



Troubleshooting

- [Alarms, on page 1](#)
- [Capture Packets, on page 6](#)
- [Packet Capture for Cloud onRamp Colocation Clusters, on page 7](#)
- [Check Traffic Health, on page 9](#)
- [Collect System Information Using Admin Tech, on page 10](#)
- [Configure Packet Trace, on page 11](#)
- [Configure SNMP Traps on Cisco vEdge Devices, on page 12](#)
- [Events, on page 14](#)
- [On-Demand Troubleshooting, on page 16](#)
- [Simulate Flows, on page 21](#)
- [Syslog Messages, on page 22](#)
- [Syslog Messages, on page 24](#)
- [Troubleshoot a Device, on page 62](#)
- [Troubleshoot Common Cellular Interface Issues, on page 62](#)
- [Troubleshoot WiFi Connections, on page 65](#)
- [View Audit Log Information, on page 69](#)
- [View and Monitor Cellular Interfaces, on page 70](#)
- [View Real Time Monitoring Options, on page 72](#)
- [View TCP Optimization Information, on page 74](#)
- [View TLOC Loss, Latency, and Jitter Information, on page 75](#)

Alarms

When something of interest happens on an individual device in the overlay network, the device reports it by sending a notification to Cisco vManage. Cisco vManage then filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.

For a list of alarms that Cisco vManage generates, see [Permanent Alarms and Alarm Fields](#).

Use the Alarms screen to display detailed information about alarms generated by controllers and routers in the overlay network.

Alarm States

Cisco vManage alarms are assigned a state based on their severity:

- Critical (red)—Serious events that impair or shut down the operation of an overlay network function.
- Major (yellow)—Serious events that affect, but do not shut down, the operational of a network function.
- Medium (blue)—Events that might impair the performance of a network function.
- Minor (green)—Events that might diminish the performance of a network function.

The alarms listed as Active generally have a severity of either critical or major.

When the notification events that Cisco vManage receives indicate that the alarm condition has passed, most alarms clear themselves automatically. Cisco vManage then lists the alarm as Cleared, and the alarm state generally changes to medium or minor.

Changes to Alarms in Cisco vManage Release 20.5.1

Table 1: Feature History

Feature	Release Information	Description
Optimization of Alarms	Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature optimizes the alarms on Cisco vManage by automatically suppressing redundant alarms. This allows you to easily identify the component that is causing issues. You can view these alarms from the Cisco vManage menu, choose Monitor > Logs > Alarms .

When a site is down, Cisco vManage reports the following alarms:

- Site down
- Node down
- TLOC down

Cisco vManage displays alarms for each component that is down. Depending on the size of your site, you may see several redundant alarms such as alarms for each TLOC in a node as well as the node alarm. In Cisco vManage Release 20.5.1, Cisco vManage intelligently suppresses redundant alarms. For example, if all the TLOCs in a node are down, Cisco vManage suppresses the alarms from each TLOC and displays only the alarm from the node. For multitenant configurations, each tenant displays alarms for the sites in its tenancy.

Scenario	Alarms Displayed	
Cisco vManage Release 20.5.1	Previous Releases	bfd-tloc-1_down
Link 1 down Link 2 up.	bfd-tloc-1_down	

Scenario	Alarms Displayed	
Link 1 down Link 2 down	bfd-site-1_down bfd-node-1_down, bfd-tloc-1_down, and bfd-tloc-2_down are suppressed by the site alarm.	bfd-site-1_down bfd-tloc-1_down
Link 1 up Link 2 down	bfd-site-1_up bfd-node-1_up bfd-tloc-1_up bfd-tloc-2_up	bfd-site-1_up bfd-tloc-1_up

View Alarms

You can view alarms from the Cisco vManage Dashboard by clicking the Alarm Bell icon in the top bar. In the Alarm Bell, the alarms are grouped into Active or Cleared.

Alternatively, follow these steps to view alarms from the Alarms screen in Cisco vManage.

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.

From the Cisco vManage menu, choose **Monitor > Alarms**.

The alarms are displayed in graphical and tabular formats.

2. To view more details for a specific alarm, click **...** for the desired alarm, and then click **Alarm Details**.

The Alarm Details window opens and displays the probable cause of the alarm, impacted entities, and other details.

Set Alarm Filters

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.

From the Cisco vManage menu, choose **Monitor > Alarms**.

2. Click **Filter**.

3. In the **Severity** field, choose an alarm severity level from the drop-down list. You can specify more than one severity level.

4. In the **Active** field, choose active, cleared, or both types of alarm from the drop-down list. Active alarms are alarms that are currently on the device but have not been acknowledged.

5. In the **Alarm Name** field, choose an alarm name from the drop-down list. You can specify more than one alarm name.

6. Click **Search** to look for alarms that match the filter criteria.

Cisco vManage displays the alarms in both table and graphical formats.

Export Alarm Data in CSV Format

To export data for all alarms to a file in CSV format, click the **Download** icon.

Cisco vManage downloads all data from the alarms table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named Alarms.csv.

Alarms data displayed on the graph can also be looked up in the Excel file.

For example, if the graph displays an alarm data (Critical 2, Major 274, Medium 4, Minor 405) with date and time as 15/Feb/2022 3:30 AM, the same alarm data is also available in the Excel file against a date and time range between 15/Feb/2022 3:00 AM and 15/Feb/2022 3:29 AM.

Enable Email Notifications

You can configure Cisco vManage to send email notifications when alarms occur on devices in the overlay network. This requires you to first configure SMTP and email recipient parameters. First configure the SMTP and email recipient parameters on this screen:

1. From the Cisco vManage menu, choose **Administration > Settings**.
2. Click **Edit** next to the **Alarm Notifications** option.
3. For **Enable Email Notifications**, choose **Enabled**.
4. Check the **Email Settings** check box.
5. Choose the security level for sending the email notifications. The security level can be **None**, **SSL**, or **TLS**.
6. In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.
7. In the **SMTP Port** field, enter the SMTP port number. For no security, the default port is 25; for SSL it is 465; and for TLS it is 587.
8. In the **From address** field, enter the full email address to include as the sender in email notifications.
9. In the **Reply to address** field, enter the full email address to include in the Reply-To field of the email. This address can be a noreply address, such as noreply@cisco.com.
10. Check the **Use SMTP Authentication** check box to enable SMTP authentication to the SMTP server.
Enter the username and password to use for SMTP authentication. The default user email suffix is appended to the username. The password that you type is hidden.
11. Click **Save**.



Note The email is sent from vManage Public-IP of VPN0 (Transport Interface) as a source interface.

