

Devices and Controllers

Table 1: Feature History

Feature Name	Release Information	Description
Data Plane CPU and Memory Utilization	Cisco IOS XE Catalyst SD-WAN Release 17.16.1a Cisco Catalyst SD-WAN Manager Release 20.16.1	With this feature you can monitor data plane CPU and memory utilization on Cisco IOS XE Catalyst SD-WAN devices using Cisco SD-WAN Manager.
QoS statistics for interfaces and tunnels	Cisco Catalyst SD-WAN Manager Release 20.18.1	You can monitor traffic across network interfaces and tunnels with real-time and historical statistics. This feature extends the existing QoS interface-level view to include class-level traffic insights and per-tunnel QoS statistics.

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

This section provides information on the Cisco Catalyst SD-WAN devices and control components.

- View the Geographic Location of Your Devices, on page 2
- View System Status, on page 5
- View Device System Resource Utilization in Cisco SD-WAN Manager, on page 6
- View Device System Resource Utilization Using the CLI, on page 6
- View and Open TAC Cases, on page 7
- View the Status of a Cisco Catalyst SD-WAN Validator, on page 8
- View the Status of a Cisco Catalyst SD-WAN Controller, on page 9
- View Control Connections, on page 10
- View Devices Connected to Cisco Catalyst SD-WAN Manager, on page 10
- View Services Running on Cisco Catalyst SD-WAN Manager, on page 10
- View Device Status in the Overlay Network, on page 11
- View Device Information, on page 11

- View Device Configuration, on page 14
- View the Software Versions Installed on a Device, on page 14
- View Device Interfaces, on page 14
- View WAN Interfaces, on page 15
- View Interfaces in Management VPN or VPN 512, on page 16
- View DHCP Server and Interface Information, on page 16
- View Interface MTU Information, on page 17
- View and Monitor Cellular Interfaces, on page 17
- View Colocation Cluster Information, on page 19
- View Cisco Colo Manager Health, on page 20
- View Cisco Catalyst SD-WAN Manager Cluster Information Using the CLI, on page 21
- View QoS statistics, on page 21
- Collect System Information in an Admin-Tech File, on page 27
- Monitor Cflowd and SAIE Flows for Cisco IOS XE Catalyst SD-WAN Devices, on page 32
- Reboot a Device, on page 33
- Reset Interfaces, on page 35
- Make Your Device Invalid, on page 35
- Bring Your Device Back to Valid State, on page 35
- Stop Data Traffic, on page 36
- Perform a Factory Reset, on page 36
- Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices, on page 37

View the Geographic Location of Your Devices

Use the **Geography** window in Cisco SD-WAN Manager to view information about the Cisco Catalyst SD-WAN devices and links in the overlay network. The **Geography** window provides a map displaying the geographic location of the devices in the overlay network.

Note The browser on which you are running Cisco SD-WAN Manager must have internet access. If you do not have internet access, ensure that the browser has access to "*.openstreetmaps.org."

To view the geographic location of the devices in the overlay network:

1. From the **VPN Group** list, choose a VPN group.
2. From the **VPN Segment** list, choose a VPN segment.
3. Set filters.

Set Map Filters

To select the devices and links you want to display on the map:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter**.

3. From the options that display, choose the device group. By default, the group **All** is selected and displays all devices in the overlay network. The group **No Groups** displays devices that are not part of a device group. If all devices are in a group, the **No Groups** option is not displayed.
4. Choose the devices you want to view. By default, the map displays all device types including edge devices, Cisco SD-WAN Validator, Cisco SD-WAN Controller, and Cisco SD-WAN Manager.
5. Choose the state of control and data links. By default, the map displays all control and data connections.
6. Close the **Filter** box by moving the cursor outside the box.

The map dynamically updates to display your selections.

View Device Information

To view basic information for a device, hover over the device icon. A pop-up box displays the system IP, hostname, site ID, device type, and device status.

To view detailed information for a device, double-click the device icon. Click **Device Dashboard**, **Device Details**, **SSH Terminal**, **Site Topology**, or **Links** to view more details for the device.

Note the following about links:

- A thin blue line displays an active control connection between two devices.
- A bold blue line displays multiple active connections between devices.
- A dotted red line displays a control connection that is down.
- A bold dotted red line displays multiple control connections that are down.
- A thin green line displays an active data connection between two devices.
- A bold green line displays multiple active data connections.
- A dotted red line displays a data connection that is down.
- A bold dotted red line displays multiple data connections that are down.
- A thick gray line displays an active consolidated control and data connection between two devices.

  If you hover over the line, a hover box tells you if the connection is up or down.

Configure and View Geographic Coordinates for a Device

To configure the geographic coordinates for a device, use the **System Feature** template under **Configuration** > **Templates**.

If the Cisco Catalyst SD-WAN device is not attached to a configuration template, you can configure the latitude and longitude directly on the device:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **SSH Terminal**.
2. Choose a device from the left pane. The SSH Terminal window opens in the right pane.
3. Enter the username and password to log in to the device.
4. Use the `show system status` command to determine whether the device is attached to a configuration template:

```
Device# show system status...
    Personality:            vedge
    Model name:             vedge-cloud
    Services:               None
    vManaged:               false
    Commit pending:         false
    Configuration template: None
```

In the output, check the values in the `vManaged` and `Configuration template` output fields. If the `vManaged` field is false, the device is not attached to a configuration template, and the `Configuration template` field value is `None`. For such a device, you can configure the GPS coordinates directly from the CLI. If the `vManaged` field is `true`, the Cisco SD-WAN Manager server has downloaded the device configuration, and the `Configuration template` field value displays the name of the configuration template. For such a device, you cannot configure the GPS coordinates directly from the CLI. If you attempt to do so, the `validate` or `commit` commands fails with the following message:

```
Aborted: 'system is-vmanaged': This device is being managed by the vManage. Configuration
 through the CLI is not allowed.
```

5. Enter configuration mode:

   For Cisco vEdge devices:

   ```
   Device# config
       Device(config)#
   ```

   For Cisco IOS XE Catalyst SD-WAN devices:

   ```
   Device# configure-transaction
       Device(config)#
   ```

6. Configure the latitude and longitude for the device.

   ```
   Device(config)# system gps-location latitude
                              degrees.minutes.seconds
       Device(config-system)# gps-location longitude
                              degrees.minutes.seconds
   ```

7. Save the configuration.

   ```
   Device(config-system)# commit
       Device(config-system)#
   ```

Note For the device/site location in Cisco SD-WAN Manager, there are several data sources including network hierarchy, GPS, geo-fencing, manual configuration and system default.

- The device location priority is: GPS > geo-fencing > manual configuration > system default

  monitoring → device table

  monitoring → device360 information icon

- The site location priority is: network hierarchy > device (the first device in site) location

  monitoring → geographical view

View System Status

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco SD-WAN Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device. If you choose a Cisco vEdge device, the window displays **System Status** by default.

   If you choose a Cisco IOS XE Catalyst SD-WAN device or any controller, click **System Status** in the left pane. The right pane displays information about the device.

Information About System Status Parameters

The **System Status** window displays the following:

- Reboot—Number of times the device has rebooted. For details about each reboot, click **Reboot**. The Reboot window opens and contains the following elements:
- Crash—Number of times the device has crashed. For details about each crash, click **Crash**. The Crash window opens and contains the following elements:
- Status of hardware components, applicable only if the selected device is a hardware:
  - Module
  - Temperature sensors
  - USB
  - Power supply
  - Fans

The status of a hardware component is represented in one of the following ways:

- Green check mark—Component is operational.
- Red circle with an X—Component is down.
- Orange triangle with an exclamation point—Component has an error.
- N/A—Not applicable since the selected device is not a hardware Cisco vEdge device.
- CPU & Memory—To the right are the time periods. Click a predefined or custom time period for which to display data.
  - CPU usage—Displays the CPU usage, as a percentage of available CPU, over the selected time range.
  - Memory usage—Displays the memory usage, as a percentage of available memory, over the selected time period.

