **vpn** | Major | viptelaVpnInterfaceStateChange | SNMP trap is generated when the administrative or operational status of an interface is changed. |
| | | viptelaVpnVrrpGroupStateChange | SNMP trap is generated when the VRRP group state is changed. |
| | | viptelaVpnCloudExpressApplicationChange | SNMP trap is generated when the cloud express application best path is changed. |
| | | viptelaVpnCloudExpressMaxLocalExitExceeded | SNMP trap is generated when the maximum local exit of cloud express is exceeded (limit is 56). |
| | | viptelaVpnCloudExpressScoreChange | SNMP trap is generated when the cloud express application best path score is changed, but there is no change in the best path (score is calculated from latency or loss). |
| | | viptelaVpnInterfaceBw | SNMP trap is generated when the interface downstream bandwidth is updated. |
| | | viptelaVpnInterfacePcsFaultDetected | SNMP trap is generated when the interface PCS fault is detected or cleared. |
| | | viptelaVpnLastResortStateChange | SNMP trap is generated when a last resort state is changed. |
| | Minor | viptelaVpnRouteInstallFail | SNMP trap is generated when the route install fails. |
| | | viptelaVpnTunnelInstallFail | SNMP trap is generated when adding a tunnel to TLOC fails. |
| | | viptelaVpnFibStateChange | SNMP trap is generated when FIB is updated. |

| Trap Type | Severity Level - Critical/Major/Minor | Trap Name | Descriptions |
|---|---|---|---|
| **wwan** | Major | viptelaWwanBearerChange | SNMP trap is generated when the data bearer is changed. |
| | | viptelaWwanDomainStateChange | SNMP trap is generated when the domain state is changed. |
| | | viptelaWwanRegStateChange | SNMP trap is generated when the network registration is changed. |
| | | viptelaWwanSimStateChange | SNMP trap is generated when the SIM state is changed. |
| | | viptelaWwanQosStateChange | SNMP trap is generated when a QoS flow state is changed. |

### Notification Messages for Cisco vEdge Devices

***Table 27: Notifications for Cisco vEdge Devices***

| Notifications | Corresponding SNMP Trap |
|---|---|
| aaa-admin-pwd-change | viptelaSystemAaaAdminPwdChange |
| access-list-association-status | viptelaPolicyAccessListAssociationStatus |
| app-list-app-aliases-notify | viptelaPolicyAppListAppAliasesNotify |
| app-list-unsupported-app-notify | viptelaPolicyAppListUnsupportedAppNotify |
| bearer-change | viptelaWwanBearerChange |
| bfd-state-change | viptelaBfdBfdStateChange |
| bgp-peer-state-change | viptelaVpnBgpPeerStateChange |
| bridge-creation | viptelaBridgeCreation |
| bridge-deletion | viptelaBridgeDeletion |
| bridge-max-mac-reached | viptelaBridgeMaxMacReached |
| cloudexpress-application-change | viptelaVpnCloudExpressApplicationChange |
| cloudexpress-max-local-exit-exceeded | viptelaVpnCloudExpressMaxLocalExitExceeded |
| cloudexpress-score-change | viptelaVpnCloudExpressScoreChange |
| control-connection-auth-fail | viptelaSecurityControlConnectionAuthFail |
| control-connection-state-change | viptelaSecurityControlConnectionStateChange |
| control-connection-tloc-ip-change | viptelaSecurityControlConnectionTlocIpChange |