Send Alarm Notifications

Before you begin: Ensure that Email Notifications are enabled under **Administration > Settings**. Click **Edit** next to **Alarm Notifications** to check whether **Alarm Notifications** are enabled and the **Email Settings** check box is checked.

To send email notifications when alarms occur:

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.
From the Cisco vManage menu, choose **Monitor > Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. Click **Add Alarm Notification**.
4. In the **Name** field, enter a name for the email notification. The name can be up to 128 characters and can contain only alphanumeric characters.
5. In the **Severity** field, choose one or more alarm severity levels from the drop-down list.
6. In the **Alarm Name** field, choose one or more alarms.
7. In the **Account Details** are, enter the following:
 - a. In the **Email** field, enter one or more email addresses.
 - b. (Optional) Click **Add New Email List** and enter an email list, if desired.
 - c. In the **Email Threshold** field, set the maximum number of emails to be sent per minute. The number can be a value from 1 through 30. The default is 5.
 - d. Check the **WebHook** check box to trigger an HTTP callback when an alarm notification event occurs:
 1. In the **WebHook URL** field, enter the URL of the webhook server.
 2. Enter the **Username** and **Password** to authenticate the webhook server.
 3. In the **WebHook Threshold** field, enter the threshold value.



Note The value you enter indicates the number of notifications to be posted for that webhook URL per minute. For example, if **WebHook Threshold** equals 2, you receive two notifications for that webhook URL per minute. Notifications that are generated beyond the threshold get dropped.

8. Under **Selected Devices**, choose **All Devices** or **Custom**.
If you choose **Custom**, a device list is displayed:
 - a. In the **Available Devices** list on the left, choose one or more devices.
 - b. Click the right arrow to move the devices to the **Selected Devices** list on the right.
 - c. Click **Add**.
9. Click **Add**.

View and Edit Email Notification

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.
From the Cisco vManage menu, choose **Monitor > Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.

3. For the desired notification, click the **View** icon to the right of the row.
4. When you are done viewing the notification, click **OK**.

Edit an Email Notification

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.
From the Cisco vManage menu, choose **Monitor > Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. For the desired email notification, click the **Edit** icon.
4. When you are done editing the notification, click **Update**.

Delete an Email Notification

1. From the Cisco vManage menu, choose **Monitor > Logs > Alarms**.
From the Cisco vManage menu, choose **Monitor > Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. For the desired email notification, click the **Trash Bin** icon.
4. In the confirmation dialog box, click **OK**.

Capture Packets

Table 2: Feature History

Feature Name	Release Information	Description
Embedded Packet Capture	Cisco IOS XE Release 17.3.1a Cisco vManage Release 20.3.1	This feature is an onboard packet capture facility that allows network administrators to capture packets flowing to, through, and from the device. The administrator can manage to analyze these packets locally or save and export them for offline analysis through Cisco vManage. This feature gathers information about the packet format and therefore helps in application analysis, security, and troubleshooting.
Embedded Packet Capture for Cisco vEdge Devices Using CLI Commands	Cisco SD-WAN Release 20.6.1	This feature provides an alternative method to capture traffic data to troubleshoot connectivity issues between Cisco vEdge devices and Cisco vManage using supported CLI commands. As part of this feature, the following commands are introduced to capture traffic details: request stream capture show packet-capture

Feature Name	Release Information	Description
Bidirectional Packet Capture for Cisco IOS XE SD-WAN Devices	Cisco IOS XE Release 17.7.1a Cisco vManage Release 20.7.1	You can now enable the Bidirectional option using Cisco vManage to capture bidirectional packets.
IPv6 Support for Bidirectional Packet Capture	Cisco IOS XE Release 17.9.1a	This feature adds support for bidirectional capture of IPv6 traffic data to troubleshoot connectivity issues using a CLI template.

Packet Capture for Cloud onRamp Colocation Clusters

Table 3: Feature History

Feature Name	Release Information	Description
Packet Capture for Cloud onRamp Colocation Clusters	Cisco SD-WAN Release 20.7.1 Cisco vManage Release 20.7.1	You can now capture packets at either the physical network interface card (PNIC) level or the virtual network interface card (VNIC) level on a Cloud Services Platform (CSP) device of a colocation cluster. To do this, you need to choose a PNIC or VNIC on the Cisco vManage interface and set the required traffic filters.

You can capture packets flowing to, through, and from a CSP device of a colocation cluster. You can capture packets at either the PNIC or the VNIC level on the CSP device.

Supported Ports for Packet Capture for Cloud onRamp Colocation Clusters

Packet capture is supported for the following ports:

Table 4: Supported Ports for Packet Capture

Mode	VNIC Level	PNIC Level
Single Tenancy	OVS-DPDK, HA-OVS-DPDK, SR-IOV, OVS-MGMT	SR-IOV, MGMT
Multitenancy (Role-Based Access Control)	OVS-DPDK, HA-OVS-DPDK, OVS-MGMT	MGMT

Enable Packet Capture on Cisco vManage

Enable the packet capture feature on Cisco vManage before capturing packets at the PNIC or VNIC level on a CSP device of a colocation cluster:

1. From the Cisco vManage menu, choose **Administration > Settings**.
2. In **Data Stream**, choose **Enabled**.

Capture Packets at PNIC Level

1. From the Cisco vManage menu, choose **Monitor > Devices**.
2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. In the left pane, click **Packet Capture**.
5. From the **PNIC ID** drop-down list, choose a PNIC.
6. (Optional) Click **Traffic Filter** to filter the packets that you want to capture based on the values in their IP headers.

Table 5: Packet Capture Filters

Field	Description
Source IP	Source IP address of the packet.
Source Port	Source port number of the packet.
Protocol	Protocol ID of the packet. The supported protocols are: ICMP, IGMP, TCP, UDP, ESP, AH, ICMP Version 6 (ICMPv6), IGRP, PIM, and VRRP.
Destination IP	Destination IP address of the packet.
Destination Port	Destination port number of the packet.

7. Click **Start**.
The packet capture begins, and its progress is displayed:
 - Packet Capture in Progress: Packet capture stops after the file size reaches 20 MB, or 5 minutes after you started packet capture, or when you click **Stop**.
 - Preparing file to download: Cisco vManage creates a file in libpcap format (a .pcap file).
 - File ready, click to download the file: Click the download icon to download the generated file.

Capture Packets at VNIC Level

1. From the Cisco vManage menu, choose **Monitor > Devices**.
2. Click **Colocation Cluster**, and choose a cluster.
3. From the list of devices that is displayed, click a CSP device name.
4. Choose a VNF, and then click **Packet Capture** in the left pane.