View Device System Resource Utilization in Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Choose a Cisco IOS XE Catalyst SD-WAN device or a controller.
3. Click **System Status** in the left pane.

   The right pane displays information about the device.
4. On the **System Status** page, view system resource details, such as control plane CPU and memory, data plane CPU and memory, and power usage details in the **CPU & Memory** pane.
5. Click either **Real Time**, a predefined time period, or a custom time period for which you want to view data.

   Cisco SD-WAN Manager shows the CPU and memory utilization details for a device for a selected time duration. The device collects the utilization data every 10 seconds and stores it in an XML or a JSON file format on the device.

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, devices export data plane CPU and memory statistics to Cisco SD-WAN Manager. The system utilization graph displays these statistics.

From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a, Cisco SD-WAN Manager displays historical power usage data over a period of time.

View Device System Resource Utilization Using the CLI

System and Resource Status

The **show sdwan system status** command displays the system status for a device and shows the CPU utilization calculation.

For releases before Cisco SD-WAN Release 20.9.1, the user CPU time (in percentage) is used to calculate the CPU utilization of a device.

For releases Cisco SD-WAN Release 20.9.1 and later, both the user CPU time and the system CPU time (in percentage) are used to calculate the CPU utilization of a device, as indicated in the **show sdwan system status**.

The following example shows the system status for Cisco SD-WAN Manager devices:

```
Device# show sdwan system status
System logging to host  is disabled
System logging to disk is enabled
System state:            GREEN. All daemons up
System FIPS state:       Disabled
Last reboot:             Image Install
CPU-reported reboot:     Initiated by other
Boot loader version:     Not applicable
System uptime:           0 days 00 hrs 23 min 31 sec
Current time:            Mon Jan 30 10:24:44 UTC 2023
```

```
Hypervisor Type:          ESXI
Cloud Hosted Instance:    false
Load average:             1 minute: 1.10, 5 minutes: 1.67, 15 minutes: 1.71
Processes:                557 total
CPU allocation:           16 total,   1 control,   7 data
CPU states:           10.38% user,   1.47% system,   88.04% idle ---------CPU Utilization
Memory usage:             32820584K total,    4488868K used,   28331716K free
                          575156K buffers,  3859052K cache
Disk usage:               Filesystem      Size   Used  Avail   Use %  Mounted on
                       /dev/disk/by-label/fs-bootflash  45580M  2327M  40934M  5% /bootflash

                                 387M  159M  223M   42   /bootflash/.installer
```

Quantum Flow Processor Status

View and Open TAC Cases

Table 2: Feature History

Feature Name	Release Information	Description
Access TAC Cases from Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1 Cisco SD-WAN Release 20.9.1	This feature allows you to access Support Case Manager (SCM) wizard using Cisco SD-WAN Manager. You can create, view, or edit the support cases directly from Cisco SD-WAN Manager without having to go to a different Case Manager portal.
SCM Integration Improvements	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	This feature introduces various enhancements to the Settings page in Cisco SD-WAN Manager and the Support Case Manager (SCM) wizard.

Supported Devices

This feature is supported on both Cisco Catalyst SD-WAN and Cisco IOS XE Catalyst SD-WAN devices.

Overview

For any Cisco SD-WAN Manager troubleshooting issues, you raise a support case in the SCM portal. In Cisco SD-WAN Manager, there is a provision to upload an Admin-Tech File to a specific Service Request (SR) on the SCM server by providing the SR number and the token details.

Starting from Cisco vManage Release 20.9.1, you can access SCM portal from Cisco SD-WAN Manager. In the SCM portal, you can create, view, or upload an admin-tech file. For more information on Admin-tech files, see Admin-Tech File.

Prerequisites to Access TAC Cases

- You need active Cisco single sign-on (SSO) login credentials to access the SCM Wizard and the cloud server.

View TAC Cases

Perform the following steps to view TAC cases from Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **TAC Cases**.
2. Login to the SCM portal using Cisco SSO login.

   The TAC Support Cases portal displays a list of cases.

Open a TAC Case

Perform the following steps to open a TAC Case from Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **TAC Cases**.
2. In the **TAC Support Cases** page, click **Open a Case**.
3. Enter all the other relevant case details.
4. Click **Create**.

   The **TAC Support Cases** portal now displays the updated list of cases.

For more information about using SCM portal, refer Cisco TAC Connect.

View the Status of a Cisco Catalyst SD-WAN Validator

You have the following options to view the status of a Cisco Catalyst SD-WAN Validator.

Use the Dashboard Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.
2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **Cisco vBond**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of Cisco SD-WAN Validator orchestrators in your overlay network.
3. To know the status of the Cisco Catalyst SD-WAN Validator, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.

2. Click **Filter** and choose **vBond** under **Types**.
3. Click the Cisco SD-WAN Validator icon to check its status.

Use the Network Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the Cisco Catalyst SD-WAN Validator that you want to view the status for. You can either scroll through the list of devices in the device table or enter **Validator** as the keyword in the search bar.
3. Click the relevant Cisco Catalyst SD-WAN Validator under the **Hostname** column. The **Control Connections** screen opens by default and displays information about all control connections that the device has with other controller devices in the network.

View the Status of a Cisco Catalyst SD-WAN Controller

You have the following options to view the status of a Cisco Catalyst SD-WAN Controller.

Use the Dashboard Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.
2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **Cisco vSmart**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of Cisco SD-WAN Controller in your overlay network.
3. To know the status of the Cisco Catalyst SD-WAN Controller, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter** and choose **vSmart** under **Types**.
3. Click the Cisco SD-WAN Controller icon to check its status.

Use the Network Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.1 and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the Cisco Catalyst SD-WAN Controller that you want to view the status for. You can either scroll through the list of devices in the device table or enter **Validator** as the keyword in the search bar.
3. Click the relevant Cisco Catalyst SD-WAN Controller instance under the **Hostname** column. The **Control Connections** screen opens by default and displays information about all control connections that the device has with other controller devices in the network.

View Control Connections

To view all control connections for a device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Choose a device to view its control connections.

   If you select a controller device—a Cisco Catalyst SD-WAN Validator, Cisco SD-WAN Manager, or a Cisco Catalyst SD-WAN Controller, the **Control Connections** screen opens by default.
3. If you choose an edge device, the System Status screen displays by default. To view control connections for the device, click **Control Connections** in the left pane. The right pane displays information about all control connections that the device has with other controller devices in the network.

The upper area of the right pane contains the following elements:

- Expected and actual number of connections.
- Control connection data in graphical format. If the device has multiple interfaces, Cisco SD-WAN Manager displays a graphical topology of all control connections for each color.

The lower area of the right pane contains the following elements:

- Search bar—Includes the Search Options drop-down, for a Contains or Match.
- Control connections data in tabular format. By default, the first six control connections are selected. The graphical display in the upper part of the right pane plots information for the selected control connections.

View Devices Connected to Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.
2. Under **Service Configuration**, click the hostname of the desired Cisco SD-WAN Manager server. The **Manager Details** screen appears.
3. Or alternatively:

   Under **Service Configuration**, for the desired Cisco SD-WAN Manager instance, click **...** and choose **Device Connected**.