| Notifications | Corresponding SNMP Trap |
|---|---|
| control-no-active-vbond | viptelaSecurityControlNoActiveVbond |
| control-no-active-vsmart | viptelaSecurityControlNoActiveVsmart |
| control-vbond-state-change | viptelaSecurityControlVbondStateChange |
| control-vedge-list-request | viptelaSecurityControlVedgeListRequest |
| cpu-usage | viptelaSystemCpuUsage |
| data-policy-association-status | viptelaPolicyDataPolicyAssociationStatus |
| device-template-attached-during-ztp | viptelaSecurityDeviceTemplateAttachedDuringZtp |
| device-template-missing | viptelaSecurityDeviceTemplateMissing |
| dhcp-address-assigned | viptelaVpnDhcpAddressAssigned |
| dhcp-address-released | viptelaVpnDhcpAddressReleased |
| dhcp-address-renewed | viptelaVpnDhcpAddressRenewed |
| dhcp-request-rejected | viptelaVpnDhcpRequestRejected |
| dhcp-server-state-change | viptelaVpnDhcpServerStateChange |
| disk-usage | viptelaSystemDiskUsage |
| domain-id-change | viptelaSystemDomainIdChange |
| domain-state-change | viptelaWwanDomainStateChange |
| emmc-fault | viptelaHardwareEmmcFault |
| fan-fault | viptelaHardwareFanFault |
| fantray-fault | viptelaHardwareFantrayFault |
| fib-update | viptelaVpnFibStateChange |
| flash-fault | viptelaHardwareFlashFault |
| interface-admin-state-change | viptelaVpnInterfaceAdminStateChange |
| interface-bw | viptelaVpnInterfaceBw |
| interface-pcs-fault-detected | viptelaVpnInterfacePcsFaultDetected |
| interface-state-change | viptelaVpnInterfaceStateChange |
| last-resort-state-change | viptelaVpnLastResortStateChange |
| memory-usage | viptelaSystemMemoryUsage |
| omp-number-of-vsmarts-change | viptelaOmpOmpNumberOfVsmartsChange |

| Notifications | Corresponding SNMP Trap |
|---|---|
| omp-peer-state-change | viptelaOmpOmpPeerStateChange |
| omp-policy | viptelaOmpOmpPolicy |
| omp-state-change | viptelaOmpOmpStateChange |
| org-name-change | viptelaSystemOrgNameChange |
| ospf-interface-state-change | viptelaVpnOspfInterfaceStateChange |
| ospf-neighbor-state-change | viptelaVpnOspfNeighborStateChange |
| pem-fault | viptelaHardwarePemFault |
| pem-state-change | viptelaHardwarePemStateChange |
| pim-fault | viptelaHardwarePimFault |
| pim-interface-state-change | viptelaVpnPimInterfaceStateChange |
| pim-neighbor-state-change | viptelaVpnPimNeighborStateChange |
| pim-state-change | viptelaHardwarePimStateChange |
| pim-tunnel-state-change | viptelaVpnPimTunnelStateChange |
| process-down | viptelaSystemProcessDown |
| process-restart | viptelaSystemProcessRestart |
| pseudo-commit-status | viptelaSystemPseudoCommitStatus |
| qos-state-change | viptelaWwanQosStateChange |
| reg-state-change | viptelaWwanRegStateChange |
| route-install-fail | viptelaVpnRouteInstallFail |
| sd-card-fault | viptelaHardwareSdcardFault |
| security-certificate-expired | viptelaSecuritySecurityCertificateExpired |
| security-certificate-expiring | viptelaSecuritySecurityCertificateExpiring |
| security-certificate-installed | viptelaSecuritySecurityCertificateInstalled |
| security-clear-installed-certificate | viptelaSecuritySecurityClearInstalledCertificate |
| security-new-csr-generated | viptelaSecuritySecurityNewCsrGenerated |
| security-root-cert-chain-installed | viptelaSecuritySecurityRootCertChainInstalled |
| security-root-cert-chain-uninstalled | viptelaSecuritySecurityRootCertChainUninstalled |
| security-unclaimed-vedge-entry-added | viptelaSecuritySecurityUnclaimedVedgeEntryAdded |