5. Alternatively, choose **Monitor > Devices > Colocation Cluster**. Next, choose a cluster and click **Network Functions**, choose a VNF, and then click **Packet Capture** in the left pane.
6. From the **VNIC ID** drop-down list, choose a VNIC.
7. (Optional) Click **Traffic Filter** to filter the packets to capture based on values in their IP headers. For more information on these filters, see the above section.
8. Click **Start**. The packet capture begins, and displays its progress.

Check Traffic Health

View Tunnel Health

To view the health of a tunnel from both directions:

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. To choose a device, click the device name under the **Hostname** column.
3. Click **Troubleshooting** in the left pane.
4. In the **Traffic** area, click **Tunnel Health**.
5. From the **Local Circuit** drop-down list, choose a source TLOC.
6. From the **Remote Device** drop-down list, choose a remote device.
7. From the **Remote Circuit** drop-down list, choose a destination TLOC.
8. Click **Go**. The lower part of the screen displays:
9. From the Chart Options drop-down list, choose one of these: Loss Percentage, Latency/Jitter, Octets.
10. (Optional) Choose a predefined or a custom time period on the left to view data for the specified time period.

The window displays:

- App-route data (either loss, latency, or jitter) in graphical format for all tunnels between the two devices in each direction.
- App-route graph legend—Identifies selected tunnels from both directions.

Check Application-Aware Routing Traffic

To check application-aware routing traffic from the source device to the destination device:

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. Choose a device from the list of devices that appears.
3. Click **Troubleshooting** in the left pane.

4. In the right pane, click **App Route Visualization** under **Traffic**.
5. From the **Remote Device** drop-down list, choose a destination device.
6. (Optional) Click **Traffic Filter**. Choose **No Filter** or **SAIE**. **No Filter** is chosen by default.



Note In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.

7. Click **Go**. The lower part of the screen displays:
8. From the Chart Options drop-down list, choose one of these: Loss Percentage, Latency/Jitter, Octets.
9. (Optional) Choose a predefined or a custom time period on the left to view data for the specified time period.

Collect System Information Using Admin Tech

Table 6: Feature History

Feature Name	Release Information	Description
Admin-Tech Enhancements	Cisco SD-WAN Release 20.1.1	This feature enhances the admin-tech file to include show tech-support memory , show policy-firewall stats platform , and show sdwan confd-log netconf-trace commands in the admin-tech logs. The admin-tech tar file includes memory, platform, and operation details.
Generate System Status Information for a Cisco vManage Cluster Using Admin Tech	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 vManage cluster. The admin-tech file is a collection of system status information intended for use by Cisco SD-WAN Technical Support for troubleshooting. Prior to this feature, Cisco SD-WAN was only able to generate an admin-tech file for a single device.

Send the `admin-tech.tar.gz` file to Cisco SD-WAN Technical Support for analysis and resolution of the issue.



Note All in-progress admin-tech requests are purged every three hours.

1. From the Cisco vManage menu, choose **Tools > Operational Commands**.
2. For the desired device, click **...** and choose **Generate Admin Tech** from the options.
3. In the **Generate admin-tech File** window, choose the information to include in the admin-tech file if desired:

- a. The **Include Logs** check box is checked by default. Uncheck this check box if you do not want to include the log files in the admin-tech file.



Note The log files are stored in the /var/log/directory on the local device.

- b. Check the **Include Cores** check box to include any core files.



Note Core files are stored in the /var/crash directory on the local device.

- c. Check the **Include Tech** check box to include any files related to device processes (daemons), memory detail, and operations.



Note The log files are stored in the /var/tech directory on the local device.

4. Click **Generate**.

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

Configure Packet Trace

Table 7: Feature History

Feature Name	Release Information	Description
Bidirectional Support for Packet Tracing	Cisco IOS XE Release 17.8.1a Cisco SD-WAN Release 20.8.1 Cisco vManage Release 20.8.1	You can configure packet tracing on edge devices.

Use the **debug platform packet-trace** command to configure a packet tracer on edge devices with various conditions such as bidirectional, VPN, circular, destination IP, source IP, interface, start, stop, logging, and clear.

Configure Packet Trace on Cisco IOS XE SD-WAN devices

1. Enable packet trace for the traffic and specify the maximum number of packets:

```
Device# debug platform packet-trace packet [number of traced packets]
```

2. Specify the matching criteria for tracing packets. Matching criteria provides the ability to filter by protocol, IP address and subnet mask, interface, and direction:

```
Device# debug platform condition [interface interface name] {match ipv4|ipv6|mac src dst} {both|ingress|egress} [bidirectional]
```

3. Enable the specified matching criteria and start packet tracing:

```
Device# debug platform condition start
```

4. Deactivate the condition and stop packet tracing:

```
Device# debug platform condition stop
```

5. Exit the privileged EXEC mode:

```
exit
```

Configure Packet Trace on Cisco vEdge devices

The following example shows how to configure conditions for packet tracing:

```
Device# debug packet-trace condition source-ip 10.1.1.1
Device# debug packet-trace condition vpn-id 0
Device# debug packet-trace condition interface ge0/1
Device# debug packet-trace condition stop
```

For more information, see [debug packet-trace condition](#) command page.

Configure SNMP Traps on Cisco vEdge Devices

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

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



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

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



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

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

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

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



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

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

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

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

In the **community-name** command, associate a previously configured 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 ul
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)#

```

Events

Use the Events screen to display detailed information on events generated by Cisco SD-WAN devices.

Set Event Filters

To set filters for searching events generated on one or more Cisco SD-WAN devices:

1. From the Cisco vManage menu, choose **Monitor > Logs > Events**.

From the Cisco vManage menu, choose **Monitor > Events**.

2. Click the **Filter**.
3. In the **Severity** field, choose the even severity level from the drop-down list.

Events generated by Cisco SD-WAN devices are collected by Cisco vManage and classified as:

- **Critical**—indicates that action needs to be taken immediately.
- **Major**—indicates that the problem needs to be looked into but is not critical enough to bring down the network.
- **Minor**—is informational only.

You can specify more than one severity level.

1. In the **Component** field, from the drop-down list, choose one or more configuration components that caused the event.
2. In the **System IP** field, choose the system IP of the devices, for which to view generated events, from the drop-down list.

3. In the **Event Name** field, choose the event name, for which to view generated events, from the drop-down list. You can choose more than one event name.
4. Click **Search** to search events that match the filter criteria.

Cisco vManage displays the events both in table and graphical format.

Export Event Data in CSV Format

To export data for all events to a file in CSV format, click the **Download** icon.

Cisco vManage downloads all data from the events table to an Excel file in CSV format. The file is downloaded to your browser's default download location and is named Events.csv.

View Device Details

To view detailed information about a device on which an event was generated:

1. From the Cisco vManage menu, choose **Monitor > Logs > Events**.

From the Cisco vManage menu, choose **Monitor > Events**.

The window displays events in both graphical and table format.

2. To view detailed information about any event generated on a device, choose the event row from the table.
3. For the desired device, click ... and choose **Device Details**.

The **Device Details** dialog box opens, displaying the hostname of the device originating the event and other details.

Using the CLI

If using the CLI to view information about a device on which an event was generated, for Cisco vEdge devices, you can use the **show notification stream viptela** command. Here is an example of the command output. The first line of the output shows the time when the message was generated (the SNMP eventTime). The time is shown in UTC format, not in the device's local time. The second line of the notification contains a description of the event, and the third line indicates the severity level.