View Services Running on Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Cluster Management**.

2. Under **Service Configuration**, click the hostname of the desired Cisco SD-WAN Manager server. The screen displays the process IDs of all the Cisco SD-WAN Manager services that are enabled on Cisco SD-WAN Manager.

View Device Status in the Overlay Network

You have the following options to view the status of a device in the overlay network.

Use the Dashboard Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Overview**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Dashboard** > **Main Dashboard**.

2. For releases before Cisco vManage Release 20.6.1, click the upward or downward arrow next to **WAN Edge**.

   For Cisco vManage Release 20.6.1 and later, click the number representing the number of **WAN Edge** devices.

3. To know the status of the WAN edge device, see the **Reachability** column in the dialog box that opens.

Use the Geography Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.
2. Click **Filter** and choose **WAN Edge** under **Types**.
3. Click the router icon to check its status.

Use the Network Screen

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the WAN edge router that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Click the relevant WAN edge router under the **Hostname** column. The **System Status** screen opens by default.

View Device Information

You can view basic or detailed information for a device in the overlay network.

To view basic information:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Geography**.

2. Hover over the device icon.

   A pop-up box displays the system IP address, hostname, site ID, device type, and device status. To view more information for a device, double-click the device icon to open the **View More Details** pop-up box. Click **Device Dashboard**, **Device Details**, **SSH Terminal**, or **Links** to get further details for the device.

To view detailed information:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Locate the WAN edge router to view the status. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.

3. Click the relevant device under the **Hostname** column. The right pane displays System Status by default. To view more detailed information for the device, choose one of the categories from the left pane.

Note Starting from Cisco vManage Release 20.9.2, the **Monitor** > **Devices** page displays the devices that are newly added or synced to Cisco SD-WAN Manager using the options available on the **Configuration** > **Devices** page.

View Device Health in Table View

Minimum supported release: Cisco vManage Release 20.10.1

You can view details about the device health for the last one hour in the table view by default in the **Monitor Device** window.

The table displays:

- Device model
- Site ID
- System IP address
- Device health
- Device reachability
- Memory utilization
- CPU load
- RA session
- RA session breakdown

Starting from Cisco Catalyst SD-WAN Manager Release 20.14.1, you can view the devices with remote access in the **Devices** table. To view remote access devices, open the filters under **Devices**, and under **Type**, check the **Remote Access** checkbox.

You can also view the health of all the devices on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

Devices Health Metrics

The devices health is calculated as follows:

Health State	Reachability	Control Plane	Data Plane	Resources	Evaluation Logic
Good	Device reachable	All control connections up	All BFD tunnels up	CPU usage < 75% Memory usage < 75%	All attributes met
Fair	Device reachable	> = 1 control connections up	> = 1 BFD tunnels up	CPU usage > 75% Memory usage > 75%	Any attributes met
Poor	Device not reachable	No control connections up	No BFD tunnels up	CPU usage > 90% Memory usage > 90%	Any attributes met

For a single device record the health is calculated as follows:

Health	QoE
Good	10
Fair	5
Poor	0

The average health metric of devices is calculated as follows:

Health	QoE
Good	QoE >= 6.67
Fair	3.34 <= QoE < 6.67
Poor	0 < QoE < 3.34

View Device Health in Heatmap View

Minimum supported release: Cisco vManage Release 20.10.1

In the heatmap view, the grid of colored squares displays the device health as **Good**, **Fair**, or **Poor**. You can hover over a square or click it to display additional details of a device at a specific time. Click the time interval drop-down list to change the time selection and filter the data for a specific interval.

You can view the health of all the devices on a single site by clicking **All Sites** and selecting the site ID to enter the single site view.

View Device Configuration

Note From Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as **Control Components** for consistency with Cisco Catalyst SD-WAN terminology.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices** .
2. Click **WAN Edge List** or **Control Components**.
3. To view the running configuration, for the desired device, click **…** and choose **Running Configuration**.

   To view the local configuration, for the desired device, click **…** and choose **Local Configuration**.

View the Software Versions Installed on a Device

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Software Versions**.

View Device Interfaces

To view information about interfaces on a device:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Interface** in the left pane. The right pane displays interface information for the device.

The upper part of the right pane contains:

- Chart Options bar—Located directly under the device name, this bar includes:
  - Chart Options drop-down—Click **Chart Options** to choose how the data should be displayed.

    - IPv4 & IPv6 drop-down—Click **IPv4 & IPv6** to choose the type of interfaces to view. The information is displayed in graphical format. By default, the graph is Combined, showing interfaces on which both IPv4 and IPv6 addresses are configured. To view IPv4 and IPv6 interfaces in separate graphs, select the Separated toggle button.
    - Time periods—Click either **Real Time**, a predefined time period, or a custom time period for which to view the data.

- Interface information in graphical format.
- Interface graph legend—Choose an interface to display information for just that interface.

The lower part of the right pane contains:

- Filter criteria.
- Interface table, which lists information about all interfaces. By default, the first six interfaces are displayed. The graphical display in the upper part of the right pane plots information for the selected interfaces.
    - Check the check box to the left to select and deselect interfaces. You can select and view information for a maximum of 30 interfaces at a time.
    - To rearrange the columns, drag the column title to the desired position.
    - For cellular interfaces, click the interface name to view a detailed information about the cellular interface.

To view interface status and interface statistics, see show interface and show interface statistics.

View WAN Interfaces

Transport interfaces in VPN 0 connect to a WAN network of some kind, such as the Internet, Metro Ethernet network, or an MPLS network.

You can view information about WAN interfaces on a device using one of the following options:

Real Time Pane

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the window that opens, choose **Real Time** in the left pane.
5. From the **Device Options** drop-down in the right pane, choose **Control WAN Interface Information**.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.12.1, a new field **Bind Interface** is introduced to display mapping relationship between the loopback interfaces and the physical interfaces.

Interface Pane

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. From the **Device Groups** drop-down list, choose the device group to which the device belongs.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, choose **Interface**.

View Interfaces in Management VPN or VPN 512

VPN 512 is commonly used for out-of-band management traffic. To display information about the interfaces in VPN 512 on a router:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Locate the device that you want to view the status for. You can either scroll through the list of devices in the device table or enter a keyword in the search bar.
3. Choose the device by clicking its name in the **Hostname** column.
4. In the left pane, click **Real Time**.
5. From the **Device Options** drop-down list in the right pane, choose **Interface Detail**.
6. In the **Select Filter** dialog box, click **Show Filters** if you want to use filters. Otherwise click **Do Not Filter**.
7. In the **Search bar**, enter **512**, which is the management VPN.

CLI equivalent: show interface vpn 512.

View DHCP Server and Interface Information

When you configure a tunnel interface on a device, several services are enabled by default on that interface, including DHCP. The device can act as a DHCP server for the service-side network to which it is connected, assigning IP addresses to hosts in the service-side network. It can also act as a DHCP helper, forwarding requests for IP addresses from devices in the service-side network to a DHCP server that is in a different subnet on the service side of the device.

To view DHCP server and interface information:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose the device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane. choose one of the following to view specific DHCP server and interface information:

Device Option	Command	Description
DHCP Servers	show dhcp server	View information about the DHCP server functionality that is enabled on the device
DHCP Interfaces	show dhcp interface	View information about the interfaces on which DHCP is enabled on an edge device or a Cisco SD-WAN Controller

View Interface MTU Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Interface Detail**.

View and Monitor Cellular Interfaces

This topic describes how to monitor the status of cellular interfaces in Cisco Catalyst SD-WAN devices.