| Notifications | Corresponding SNMP Trap |
|---|---|
| security-vedge-entry-added | viptelaSecuritySecurityVedgeEntryAdded |
| security-vedge-entry-removed | viptelaSecuritySecurityVedgeEntryRemoved |
| security-vedge-serial-file-uploaded | viptelaSecuritySecurityVedgeSerialFileUploaded |
| security-vsmart-serial-file-uploaded | viptelaSecuritySecurityVsmartSerialFileUploaded |
| service-gre-state-update | viptelaSecurityGreStateUpdate |
| sfp-state-change | viptelaHardwareSfpStateChange |
| sfp-support-state | viptelaHardwareSfpSupportState |
| sim-state-change | viptelaWwanSimStateChange |
| site-id-change | viptelaSystemSiteIdChange |
| sla-change | viptelaAppRouteSlaChange |
| sla-config | viptelaPolicySlaConfig |
| sla-violation | viptelaPolicySlaViolation |
| sla-violation-pkt-drop | viptelaPolicySlaViolationPktDrop |
| system-aaa-login-fail | viptelaSystemSystemAaaLoginFail |
| system-commit | viptelaSystemSystemCommit |
| system-ip-change | viptelaSystemSystemIpChange |
| system-login-change | viptelaSystemSystemLoginChange |
| system-logout-change | viptelaSystemSystemLogoutChange |
| system-reboot-aborted | viptelaActionsSystemRebootAborted |
| system-reboot-complete | viptelaActionsSystemRebootComplete |
| system-reboot-issued | viptelaActionsSystemRebootIssued |
| system-software-install-status | viptelaActionsSystemSoftwareInstallStatus |
| tempsensor-fault | viptelaHardwareTempsensorFault |
| tempsensor-state | viptelaHardwareTempsensorState |
| tunnel-install-fail | viptelaVpnTunnelInstallFail |
| tunnel-ipsec-manual-rekey | viptelaSecurityTunnelIpsecManualRekey |
| tunnel-ipsec-rekey | viptelaSecurityTunnelIpsecRekey |
| usb-state-change | viptelaHardwareUsbStateChange |

| Notifications | Corresponding SNMP Trap |
|---|---|
| vbond-reject-vedge-connection | viptelaSecurityVbondRejectVedgeConnection |
| vmanage-connection-preference-changed | viptelaSecurityVmanageConnectionPreferenceChanged |
| vrrp-group-state-change | viptelaVpnVrrpGroupStateChange |
| zbfw-clear-flow-table-full | viptelaPolicyZbfClearFlowTableFull |
| zbfw-clear-half-open-hit | viptelaPolicyZbfClearHalfOpenHit |
| zbfw-flow-creation | viptelaPolicyZbfFlowCreation |
| zbfw-flow-deletion | viptelaPolicyZbfFlowDeletion |
| zbfw-flow-table-full | viptelaPolicyZbfFlowTableFull |
| zbfw-half-open-limit-hit | viptelaPolicyZbfHalfOpenHit |
| zbfw-pkt-log | viptelaPolicyZbfPktLog |

# Supported SNMP MIBs

*Table 28: Feature History*

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

| Feature Name | Release Information | Description |
|---|---|---|
| Cisco Catalyst SD-WAN MIBs | Cisco IOS XE Catalyst SD-WAN Release 17.8.1a<br>Cisco vManage Release 20.8.1 | The following Cisco Catalyst SD-WAN MIBs are introduced on Cisco IOS XE Catalyst SD-WAN devices:<br>CISCO-SDWAN-PROBE-MIB.my<br>CISCO-SDWAN-OMP-MIB.my (additional tables added)<br>CISCO-SDWAN-SECURITY-MIB.my (additional tables added) |

### Cisco IOS XE Catalyst SD-WAN Devices

You can download the MIBs supported on Cisco IOS XE Catalyst SD-WAN devices from https://github.com/cisco/cisco-mibs

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.8.1a, OMP MIB tables and scalar objects are supported in CISCO-SDWAN-OMP-MIB.my.

In Cisco IOS XE Release 17.6.1a, only ciscoSdwanOmpOmpNumberOfVsmartsChange, ciscoSdwanOmpOmpStateChange, ciscoSdwanOmpOmpPeerStateChange, and ciscoSdwanOmpOmpPolicy OMP traps are supported and no OMP MIB tables and scalar objects are supported in CISCO-SDWAN-OMP-MIB.my.

**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 Catalyst SD-WAN devices as alternative APIs for monitoring and troubleshooting.

**Note** Starting from Cisco IOS XE Release 17.6.3, CISCO-SDWAN-APP-ROUTE-MIB includes appRouteStatisticsAppProbeClassTable and appRouteStatisticsAppProbeClassIntervalTable OIDs to support Mean Jitter, Latency and Packet Drop data requests from SNMP.

**Note** Starting from Cisco IOS XE Catalyst SD-WAN Release 17.9.2a, if a SNMP MIB table includes a large number of table entries, then we recommend that you use **snmp-server subagent fetch count***100* command. By default, the count value is 50.

### Cisco vEdge Devices

For supported Cisco vEdge MIBs, see https://github.com/cisco/cisco-mibs/tree/main/viptela-mibs.

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