```
vEdge# show notification stream viptela
notification
eventTime 2015-04-17T14:39:41.687272+00:00
bfd-state-change
severity-level major
host-name vEdge
system-ip 1.1.4.2
src-ip 192.168.1.4
dst-ip 108.200.52.250
proto ipsec
src-port 12346
dst-port 12406
local-system-ip 1.1.4.2
local-color default
remote-system-ip 1.1.9.1
remote-color default
new-state down
!
!
notification
eventTime 2015-04-17T15:12:20.435831+00:00
tunnel-ipsec-rekey
```

```

severity-level minor
host-name vEdge
system-ip 1.1.4.2
color default
!
!
notification
eventTime 2015-04-17T16:56:50.314986+00:00
system-login-change
severity-level minor
host-name vEdge
system-ip 1.1.4.2
user-name admin
user-id 9890
!

```

On-Demand Troubleshooting

Table 8: Feature History

Feature Name	Release Information	Description
On-Demand Troubleshooting	Cisco IOS XE Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	You can view detailed information about the flow of traffic from a device, and use this information to assist with troubleshooting.

Information About On-Demand Troubleshooting

On-demand troubleshooting lets you view detailed information about the flow of traffic from a device.

By default, Cisco vManage captures aggregated information about flows. You can obtain detailed information for specific devices and for specific historical time periods by adding an on-demand troubleshooting entry. When you add an entry, Cisco vManage compiles detailed information according to parameters that you configure.

To conserve system resources, Cisco vManage compiles detailed information only when you request it by adding an entry. In addition, Cisco vManage stores the information for a limited time (3 hours by default), then removes it. You can request the same information again, if needed.

Restrictions for On-Demand Troubleshooting

Ensure that no Cisco or third-party APIs that instruct on-demand troubleshooting to stop are called when you are using on-demand troubleshooting. These APIs prevent on-demand troubleshooting from compiling information.

Page Elements

The **On Demand Troubleshooting** window provides options for configuring and adding an on-demand troubleshooting entry. The **On Demand Troubleshooting** window displays information about existing on-demand troubleshooting entries and provides the following information and options.

Item (Field)	Description
ID	System-assigned identifier of the entry.
Device ID	System IP of the device to which the entry applies.
Data Type	Type of data for which the entry provides detailed information.
Creation Time	Date and time that you added the entry.
Expiration Time	Date and time that the entry expires. At this expiration time, the entry is removed from the table automatically, and the corresponding detailed information is no longer available. By default, an entry is removed 3 hours after its creation time.
Data Backfill Start Time	Start date and time of the data backfill period.
Data Backfill End Time	End date and time of the data backfill period.
Status	Status of the entry: <ul style="list-style-type: none"> • IN_PROGRESS: Detailed troubleshooting information is in the process of being compiled. • QUEUED: Detailed troubleshooting information is queued for compilation. • COMPLETED: Detailed troubleshooting information has been compiled.

Configure On-Demand Troubleshooting

You can configure on-demand troubleshooting for a device from the **Tools > On Demand Troubleshooting** window in Cisco vManage. This window provides options for adding an on-demand troubleshooting entry, and for managing existing entries.

Cisco vManage Release 20.6.x and earlier: You can configure on-demand troubleshooting for a device from the **Monitor > On Demand Troubleshooting** window in Cisco vManage.

You can also start on-demand troubleshooting from various locations in the **Monitor > Devices** window for a device. See [View On-Demand Troubleshooting Information for a Device, on page 19](#).

Cisco vManage Release 20.6.x and earlier: You can start on-demand troubleshooting from various locations in the **Monitor > Network** window for a device.

On-demand troubleshooting is qualified for troubleshooting entries for up to 10 devices concurrently.

Add an On-Demand Troubleshooting Entry

Adding an entry in the **On Demand Troubleshooting** window instructs Cisco vManage to compile detailed troubleshooting information for the device that you specify, using the parameters that you configure.

To add an on-demand troubleshooting entry, follow these steps:

1. From the Cisco vManage menu, choose **Tools > On Demand Troubleshooting**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > On Demand Troubleshooting**.
2. From the **Select Device** drop-down list, choose the Cisco IOS XE SD-WAN device or the Cisco vEdge device for which you want to enable on-demand troubleshooting.
3. From the **Select Data Type** drop-down list, choose **SAIE** or **ConnectionEvents**.
4. Choose an option for the data backfill period:
 - **Last 1 hour**: Provides detailed stream information for the period beginning 1 hour before you add the troubleshooting entry and ending at the time that you add the entry.
 - **Last 3 hours**: Provides detailed stream information for the period beginning 3 hours before you add the troubleshooting entry and ending at the time that you add the entry.
 - **Custom Date and Time Range**: Use the **Start date and time** and the **End date and time** fields to designate the backfill period that you want. Note that the **End date and time** value cannot be later than the current date and time.

5. Click **Add**.

The troubleshooting entry appears in the table of entries. When the value in the **Status** field for the entry shows the value **Completed**, you can view the troubleshooting information from the **Monitor > Devices** window, as described in [View On-Demand Troubleshooting Information for a Device, on page 19](#).

Update an On-Demand Troubleshooting Entry

Update an on-demand troubleshooting entry to make changes to its configuration settings. For example, update an entry to adjust its backfill period.

Only entries that are in the QUEUED state can be updated.

To update an on-demand troubleshooting entry, follow these steps:

1. From the Cisco vManage menu, choose **Tools > On Demand Troubleshooting**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > On Demand Troubleshooting**.
2. In the table of entries, click ... adjacent to the entry that you want to update and choose **Update**.
3. In the **Update Troubleshoot Status** dialog box that is displayed, configure the settings as needed, and click **Add**.

Delete an On-Demand Troubleshooting Entry

Deleting an on-demand troubleshooting entry removes the entry from Cisco vManage. After you delete an entry, you can no longer view its detailed information.

Deleting an entry can help free resources in Cisco vManage.

To delete an on-demand troubleshooting entry, follow these steps:

1. From the Cisco vManage menu, choose **Tools > On Demand Troubleshooting**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > On Demand Troubleshooting**.

2. In the table of entries, click ... adjacent to the entry that you want to delete and choose **Delete on demand queue**.
3. In the **Delete On Demand Status** window that is displayed, click **OK**.

View On-Demand Troubleshooting Information for a Device

You can view on-demand troubleshooting information for a device from the **Network** window for that device.

Before you can view this information, at least one on-demand troubleshooting entry must exist for the device. Add an entry from the **On Demand Troubleshooting** window as described in [Add an On Demand Troubleshooting Entry](#), or add an entry from the **Network** window as described in the following procedure.