Monitor Cellular Interfaces

You can verify signal strength and service availability using either Cisco SD-WAN Manager or the LED on the router. You can view the last-seen error message for cellular interfaces from Cisco SD-WAN Manager.

Verify Signal Strength

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. From the **Device Groups** drop-down list, choose a group that the device belongs to.
3. Choose a device by clicking its name in the **Hostname** column.
4. Click **Real Time** in the left pane.
5. From the **Device Options** drop-down list in the right pane, choose **Cellular Radio**.

   The values for the different cellular signals are displayed. If signal strength is poor, or there is no signal, see Troubleshoot Common Cellular Interface Issues.

CLI equivalent: **show cellular status**

Verify Radio Signal Strength Using the Router LED

To check signal strength and service availability of a cellular connection from the router, look at the WWAN Signal Strength LED. This LED is typically on the front of the routers, and is labeled with a wireless icon.

The following table explains the LED color and associated status:

Table 3:

Color	Signal Strength	State	Description
Off	—	—	LTE interface disabled (that is, admin status is down) or not configured
Green	Excellent	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data being received and transmitted)
Yellow	Good	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data being received and transmitted)
Orange	Poor	Solid	LTE interface enabled and in dormant mode (no data being received or transmitted)
		Blinking	LTE interface enabled and in active mode (data are being received and transmitted)
Red	Critical Issue	Solid	LTE interface enabled but faulty; issues include no connectivity with the base transceiver station (BTS) and no signal

View Error Messages for Cellular Interfaces

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Cellular Status**.

   The output displayed includes a column for Last Seen Error

CLI equivalent **show cellular status**

View Cellular Connections

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.
3. Click **Real Time** in the left pane.
4. From the **Device Options** drop-down list in the right pane, choose **Cellular Connection**.

   The output displayed includes columns for **Profile APN** and the link time **Up Since**.

Table 4:

Field	Description
Profile APN	Displays the access point name for cellular connections.
Up Since	Displays the actual time since the connection was established.

CLI equivalent: **show cellular** <*interface*> **connection**

View Colocation Cluster Information

To view the cluster information and their health states. Reviewing this information can help you to determine which CSP device is responsible for hosting each VNF in a service chain.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Click **Colocation Cluster**.

   All clusters with relevant information are displayed in a tabular format. Click a cluster name.

   From the primary part of the left pane, you can view the cluster topology. In the right pane, you can view the cluster information such as the available and the total CPU resources, available and allocated memory, and so on, based on the size of Cloud OnRamp for Colocation.

The detail part of the left pane contains:

- Filter criteria–choose the fields to be displayed from the search options drop-down.
- A table that lists information about all devices in the cluster (CSP devices and switches).

  Click a CSP cluster. VNF information is displayed in a tabular format. The table includes information such as VNF name, service chains, CPU use, memory consumption, disk, management IP, and other core parameters that define performance of a network service.

3. Click **Services**.

   Under this area, you can view:

   - All service groups that are attached to the cluster in a tabular format. The first two columns display the name and description of the service chain within the service group.
   - Click **Diagram** to view the service group with all its service chains and VNFs in the design view window.
   - Click a VNF. You can view CPU, memory, and disk allocated to the VNF in a dialog box.
   - Choose a service group from the **Service Groups** drop-down list. The design view displays the selected service group with all its service chains and VNFs.

View Cisco Colo Manager Health

To view Cisco Colo Manager (CCM) health for a device, CCM host system IP, CCM IP, and CCM state:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.

   The right pane displays VNF information in a tabular format. The table includes information such as CPU use, memory consumption, and disk, and other core parameters that define performance of a network service.

2. Click a CSP device from the table.
3. From the left pane, click **Colo Manager**.

   The right pane displays information about the memory usage, CPU usage, uptime, and so on, for the colo manager.

View Cisco Catalyst SD-WAN Manager Cluster Information Using the CLI

Table 5: Feature History

Feature Name	Release Information	Description
Analyze the Health of the Cisco SD-WAN Manager Cluster and Cluster Services Using the CLI	Cisco vManage Release 20.9.1	With this feature, you can analyze the health of the Cisco SD-WAN Manager cluster and the status of the cluster services using the **request nms cluster diagnostics** CLI command.

You can use the **request nms cluster diagnostics** command to verify the health of the Cisco SD-WAN Manager cluster and the status of the cluster services running on the cluster. Run the command directly on the Cisco SD-WAN Manager device for which you are running the Cisco SD-WAN Manager cluster.

The **request nms cluster diagnostics** command provides diagnostics information for the Cisco SD-WAN Manager cluster and status information for the following Cisco SD-WAN Manager services:

- Application server
- Messaging server
- Configuration database
- Statistics configuration database
- Coordination server

For more information on the **request nms cluster diagnostics** command, see the *Cisco Catalyst SD-WAN* Command Reference Guide.

View QoS statistics

QoS queue statistics

Quality of Service (QoS) is used to manage and prioritize network traffic. QoS queue statistics measure the performance and utilization of network traffic queues, including metrics such as transmitted packets and dropped packets. These statistics help evaluate how effectively the network is prioritizing and managing traffic flows.

The QoS feature in Cisco SD-WAN Manager enables you to

- monitor the performance of ingress and egress traffic classes to ensure optimal performance across the network
- view tranmission rates for interfaces and tunnel endpoints, both before and after policy application, and

- identify drops caused by policing configured via interfaces and tunnel endpoints, even when policing is enabled via CLI template.

From Cisco Catalyst SD-WAN Manager Release 20.18.1, when you display statistics for a single interface, you can filter by traffic class.

Benefits of QoS queue statistics

- Continuous monitoring: The **QoS Monitor** page in SD-WAN Manager provides real-time QoS statistics for interfaces, tunnel endpoints, and traffic classes.
- Historical data visibility: The **QoS Monitor** page enables you to view historical data for interfaces and tunnels by selecting a time interval.

Restrictions for QoS statistics

Per tunnel QoS statistics

SD-WAN Manager supports per-tunnel QoS statistics only in the controller mode.

Drop statistics

In custom QoS policer configurations that use color selection for conform, exceed, or violate actions, a device may retain exceed-action or violate-action drop packets. As a result, these packets are not included in the drop statistics.

Supported QoS actions

QoS actions like bandwidth, priority, random-detect, child-level shaping, and policing are supported and displayed in the statistics. If a class-map does not contain any of these actions, it will not be collected or displayed. Fair-queuing is not supported.

Real-time QoS

- The **Real Time** view for **Tunnel QoS Summary Statistics** can display up to 4,000 entries.

Monitor the QoS statistics for interfaces

Monitor real-time and historical network traffic for interfaces.

Before you begin

To monitor QoS statistics on interfaces, enable the QoS feature on routers.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **QoS** to open the **QoS Monitor** page.

Step 4 Select a time interval for displaying QoS statistics.

Use the **Custom** option to define a specific range of start and end dates and times.

The **Post Policy Rate** and **Post Policy Counter** charts show the traffic and drop rates for the interfaces.

Interface QoS statistics

On the Interface page, you can view

- post-policy rate and post-policy counter charts for interfaces, and
- pre-policy transmission rates, post-policy transmission rates, and drop rates for each traffic class.