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. In the **Hostname** column, click the device for which you want to view the information.
3. Perform either of these actions:
 - To view the troubleshooting information for an SAIE application:
 - a. Click **SAIE Applications**.



Note In Cisco vManage Release 20.7.x and earlier releases, **SAIE Applications** is called **DPI Applications**.

- b. In the **Applications Family** table, click an application family.
 - c. In the **Applications** table, click an application.
- To view troubleshooting information for a specific metric, in the left pane, under **ON-DEMAND TROUBLESHOOTING** click an option. Not all options apply to all device types.
 - **FEC Recovery Rate**
 - **SSL Proxy**
 - **AppQoe TCP Optimization**
 - **AppQoE DRE Optimization**
 - **WAN Throughput**
 - **Flows**
 - **Top Talkers**

If on-demand troubleshooting is configured for the device, detailed troubleshooting information appears. This information includes traffic statistics and metrics such as source IP address, destination IP address, number of packets, number of bytes, and more. Use the options that are available and hover your cursor over elements on the graphs to view the information that you need.



Note Starting from Cisco IOS XE Release 17.9.1a, use the **policy ip visibility features enable** command to manually enable or disable the feature fields in Flexible Netflow (FNF). Use the **show sdwan policy cflowd-upgrade-status** command to check which features were enabled before the version upgrade. You have to manually control the features after a version upgrade using the disable or enable commands. For more information, see policy ip visibility command page.

If on-demand troubleshooting information is not configured, the **Enable On Demand Troubleshooting** option is displayed. Continue to Step 4.

4. If the **Enable On Demand Troubleshooting** option is displayed, perform these actions to start this feature for the selected device:
 - a. Click **Enable On Demand Troubleshooting**.
 - b. Choose one of the following options:
 - **Quick Enable:** Starts an on-demand troubleshooting entry with a backfill period of 3 hours. With this option, detailed stream information for the past 3 hours becomes available.

After you choose this option, click **Refresh** to view the detailed troubleshooting information. It can take a few minutes for this information to become available. Alternatively, click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window that includes the entry that you just added.
 - **Go to On Demand Troubleshooting:** Displays the **On Demand Troubleshooting** window. Add an entry in this window as described in [Add an On Demand Troubleshooting Entry](#). Repeat Steps 1 to Step 3 in this procedure to view the detailed information.

View Detailed Top Source Data

After on-demand troubleshooting is configured, you can view detailed information about top application usage for a device. To do so, follow these steps:

1. From the Cisco vManage menu, choose **Monitor > Overview > Top Applications**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Dashboard > Main Dashboard > Top Applications**.
2. In the **SAIE Application** tab, click an application usage bar in the chart.



Note In Cisco vManage Release 20.7.x and earlier releases, **SAIE Application** is called **DPI Application**.

3. In the chart for the application that you selected, click the device usage bar.

If on-demand troubleshooting is configured for the device, detailed top source data appears.

If on-demand troubleshooting information is not configured, the **Go to On Demand Troubleshooting** option appears. Continue to Step 4.
4. If the **Go to On Demand Troubleshooting** option appears, perform these actions:

- a. Click **Go to On Demand Troubleshooting** to display the **On Demand Troubleshooting** window.
- b. In the **On Demand Troubleshooting** window, add an entry, as described in [Add an On Demand Troubleshooting Entry](#).
- c. Repeat Step 1 to Step 3 in this procedure to view the detailed information.

Simulate Flows

Table 9: Feature History

Feature Name	Release Information	Description
Forwarding Serviceability		This feature enables service path and tunnel path under Simulate Flows function in the Cisco vManage template and displays the next-hop information for an IP packet. This feature enables Speed Test and Simulate Flow functions on the Cisco IOS XE SD-WAN devices.

To view the next-hop information for an IP packet available on routers:

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. Choose a device from the list of devices that appears.
3. Click **Troubleshooting** in the left pane.
4. Under **Traffic**, click **Simulate Flows**.
5. To specify the data traffic path, choose values or enter data in the required fields:
 - VPN—VPN in which the data tunnel is located.
 - Source/Interface—Interface from which the cflowd flow originates.
 - Source IP—IP address from which the cflowd flow originates.
 - Destination IP—Destination IP address of the cflowd flow.
 - Application—Application running on the router.
 - Custom Application (created in CLI)
6. Click **Advanced Options**.
 - a. In the **Path** field, choose **Tunnel** or **Service** to indicate whether the data traffic path information comes from the service side of the router or from the tunnel side.
 - b. In the **Protocol** field, enter the protocol number.
 - c. In the **Source Port** field, enter the port from which the cflowd flow originates.
 - d. In the **Destination Port** field, enter the destination port of the cflowd flow.

- e. In the **DSCP** field, enter the DSCP value in the cflowd packets.
 - f. (Optional) Check the **All Paths** check box to view all possible paths for a packet.
7. Click **Simulate** to determine the next hop that a packet with the specified headers would take.

For service path and tunnel path commands, see [show sdwan policy service-path](#) and [show sdwan policy tunnel-path](#).

Syslog Messages

When something of interest happens on an individual device in the overlay network, one of the ways the device reports it is by generating a system logging (syslog) message and place it in a syslog file in the /var/log directory on the local device and, if configured, on a remote device.

On Cisco SD-WAN devices, you can log event notification system log (syslog) messages to files on the local device or on a remote host, or both. On the local device, syslog files are placed in the /var/log directory.

Configure System Logging

Logging syslog messages with a priority level of "error," to the local device's hard disk, is enabled by default. Log files are placed in the local /var/log directory. By default, log files are 10 MB in size, and up to 10 files are stored. After 10 files have been created, the oldest one is discarded to create a file for newer syslog messages.

To modify the default syslog parameters from Cisco vManage, use the Logging feature template. From the CLI, include the **logging disk** or **logging server** commands in the device configuration.

View Syslog Logging Information

1. From the Cisco vManage menu, choose **Administration > Settings** and, ensure that **Data Stream** is enabled.
2. From the Cisco vManage menu, choose **Monitor > Devices**, and choose a device from the list of devices that appears.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**, and choose a device from the list of devices that appears.
3. Click **Troubleshooting** in the left pane.
4. In the **Logs** area, click **Debug Log**.
5. In the **Log Files** field, choose the name of the log file. The lower part of the screen displays the log information.

To view the contents of a syslog file from the CLI, use the **show log** command. For example:

```
Device# show log auth.log tail 10==> /var/log/auth.log <==auth.info: Nov 14 14:33:35 vedge
  sshd[2570]: Accepted publickey for admin from 10.0.1.1 port 39966 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 14 14:39:42 vedge sshd[2578]:
  Received disconnect from 10.0.1.1 port 39966:11: disconnected by userauth.info: Nov 14
14:39:42 vedge sshd[2578]: Disconnected from 10.0.1.1 port 39966auth.info: Nov 16 10:51:45
  vedge sshd[6106]: Accepted publickey for admin from 10.0.1.1 port 40012 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.info: Nov 16 11:21:55 vedge sshd[6108]:
  Received disconnect from 10.0.1.1 port 40012:11: disconnected by userauth.info: Nov 16
```

```
11:21:55 vedge sshd[6108]: Disconnected from 10.0.1.1 port 40012auth.info: Nov 17 12:59:52
vedge sshd[15889]: Accepted publickey for admin from 10.0.1.1 port 40038 ssh2: RSA
SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrIlsauth.info: Nov 17 13:45:13 vedge
sshd[15894]: Received disconnect from 10.0.1.1 port 40038:11: disconnected by userauth.info:
Nov 17 13:45:13 vedge sshd[15894]: Disconnected from 10.0.1.1 port 40038auth.info: Nov 17
14:47:31 vedge sshd[30883]: Accepted publickey for admin from 10.0.1.1 port 40040 ssh2:
RSA SHA256:pkFQ5wE//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrIls
```

To view the configured system logging settings for a device, use the **show logging** command from the CLI. For example:

```
Device# show logging
System logging to host in vpn 0 is disabled
Priority for host logging is set to: emerg

System logging to disk is disabled
Priority for disk logging is set to: err
File name for disk logging is set to: /var/log/vsyslog
File size for disk logging is set to: 10 MB
File recycle count for disk logging is set to: 10

Syslog facility is set to: all facilities
```

System Log Files

Syslog messages at or above the default or configured priority value are recorded in a number of files in the `/var/log` directory on the local device. These files include the following:

- `auth.log`—Login, logout, and superuser access events, and usage of authorization systems.
- `kern.log`—Kernel messages
- `messages`—Consolidated log file that contains syslog messages from all sources
- `vconfd`—All configuration-related syslog messages
- `vdebug`—All debug messages for modules whose debugging is turned on and all syslog messages above the configured priority value. Debug logging supports various levels of logging based on the module. Different modules implement the logging levels differently. For example, the system manager (`sysmgr`) has two logging levels (on and off), while the chassis manager (`chmgr`) has four different logging levels (off, low, normal, and high). You cannot send debug messages to a remote host. To enable debugging, use the **debug** operational command
- `vsyslog`—All syslog messages from Cisco SD-WAN processes (daemons) above the configured priority value. The default priority value is "informational" (severity level 6), so by default, all "notice", "warning", "error", "critical", "alert", and "emergency" syslog messages (severity levels 5 through 0, respectively) are saved

The Cisco SD-WAN software does not use the following standard LINUX files, which are present in `/var/log`, for logging: `cron.log`, `debug`, `lpr.log`, `mail.log`, and `syslog`.

The writing of messages to syslog files is not rate-limited. This means that if many syslog messages are generated in a short amount of time, the overflow messages are buffered and placed in a queue until they can be written to a syslog file. The overflow messages are not dropped.

For repeating syslog messages—identical messages that occur multiple times in succession—only one copy of the message is placed in the syslog file. The message is annotated to indicate the number of times that the message occurred.

The maximum length of a syslog message is 1024 bytes. Longer messages are truncated.

Syslog messages related to AAA authentication and Netconf CLI access and usage are placed in the auth.log and messages files. Each time Cisco vManage logs in to a Cisco vEdge device to retrieve statistics and status information and to push files to the router, the router generates AAA and Netconf log messages. So, over time, these messages can fill the log files. To prevent these messages from filling the log files, you can disable the logging of AAA and Netconf syslog messages:

```
Device(config)# system aaa logsViptela(config-logs)# audit-disableViptela(config-logs)#  
netconf-disable
```

Syslog Message Format

Syslog message generated by the Cisco SD-WAN software have the following format:

```
facility.source  
date - source - module - level - MessageID: text-of-syslog-message
```

Here is an example syslog message. This is logged with local7 facility and level "notice".

Syslog Message Acronyms

The following acronyms are used in syslog messages and in the explanations of the messages:

Table 10:

Acronym	Meaning
confd	CLI configuration process
FTM	Forwarding table manager
FP	Forwarding process
RTM	Route table manager
TTM	Tunnel table manager

To see a list of the various syslog messages generated, see Syslog Messages in the Appendix.

Syslog Messages

The tables below list the syslog messages generated by Cisco vEdge devices and Cisco IOS XE SD-WAN devices. The messages are grouped based on the software module that generates them. The software modules are typically processes (daemons) that run on the device.

All syslog messages are generated on all the devices unless otherwise indicated.

Each syslog message has a corresponding number. The tables list all syslog messages and their number even if the messages are defined in the header files but are not currently used in the operating software. For these messages, the Message Format, Description, and Action fields are empty.

In these tables, the Action field indicates the recommended action you should take in response to the syslog message:

- A—Automatically open a ticket in your organization's support team.
- AE—Automatically open a support ticket and escalate the ticket
- E—Send email to the appropriate team within your organization.

If you see a syslog message that is not listed in one of the tables below, please send the message, along with the device and software version, to Cisco support.

CFGMGR: Configuration Manager Process

Priority: Informational

Message	Number	Message Format	Description	Action
CFGMGR_SYSLOG_END	399999	Terminating cfgmgr	Configuration manager is stopping	E
CFGMGR_SYSLOG_SPEED_DUPLEX_NOT_SUPPORTED	300003	—	Interface does not support duplex mode	E
CFGMGR_SYSLOG_SPURIOUS_TIMER	300002	—	Internal error	A
CFGMGR_SYSLOG_IF_STATE	300004	—	Interface state reported by configuration manager	E
CFGMGR_SYSLOG_START	300001	Starting cfgmgr	Configuration manager is starting	E

CFLOWD: Cflowd Traffic Flow Monitoring Process

Priority: Informational

Message	Number	Message Format	Description	Action
CFLOWD_SYSLOG_MSG	2200002	Received information about vpn_id %ld, vpn_id	Cflowd detected a VPN change	E

Priority: Notice

Message	Number	Message Format	Description	Action
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd because sysmgr terminated	Cflowd module going down at request of sysmgr	E

Message	Number	Message Format	Description	Action
CFLOWD_SYSLOG_END	2299999	Terminating module cflowd with error code %d	Cflowd initialization failed and cflowd is about to go down, or cflowd module is going down	A
CFLOWD_SYSLOG_START	2200001	Starting module cflowd	Cflowd module is starting	E

CHMGR: Chassis Manager

The chassis manager process runs only on physical routers.

Priority: Informational

Message	Number	Message Format	Description	Action
CHMGR_CHASSIS_INFO	100009	Chassis-Type %s max-modules %d	Informational message indicating chassis type and maximum number of modules (PIMs + fixed) supported by chassis	E
CHMGR_FAN_SPEED_HIGH	100003	—	Fan speed is high	E
CHMGR_FAN_SPEED_NORMAL	100004	—	Fan speed is normal	E
CHMGR_FANTRAY_INSERTED	100052	Fantray %d inserted	Fan tray inserted (on vEdge 2000 only)	E
CHMGR_FANTRAY_REMOVED	100053	Fantray %d removed	Fan tray removed (on vEdge 2000 only)	E
CHMGR_MODULE_INSERTED	100007	Module %d inserted - port type: %s, num_ports: %s	PIM module inserted	E
CHMGR_MODULE_REMOVED	100008	Module %d removed	PIM module removed	E
CHMGR_PIM_OK	100057	—	PIM module status is normal	E
CHMGR_PORT_INSERTED	100005	Port %s inserted in module %d	SFP inserted	E
CHMGR_PORT_REMOVED	100006	Port %s removed from module %d	SFP removed	E
CHMGR_SIGTERM	100024	Received sigterm, exiting gracefully	Debug-level message indicating that chassis manager is going down	E
CHMGR_SYSLOG_START	100001	Starting chassis manager	Chassis manager process is starting	E
CHMGR_USB_INSERTED	100058	USB media inserted in slot %d	USB media inserted	E

Message	Number	Message Format	Description	Action
CHMGR_USB_REMOVED	100059	USB media removed from slot %d	USB media removed	E

Priority: Notice

Message	Number	Message Format	Description	Action
CHMGR_EMMC_OK	100039	eMMC read successful	EMMC read was successful	E
CHMGR_FAN_OK	100041	Fan Tray %d Fan %d fault cleared, ftrayid, id	Fan fault cleared	E
CHMGR_FANTRAY_OPER	100055	Fan tray '%d' up, ftrayid	Fan tray detected	A
CHMGR_FLASH_OK	100037	Flash memory status read successful	Flash read successful	E
CHMGR_PEM_OK	100043	Power supply '%d' fault cleared	Power supply fault cleared	E
CHMGR_PEM_OPER	100045	Power supply '%d' up	Power supply inserted or detected	E
CHMGR_SDCARD_OK	100047	SD card read successful	SD card read successful	E
CHMGR_SFP_UNSUPPORTED	10060	SFP %s is not supported	SFP is not supported	E
CHMGR_SHORT_RESET_REQUEST	100018	—	Chassis manager received a request to reboot the router	E
CHMGR_TEMP_GREEN	100030	%s temperature (%d degrees C) is below yellow threshold (%d degrees C)	Temperature sensor reading below yellow threshold	E
CHMGR_TEMP_OK	100027	%s temperature sensor fault cleared	Temperature sensor read successful after a previous failed attempt	E

Priority: Warning

Message	Number	Message Format	Description	Action
CHMGR_HOTSWAP_DIFF_MOD	100051	Hot-Insertion of a module of different type requires reboot. Module %d will remain down,	PIM module of a different type was inserted in the slot; it was detected, but will remain down until the next reboot	E

Priority: Error

Message	Number	Message Format	Description	Action
CHMGR_CONFD_DATAACB_REGISTER_FAILED	100023	Failed to register data cb	Internal error registering a data callback function with confd	AE
CHMGR_CONFD_REPLY_FAILED	100022	Failed to send oper data reply - %s (%d)	Internal error occurred when processing chassis manager-related configuration of show command	A
CHMGR_EEPROM_READ_FAILED	100011	Failed to read module %d eeprom on chassis %s, module, chassis-name	Failed to read details of inserted PIM	AE
CHMGR_EEPROM_VERSION_ERROR	100012	Unsupported eeprom format version for module %d	EEPROM version of PIM module is supported; module will not be recognized	AE
CHMGR_EMMC_FAULT	100038	eMMC fault detected	Error occurred reading EMMC information	A
CHMGR_FAN_FAULT	100040	Fan Tray %d Fan %d fault detected, ftrayid, id	Fan fault detected	A
CHMGR_FANTRAY_DOWN	100054	Fan tray '%d' not present, ftrayid id	Fan tray not detected	A
CHMGR_FLASH_FAULT	100036	Flash memory status fault	Internal error reading flash	AE
CHMGR_GET_HWADDR_FAILED	100010	Failed to get macaddr for %s, p_ifname	Internal error resulting from failure to obtain an interface's MAC address	A

Message	Number	Message Format	Description	Action