Table 6: Interface QoS charts

Chart	Description
Post Policy Rate	Displays data in kilobits per second (Kbps) and packet per second (PPS). • **Rate (Kbps)**: Displays the rate of traffic that successfully passed through the interface after the QoS policy was enforced. Hover over the chart to compare traffic rates across interfaces. • **Drop (Kbps)**: Displays the rate of traffic dropped due to policy enforcement on the interface. It provides basic drop statistics.
Post Policy Counter	Displays data in bytes and packets. • **Counter (bytes)**: Displays the total number of bytes forwarded through the interface after the QoS policy was applied. Hover over the chart to view byte or packet counts per interface. • **Drop (bytes)**: Displays the bytes dropped due to policy enforcement on the interface. It includes only basic drop statistics.

You can also view pre-policy, post-policy, and drop statistics for each interface to analyze class-level traffic details.

Each interface includes this:

Table 7: Interface QoS summary

Column	Description
Interface	Displays the name of the interface. Click an interface to view its classes, including pre-policy, post-policy, and drop rates.

Column	Description
Pre policy TX	Displays the rate of traffic transmitted before the policy was applied to the interface.
Post policy TX	Displays the rate of traffic transmitted after the policy was applied to the interface.
Drop	Displays the rate of traffic dropped after the policy was applied to the interface. The drop rate is the difference between post-policy and pre-policy transmission rates.

Monitor the QoS statistics for tunnels

Monitor real-time and historical network traffic for tunnels.

Before you begin

To monitor QoS statistics on tunnel endpoints, enable the QoS feature on routers.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **QoS** to open the **QoS Monitor** page.

Step 4 Click **Tunnel**.

Step 5 Select the time interval to display QoS statistics.

Use the **Custom** option to define a specific range of start and end dates and times.

The **Post Policy Rate** and **Post Policy Counter** charts show the traffic and drop rates for the tunnels.

Tunnel QoS statistics

On the Tunnel page, you can view

- post-policy rate and post-policy counter charts for tunnels, and
- pre-policy transmission rates, post-policy transmission rates, and drop rates for each traffic class.

Table 8: Tunnel QoS charts

Chart	Description
Post Policy Rate	Displays data in kilobits per second (Kbps) and packet per second (PPS). • **Rate (Kbps)**: Displays the rate of traffic that successfully passed through the interface after the QoS policy was enforced. Hover over the chart to compare traffic rates across tunnels. • **Drop (Kbps)**: Displays the rate of traffic dropped due to policy enforcement on the tunnel. It provides basic drop statistics.
Post Policy Counter	Displays data in Bytes and Packets. • **Counter (bytes)**: Displays the total number of bytes forwarded through the interface after the QoS policy was applied. Hover over the chart to view byte or packet counts per tunnel. • **Drop (bytes)**: Displays the bytes dropped due to policy enforcement on the tunnel. It includes only basic drop statistics.

You can also view pre-policy, post-policy, and drop statistics for each tunnel to analyze class-level traffic details.

Each tunnel includes this:

Table 9: Tunnel QoS summary

Column	Description
Tunnel Endpoints	Displays name of the tunnel endpoint. Click a tunnel endpoint to view its classes, including pre-policy, post-policy, and drop rates.
Remote System IP	Displays the IP address of the remote system.
Pre policy TX	Displays the rate of traffic transmitted before the policy was applied to the tunnel.
Post policy TX	Displays the rate of traffic transmitted after the policy was applied to the tunnel.
Drop	Displays the rate of traffic dropped after the policy was applied to the tunnel. The drop rate is the difference between post policy and pre policy transmission rates.

Monitor real time tunnel QoS statistics

Use the **Real Time** option to view QoS Statistics for each tunnel endpoint in real time.

Procedure

Step 1 From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

Step 2 Choose a device by clicking its name in the **Hostname** column.

Step 3 Click **Real Time**.

Step 4 From the **Device Options** drop-down list, choose either of these:

- **Tunnel QoS Statistics**: Use this option to filter the tunnel endpoints.
- **Tunnel QoS Summary Statistics**: Use this option to view a summary for all tunnel endpoints.

You can view a summary for the tunnel endpoints.

Column	Description
Tunnel Endpoint	Combination of the system IP address of the selected device along with local color of the tunnel endpoint, remote IP address, remote color, and the tunnel encapsulation type.
Queued Pkts	Number of packets queued for the tunnel endpoint. When there are no drops, the queued packets and transmitted packets have the same value.
Queued Bytes	Count in bytes queued for the tunnel endpoint. When there are no drops, the queued bytes and transmitted bytes have the same value.
Tx Pkts	Number of packets transmitted through the tunnel endpoint. When there are no drops, the queued packets and transmitted packets have the same value.
Tx Bytes	Traffic (in bytes) transmitted through the tunnel endpoint. When there are no drops, the queued bytes and transmitted bytes have the same value.
Drop Pkts	Number of packets dropped during transmission.
Drop Bytes	Traffic (in bytes) dropped during transmission.
Last Updated	Timestamp when the statistics are generated on the device. These statistics are updated every 10 seconds.

Collect System Information in an Admin-Tech File

Table 10: Feature History

Feature Name	Release Information	Description
Admin-Tech Enhancements	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This feature enhances the admin-tech file to include commands like **show tech-support memory**, **show policy-firewall stats platform**, **show sdwan confd-log netconf-trace** and so on in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.
Generate System Status Information for a Cisco SD-WAN Manager Cluster Using Admin Tech	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature adds support for generating an admin-tech file for a Cisco SD-WAN Manager cluster. The admin-tech file is a collection of system status information intended for use by Cisco Catalyst SD-WAN Technical Support for troubleshooting. Before this feature was introduced, Cisco Catalyst SD-WAN was only able to generate an admin-tech file for a single device.
View Generated Admin-Tech Files at Any Time	Cisco IOS XE Catalyst SD-WAN Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature provides support for viewing the generated admin-tech files whenever the admin-tech files are available on a device. You can view the list of generated admin-tech files and then decide which files to copy from your device to Cisco SD-WAN Manager. You can then download the selected admin-tech files to your local device, or delete the downloaded admin-tech files from Cisco SD-WAN Manager, the device, or both.
Additional Diagnostics Information Added to Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enhances the output of the admin-tech file with additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.
Upload an Admin-Tech File to a TAC Case	Cisco IOS XE Catalyst SD-WAN Release 17.7.1a Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	This feature enables you to upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case. When you create a TAC case, you can upload the generated admin-tech files to TAC service requests from Cisco SD-WAN Manager. This streamlines the steps required for working with TAC to troubleshoot a problem.

Feature Name	Release Information	Description
Generate an Admin-Tech File with the Feature Filter	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	This feature adds new options for information to include in the admin-tech file. For Cisco IOS XE Catalyst SD-WAN devices, you can include information about IPsec and security policy. For Cisco Catalyst SD-WAN Control Components, you can include information about the forwarding information base and routing information base.
Include Custom CLI Command Output in an Admin-Tech File	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can include the output of specific **show** commands in an admin-tech file. This is helpful for troubleshooting.
Cellular Modem Auto-Collect Crash Data	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	You can use the **lte modem crash-action auto-collect** command to configure a router to collect essential information about cellular modem operation, ensuring that the admin-tech file contains necessary details for troubleshooting in the event of an LTE modem crash.

Information About Admin Tech for Collecting System Information

An admin-tech file is a collection of system status information used for troubleshooting a given issue. Send your Cisco SD-WAN Manager admin-tech files to Cisco Catalyst SD-WAN Technical Support to resolve your issue.

You can generate an admin-tech file for a single device or for all the nodes in a Cisco SD-WAN Manager cluster.

Note Starting from Cisco vManage Release 20.7.1, the admin-tech file includes additional diagnostics information collected from the application server, the configuration database, the statistics database, and other internal services.

Note The admin-tech generation fails if any malformed characters are present in the disk.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, the generation of admin tech in Cisco SD-WAN Manager fails when disk space usage exceeds the designated limits. When the total utilized space surpasses the limit, you may attempt to delete the existing admin tech data from Cisco SD-WAN Manager.

If this action is ineffective, or if there are no admin tech files available for deletion, please contact your network administrator for further assistance in freeing up disk space. The administrator can ensure that the total utilized space at /opt/data/ remains below 80% and can attempt to delete admin tech across tenants in a multi-tenant setup.

Benefits of an Admin-Tech File for Collecting System Information

- Provides a consolidated file with system status information to submit to Cisco Catalyst SD-WAN Technical Support for diagnostics and troubleshooting.
- Provides support for directly uploading admin-tech files to Cisco Catalyst SD-WAN Technical Support

Prerequisites for Collecting System Information in an Admin-Tech File

- All of the nodes in the Cisco SD-WAN Manager cluster must be in a healthy state to generate an admin-tech file for all of the nodes in the cluster.

Restrictions for Collecting System Information in an Admin-Tech File

- All in-progress admin-tech requests are purged every three hours.
- You can have only one outstanding admin-tech request for a Cisco SD-WAN Manager cluster at a time. A second admin-tech request fails if there is an existing admin-tech request.
- Admin tech for a Cisco SD-WAN Manager cluster is successful only if admin tech is not running for individual devices.

Generate Admin-Tech Files

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. Do one of the following:
   - To generate an admin-tech file for all the nodes in a Cisco SD-WAN Manager cluster, click **Generate Admin Tech for Manager**.
   - To generate an admin-tech file for a single device, click ... adjacent to the device and choose **Generate Admin Tech for Manager**.
3. In the **Generate admin-tech File** pane, choose the content to include in the admin-tech tar file, as follows:

Field	Description
Logs	Include log files. **Note** The log files are stored in the `/harddisk/tracelogs` directory on the local device.
Core	Include core files. **Note** The core files are stored in the `/harddisk/core` directory on the local device.
Tech Features	**Note** From Cisco Catalyst SD-WAN Manager Release 20.15.1, this field is no longer available. This option is available in Cisco SD-WAN Manager Releases 20.13.x and 20.14.x. Choose additional information to include in the admin-tech file. The options depend on whether you are generating an admin-tech file for a single Cisco IOS XE SD-WAN device or for all devices and Cisco Catalyst SD-WAN Control Components. For Cisco IOS XE Catalyst SD-WAN devices: • **IPsec**: Include IPsec information. • **Security Policy**: Include security policy information. The technical information for the features is stored in a separate tech files in the folder /var/tech/ directory. By default, the admin file collects the technical information for IPsec and security features. The feature specific technical files are named as /var/tech/ipsec and /var/tech/security. For Cisco SD-WAN Control Components: • **All**: Include forward information base and route information base details. **Include fib detail**: Include forwarding information base details. **Include rib detail**: Include routing information base details.

Field	Description
Use Custom Commands	(Optional) Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 Enter **show** commands, separated by commas, to include **show** command output in the admin-tech file. The command output is available in the `/var/tech/custom` file path in the admin-tech zip file. From Cisco IOS XE Catalyst SD-WAN Release 17.16.1a and Cisco Catalyst SD-WAN Manager Release 20.16.1, some OMP and TTM commands are not supported. If you enter an unsupported command, the admin-tech file displays an error.

4. Click **Generate**.

   Cisco SD-WAN Manager creates the admin-tech file.

   The file name has the format *date-time*-admin-tech.tar.gz.

By default, the admin-tech file collects the technical information for IPsec and security features. The feature-specific technical files are named as `/var/tech/ipsec` and `/var/tech/security`.

For more information on admin-tech and technical support commands, see request admin-tech and show tech-support.

View Admin-Tech Files

You can perform any of the following operations after the admin-tech file is generated:

- View the list of the generated admin-tech files.
- Copy the selected admin-tech files from your device to Cisco SD-WAN Manager.
- Download the selected admin-tech files to your local device.
- Delete the selected admin-tech files from Cisco SD-WAN Manager, the device, or both.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **. . .** and choose **View Admin Tech List**.

   A tar file appears that contains the admin-tech contents of the device that you selected earlier. This file has a name similar to *`ip-address-hostname`*`-20210602-032523-admin-tech.tar.gz`, where the numeric fields are the date and the time.

   You can view the list of the generated admin-tech files and decide which files that you want to copy to Cisco SD-WAN Manager.
3. Click the **Copy** icon to copy the admin-tech file from the device to Cisco SD-WAN Manager.

   A hint appears letting you know that the file is being copied from the device to Cisco SD-WAN Manager.

4. After the file is copied from the device to Cisco SD-WAN Manager, you can click the **Download** icon to download the file to your local device.

   You can view the admin-tech file size after the file is copied to Cisco SD-WAN Manager.

5. After the admin-tech file is successfully copied to Cisco SD-WAN Manager, you can click the **Delete** icon and choose which files to delete from Cisco SD-WAN Manager, the device, or both.

For more information on admin tech and technical support commands, see request admin-tech and show tech-support.

Upload an Admin-Tech File to a TAC Case

From Cisco vManage Release 20.7.1, Cisco IOS XE Catalyst SD-WAN Release 17.7.1a, and Cisco SD-WAN Release 20.7.1, you can upload an admin-tech file directly from Cisco SD-WAN Manager when opening a TAC case.

Before You Begin

Ensure that you have generated admin-tech files from Cisco SD-WAN Manager.

Upload an Admin-Tech File to a TAC Case

Perform the following steps to upload an admin-tech file to a TAC case:

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. After you generate **Admin-Tech** files, click **Show Admin Tech List**.

   The **List of Admin-techs** window is displayed.
3. From the list of Admin-tech files, select the admin-tech file and click **Upload**.
4. In the **SR Number** and **Token** fields, enter the details.
5. Choose the **VPN** from the VPN options. The options are VPN 0 and VPN 512.
6. Click **Upload**.

   The selected admin-tech file is uploaded to the relevant service request.

Monitor Cflowd and SAIE Flows for Cisco IOS XE Catalyst SD-WAN Devices

Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.10.1a and Cisco vManage Release 20.10.1

For more information on monitoring Cflowd traffic flows, see Traffic Flow Monitoring with Cflowd.

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.
2. Click **…** adjacent to the Cisco IOS XE Catalyst SD-WAN device name and choose **Real Time**.
3. From the **Device Options** drop-down list, choose one of the following options:
   - **cFlowd Flows/DPI**

- **cFlowd ipv6 Flows/DPI**

4. Click **Show Filters**.

   You can search for Cflowd flow records based on the selected filters.

Note The filters are displayed only if you selected one of the Cflowd flows with the DPI device options.

Table 11: Filters for Cflowd with DPI Device Options

Field	Description
VPN ID	Enter the VPN ID.
Source IP	Enter the source IPv4 or IPv6 address.
Destination IP	Enter the destination IPv4 or IPv6 address.
Application	Enter the name of the application for which you are configuring Cflowd and SAIE monitoring.
Application Family	Enter the name of the application family for which you are configuring Cflowd and SAIE monitoring.

5. Click **Search** or **Reset All** to reset all the search filters.

Reboot a Device

Use the Device Reboot screen to reboot one or more Cisco Catalyst SD-WAN devices.

Reboot Devices

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Click **WAN Edge**, **Control Components**, or **Manager** depending on the device type that you want to reboot..
3. Check the check boxes next to the device or devices that you want to reboot.
4. Click **Reboot**.

View Active Devices

To view a list of devices on which the reboot operation was performed:

1. From the Cisco SD-WAN Manager toolbar, click the **Tasks** icon. Cisco SD-WAN Manager displays a list of all running tasks along with the total number of successes and failures.
2. Click a row to see details of a task. Cisco SD-WAN Manager opens a pane displaying the status of the task and details of the device on which the task was performed.

Reload a Security Application

The **Reload Services** option in the **Maintenance** > **Device Reboot** window lets you to recover a security application from an inoperative state. Ensure that you use this service as an initial recovery option. See Determine Security Applications in Inoperative State, on page 34.

Ensure that a security application has already been installed on the device that you choose to reload services for. To reload one or more security applications:

1. From the Cisco SD-WAN Manager menu, choose **Maintenance** > **Device Reboot**.
2. Under **WAN Edge**, check the check box for the Cisco Catalyst SD-WAN device you want to choose.
3. Click **Reload Services**.

   The **Reload Container** dialog box appears.
4. If the security application version is correct, check the check box against the version of the security application.
5. Click **Reload**.

   The security application stops, is uninstalled, reinstalled, and restarted.

Reset a Security Application

The **Reset Services** option in the **Maintenance** > **Device Reboot** window enables you to recover a security application from an inoperative state.

Use the **Reset Services** option when the virtual network configuration of a security application changes, such as, the virtual port group configuration on a device.

- Ensure that a security application is already been installed on the device that you choose to reset services for.
- Ensure that the chosen security application is in a running state.

To reset one or more security applications:

1. Click **WAN Edge** and check against a Cisco Catalyst SD-WAN device to reload the security application.
2. Click **Reset Services**.

   The **Reset Container** dialog box opens.
3. If the security application version is correct, check the check box against the version of the device.
4. Click **Reset**.

   The security application is stopped, and then restarted.

Determine Security Applications in Inoperative State

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Devices**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **Network**.
2. Choose a device by clicking its name in the **Hostname** column.

3. In the left pane, click **Real Time**.

   The real time device information appears in the right pane.

4. From the **Device Options** drop-down list, choose **App Hosting Details**.

   A table appears with the device-specific application hosting information. In the table, if the state of the device is ACTIVATED, DEPLOYED, or STOPPED, perform a reload or reset operation on the security application.

   If the state of the device is RUNNING, the security application is in an operative state.

5. From the **Device Options** drop-down list, choose **Security App Dataplane Global**.

   A table appears with the device-specific application data plane information. In the table, if the **SN Health** of the device is yellow or red, perform a reload or reset operation on the security application.

   If the **SN Health** of the device is green, the security application is in an operative state.

Reset Interfaces

Use the Interface Reset command to shutdown and then restart an interface on a device in a single operation without having to modify the device's configuration.

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. For the desired template, click **…** and choose **Reset Interface**.
3. In the **Interface Reset** dialog box, choose the desired interface.
4. Click **Reset**.

Make Your Device Invalid

You can make your device invalid should your device go beyond its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Make Device Invalid**.
3. Confirm that you want to make the device invalid and click **OK**.

Bring Your Device Back to Valid State

1. From the Cisco Catalyst SD-WAN menu, choose **Configuration** > **Certificates**.
2. Choose the invalid device and look for the **Validate** column.
3. Click **Valid**.
4. Click **Send to Controllers** to complete the action.

Stop Data Traffic

You can stop data traffic to your device should your device exceed its target location.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Stop Traffic**.
3. Confirm that you want to stop data traffic to your device and click **OK**.

Perform a Factory Reset

If your device is outside its target boundary, you may need to perform a factory reset of your device.

Note The **Factory Reset** operational command is supported only for Cisco ISR 1000 series and Catalyst 8K devices.

For more information on geofencing, see the *Cisco IOS XE Catalyst SD-WAN Systems and Interfaces Configuration Guide*.

1. From the Cisco Catalyst SD-WAN menu, choose **Tools** > **Operational Commands**.
2. For the desired device, click **…** and choose **Factory Reset**.
3. Choose one of the following options:
   - **Retain License**: Wipes all the device settings and partitions except for licenses. **Retain License** is a sub option to the factory-reset option.
   - **Full Wipe** factory-reset: Wipes all the device settings and partitions.

Note After a full-wipe operation, the device can only be booted up using a USB or TFTP.

4. Click **Reset**.

Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

Table 12: Feature History

Feature Name	Release Information	Description
Resource Monitoring on Cisco SD-WAN Controllers and Cisco vEdge Devices	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	With this feature, you can configure usage watermarks for resources such as CPU, memory, and disk on Cisco SD-WAN controllers and Cisco vEdge devices. In addition, in Cisco SD-WAN Manager servers, you can configure watermarks to monitor disk read and write speeds. Devices poll the resource usage and notify events to Cisco SD-WAN Manager. Cisco SD-WAN Manager raises alarms to alert you about changes in resource usage, or disk read or write speed so that you can take the necessary corrective action.

Information About Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

Note Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, there have been changes in how CPU utilization is calculated and reported on Cisco IOS XE Catalyst SD-WAN devices.

Before Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1: CPU utilization was calculated as an average across all CPU cores (Control Plane, Data Plane, and Service Plane).

Starting with Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1, CPU utilization is calculated and reported based solely on the control plane CPU cores. This CPU utilization can be viewed from the **System Status** option in Cisco SD-WAN Manager. See View Device System Resource Utilization in Cisco SD-WAN Manager.

Additionally, this updated CPU utilization information is also available using the **show sdwan system status** and **show processes cpu platform profile CP** CLI commands. See show sdwan system status, show processes cpu platform.

Cisco SD-WAN Release 20.7.1and Cisco vManage Release 20.7.1 introduce a Monit-utility-based workflow for monitoring the usage of the CPU, memory, and disk on Cisco SD-WAN Control Components and Cisco

vEdge devices. While Cisco SD-WAN Release 20.6.x and earlier releases, and Cisco vManage Release 20.6.x and earlier releases allowed the monitoring of how these resources are being used, the monitoring and reporting was based on predefined watermarks and a default polling interval. From Cisco SD-WAN Release 20.7.1 and Cisco vManage Release 20.7.1, you can customize the watermarks and the polling interval as appropriate to the resources in your deployment.

To monitor the usage of the CPU, memory, and disk, you can configure high-usage, medium-usage, and low-usage watermarks, and how frequently a device must check and report resource usage to Cisco SD-WAN Manager. In addition, you can monitor the disk read and write speeds on Cisco SD-WAN Manager servers by configuring appropriate read and write watermarks and the polling interval. You can use CLI templates or log in to the device CLI to configure custom watermarks and polling intervals for various devices and control components, as necessary.

Default Configuration

Devices and control components have a default configuration for the usage watermarks and the polling interval for monitoring the CPU, memory, and disk usage:

- High-usage-watermark: 90 percent
- Medium-usage-watermark: 75 percent
- Low-usage-watermark: 60 percent
- Polling interval: 5 seconds

The disk read and write speeds on Cisco SD-WAN Manager do not have a default configuration and are only monitored after you configure the necessary watermarks and polling interval.

Polling, Events, and Alarms

Based on the configuration, the device or controller polls the resource usage through monit and notifies events based on the polled usage information to Cisco SD-WAN Manager. Cisco SD-WAN Manager compares the event information with the event information received for the previous polling interval. If Cisco SD-WAN Manager detects a change in resource usage, it raises an appropriate alarm.

Devices and control components notify the following events to Cisco SD-WAN Manager:

- CPU usage
- Disk Usage
- Memory Usage
- Disk read speed (Cisco SD-WAN Manager only)
- Disk write speed (Cisco SD-WAN Manager only)

The event notifications have the following severity and status based on how the polled usage value compares with the configured watermarks:

Comparison	Severity	Status
Above the high watermark	Critical	usage-critical
Between the medium and high watermarks	Major	usage-warning
Between the low and medium watermarks	Minor	usage-notice

Below the low watermark	Minor	usage-healthy

For more information on viewing and managing events, see Events.

Based on the events, Cisco SD-WAN Manager can raise the following types of alarms:

- CPU Usage
- Disk Usage
- Memory Usage
- Disk Read Speed (Cisco SD-WAN Manager only)
- Disk Write Speed (Cisco SD-WAN Manager only)

The alarms map to the event status and severity as follows:

Alarm	Severity	Status
Critical (Red)	Critical	usage-critical
Major (Orange)	Major	usage-warning
Minor (Yellow)	Minor	usage-notice
Minor (Green)	Minor	usage-healthy

- Initially, Cisco SD-WAN Manager raises an alarm when the event status is other than usage-healthy, indicating excessive resource usage.
- If a subsequent event has the same status as the event Cisco SD-WAN Manager received previously, the alarm remains unchanged.
- If a subsequent event is of lesser severity and indicates a healthier usage status, Cisco SD-WAN Manager raises an appropriate alarm. The new alarm clears the earlier higher-severity alarm.
- Cisco SD-WAN Manager raises the Minor (Green) alarm only when the resource usage returns from a more severe state to the usage-healthy state. The Minor (Green) alarm indicates that the resource usage has returned to a normal level from an earlier excessive level.

For more information on viewing and managing alarms, see Alarms.

Supported Devices for Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices

- Cisco SD-WAN Manager server running Cisco vManage Release 20.7.1 or later
- Cisco SD-WAN Controller running Cisco SD-WAN Release 20.7.1 or later
- Cisco SD-WAN Validator running Cisco SD-WAN Release 20.7.1 or later
- Cisco vEdge devices running Cisco SD-WAN Release 20.7.1 or later

Configure Resource Monitoring on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI

You can configure the resource monitoring watermarks and polling interval using CLI commands in a CLI template.

This section provides sample CLI configurations to configure the watermarks and polling interval for resource monitoring.

Configure CPU Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage percentage
Device(config-cpu-usage)# medium-watermark-percentage percentage
Device(config-cpu-usage)# low-watermark-percentage percentage
Device(config-cpu-usage)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# cpu-usage
Device(config-cpu-usage)# high-watermark-percentage 80
Device(config-cpu-usage)# medium-watermark-percentage 70
Device(config-cpu-usage)# low-watermark-percentage 50
Device(config-cpu-usage)# interval 10
```

Configure Memory Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage percentage
Device(config-memory-usage)# medium-watermark-percentage percentage
Device(config-memory-usage)# low-watermark-percentage percentage
Device(config-memory-usage)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# memory-usage
Device(config-memory-usage)# high-watermark-percentage 80
Device(config-memory-usage)# medium-watermark-percentage 70
Device(config-memory-usage)# low-watermark-percentage 50
Device(config-memory-usage)# interval 10
```

Configure Disk Usage Watermarks and Polling Interval

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage file-system-path
Device(config-disk-usage-/opt/data)# high-watermark-percentage percentage
```

```
Device(config-disk-usage-/opt/data)# medium-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# low-watermark-percentage percentage
Device(config-disk-usage-/opt/data)# interval seconds
```

Example:

```
Device# config
Device(config)# system
Device(config-system)# alarms
Device(config-alarms)# disk-usage /opt/data
Device(config-disk-usage-/opt/data)# high-watermark-percentage 80
Device(config-disk-usage-/opt/data)# medium-watermark-percentage 70
Device(config-disk-usage-/opt/data)# low-watermark-percentage 50
Device(config-disk-usage-/opt/data)# interval 10
```

Configure Disk IO Speed Watermarks and Polling Interval on Cisco SD-WAN Manager

```
sd-wan-manager# config
sd-wan-manager(config)# system
sd-wan-manager(config-system)# alarms
sd-wan-manager(config-alarms)# disk-speed disk-partition
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps
speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps
speedsd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps speed
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval seconds
```

Example:

```
vManage# config
sd-wan-manager(config)# system
sd-wan-manager(config-system)# alarms
sd-wan-manager(config-alarms)# disk-speed /dev/nvme1n1
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-high-watermark-kBps 1000
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-medium-watermark-kBps 500
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# read-low-watermark-kBps 100
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-high-watermark-kBps 1000
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-medium-watermark-kBps 500
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# write-low-watermark-kBps 100
sd-wan-manager(config-disk-speed-/dev/nvme1n1)# interval 100
```

Verify Resource Monitoring Configuration on Cisco SD-WAN Control Components and Cisco vEdge Devices Using the CLI

Verify Configuration of CPU Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms cpu-usage** command and shows the configured CPU usage watermarks and the polling interval:

```
Device# show alarms cpu-usage

            HIGH        MEDIUM      LOW
            WATERMARK   WATERMARK   WATERMARK
CPU USAGE   PERCENTAGE  PERCENTAGE  PERCENTAGE  INTERVAL
-------------------------------------------------------------------
cpu-usage   80          70          50          10
```

Verify Configuration of Memory Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms memory-usage** command and shows the configured memory usage watermarks and the polling interval:

```
Device# show alarms memory-usage

              HIGH         MEDIUM       LOW
              WATERMARK    WATERMARK    WATERMARK
MEMORY USAGE  PERCENTAGE   PERCENTAGE   PERCENTAGE   INTERVAL
-----------------------------------------------------------------
memory-usage  80           70           50           10
```

Verify Configuration of Disk Usage Watermarks and Polling Interval

The following is a sample output of the **show alarms disk-usage** command and shows the configured disk usage watermarks and the polling interval:

```
Device# show alarms disk-usage

             HIGH          MEDIUM        LOW
FILESYSTEM   WATERMARK     WATERMARK     WATERMARK
PATH         PERCENTAGE    PERCENTAGE    PERCENTAGE   INTERVAL
-----------------------------------------------------------------
/rootfs.rw    90            75            60           5
/tmp          90            75            60           5
/opt/data     80            70            50           10
```

Verify Configuration of Disk IO Speed Watermarks and Polling Interval

The following is a sample output of the **show alarms disk-speed** command and shows the configured disk IO speed watermarks and the polling interval:

```
sd-wan-manage# show alarms disk-speed

                      READ                    WRITE       WRITE
            READ HIGH MEDIUM      READ LOW    HIGH        MEDIUM      WRITE LOW
            WATERMARK WATERMARK   WATERMARK   WATERMARK   WATERMARK   WATERMARK
DISK PATH   K BPS     K BPS       K BPS       K BPS       K BPS       K BPS       INTERVAL
-------------------------------------------------------------------------------------------
/dev/sda2   1000      500         100         1000        500         100         100
```

View Event Notifications on a Device

The following is a sample output of the **show notification stream viptela** command and shows a CPU usage event:

```
sd-wan-manager# show notification stream viptela
notification
 eventTime 2021-09-08T02:57:14.91578+00:00
 cpu-usage
  severity-level minor
  host-name vm12
  system-ip 172.16.255.22
  cpu-status usage-notice
  warning System CPU usage is above 50%
  cpu-user-percentage 40.9
  cpu-system-percentage 10.6
  cpu-idle-percentage 48.50
 !
!
```