CHMGR_GET_IFFLAG_FAILED	100016	Failed to get ifflags for %s err %d, p_port->kernel_name, errno	Interface initialization failure; interface may remain down, or device may reboot	A
CHMGR_IFFLAGS_SET_FAIL	100050	—	Setting an interface flag failed	E
CHMGR_IF_GSO_OFF_FAILED	100025	—	Setting interface options failed	E
CHMGR_PEM_DOWN	100044	Power supply '%d' down or not present	Power supply removed or not detected	A
CHMGR_PEM_FAULT	100042	Power supply '%d' fault detected	Power supply fault detected	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault	PIM power fault detected	AE
CHMGR_PIM_FAULT	100056	PIM %d power fault cleared	PIM power fault cleared	A
CHMGR_SDCARD_FAULT	100046	SD card fault detected (no present or unreadable)	SD card fault detected	A
CHMGR_SET_IFFLAG_FAILED	100017	Failed to set ifflags to %x for %s err %d	Interface initialization failure; interface may remain down, or device may reboot	A
CHMGR_SHORT_RESET_CLEAR_FAILED	100019	—	Clearing a reboot request failed.	A
CHMGR_SHORT_RESET_FAILED	100020	—	Request to reset the router by rebooting failed	A

Message	Number	Message Format	Description	Action
CHMGR_SPURIOUS_TIMER	100035	Spurious timer ignored what = %#x arg = %p	Internal error	A
CHMGR_SYSOUT_OF_RESOURCES	100049	Timer add failed. Out of resources	Internal error; if fatal, device may reboot to recover	A
CHMGR_UNKNOWN_MODULE_TYPE	100013	Invalid module-type %x in module-slot %d on chassis %s,	Unrecognized PIM module type in slot	AE
CHMGR_UNSUPPORTED_MODULE_TYPE	100014	Module-Type %s not supported in slot %d on chassis %s	PIM module is not supported in slot in which it is inserted	A

Priority: Critical

Message	Number	Message Format	Description	Action
CHMGR_IF_RENAME_FAILED	100015	Unable to rename %s to %s	Interface initialization failed; interface may remain down or the device may reboot	A
CHMGR_TEMP_FAULT	100026	%s temperature sensor fault detected. Unable to read temperature	Failed to read from a temperature sensor; possible temperature sensor failure	A
CHMGR_TEMP_RED	100028	%s temperature (%d degrees C) is above red threshold (%d degrees C).	Temperature sensor reading above red threshold	AE
CHMGR_TEMP_YELLOW	100029	%s temperature (%d degrees C) is above yellow threshold (%d degrees C),	Temperature sensor reading above yellow threshold	A

Priority: Alert

Message	Number	Message Format	Description	Action
CHMGR_CONFD_INIT_FAILED	100021	Initialization failed. vconfd_module_init returned %d	Chassis manager failed to initialize and start	AE

CVMX: Internal Cavium Driver Process

Priority: Informational

Message	Number	Message Format	Description	Action
CVMX_SYSLOG_END	999999	Terminating Cavium drivers	Internal Cavium drivers ending	E
CVMX_SYSLOG_START	900001	Starting Cavium drivers	Internal Cavium drivers starting	E

CXP: Cloud onRamp for SaaS Process

Priority: Informational

Message	Number	Message Format	Description	Action
CXP_SYSLOG_END	2799999	Terminating Cloud onRamp process	Cloud onRamp for SaaS ending	E
CXP_SYSLOG_START	2700001	Starting Cloud onRamp process	Cloud onRamp for SaaS starting	E

CONTAINER: Containers

Priority: Informational

Message	Number	Message Format	Description	Action
CONTAINER_SYSLOG_END	2699999	Terminating container process	Container process ending	E
CONTAINER_SYSLOG_START	2600001	Starting container process	Container process starting	E

DBGD: Debug Process

Priority: Informational

Message	Number	Message Format	Description	Action
DBGD_SYSLOG_END	2900001	Terminating debug process	Debug process ending	E
DBGD_SYSLOG_START	2999999	Starting debug process	Debug process starting	E

DHCP: DHCP Client

The DHCP client process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_CLEAR_INTERFACE	1300006	Clearing dhcp state for interface %s,	DHCP client cleared DHCP state for interface	E

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_DISCOVER_TIMEOUT	1300005	No response for dhcp discover packets for interface %s,	DHCP discovery failure	E
DHCP_SYSLOG_END	1300001	Terminating syslog process	Syslog process ending	E
DHCP_SYSLOG_IP_ADDR_ASSIGNED	1300002	Assigned address %s to interface %s	DHCP client assigned address to interface	E
DHCP_SYSLOG_IP_ADDR_RELEASED	1300003	Released address for interface %s	DHCP client released address	E
DHCP_SYSLOG_IP_ADDR_RENEWED	1300010	Renewed address %s for interface %s	DHCP client address renewed	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [50%%] for interface %s address %s/%d	DHCP client renewal request at 50% of lease expiration time	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [85%%] for interface %s address %s/%d	DHCP client renewal request at 85% of lease expiration time	E
DHCP_SYSLOG_IP_ADDR_REQUEST_RENEW	1300004	Requesting renew [100%%] for interface %s address %s/%d	DHCP client renewal request at 100% of lease expiration time	E
DHCP_SYSLOG_START	1399999	Starting syslog process	Syslog paroces starting	E

Priority: Critical

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_IP_ADDR_CONFLICT	1300007	Interface %s IP Address %s conflict with interface %s,	DHCP client detected IP address conflict with another interface	E

DHCP: DHCP Server

The DHCP server process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server bindings for interface %s, vpn %ld,	DHCP server cleared bindings for interface	E
DHCP_SYSLOG_CLEAR_SERVER_BINDINGS	1300008	Clearing dhcp server binding for interface %s, vpn %ld, mac addr %x:%x:%x:%x:%x:%x,	DHCP server cleared bindings for interface	E

FPMD: Forwarding Policy Manager Process

Priority: Informational

Message	Number	Message Format	Description	Action
FPMD_SYSLOG_ACL_PROGRAM_SUCCESS	1100005	Successfully reprogrammed access list - %s	Access list successfully created	E
FPMD_SYSLOG_END	1199999	Terminating fpmd	Forwarding policy manager process is ending	E
FPMD_SYSLOG_POLICY_PROGRAM_SUCCESS	1100004	Successfully reprogrammed policy %s - %s	Policy created successfully	E
FPMD_SYSLOG_START	1100001	Starting fpmd	Forwarding policy manager process is starting	E

Priority: Alert

Message	Number	Message Format	Description	Action
FPMD_SYSLOG_ACL_PROGRAM_FAILED	1100003	Failed to allocate memory for access list %s. Continuing without the access	Access list could not be created	A
FPMD_SYSLOG_POLICY_PROGRAM_FAILED	1100002	Failed to allocate memory for policy %s - %s. Continuing without the policy	Policy could not be created	A

FTMD: Forwarding Table Management Process

The forwarding table management process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
FTMD_SLA_CLASS_ADD	1000020	SLA Class %s added at index %d: loss = %d%%, latency = %d ms	SLA class added	E
FTMD_SYSLOG_BFD_STATE	1000009	record with discriminator %u invalid	BFD state is invalid	E
FTMD_SYSLOG_BFD_STATE	1000009	BFD Session %s.%u->%s.%u %s:%u->%s:%u %s %s %s %d	BFD state changed	E
FTMD_SYSLOG_DBGD_STATE	1000036	Connection to DBGD came up Connection to DBGD went down DBGD FTM: Initialized message queue DBGD FTM oper %d vpn %u sip %s:%u dip %s %u DBGD FTM: oper %d vpn %lu localc %d remote %d remoteip %s	Messages related to the FTM debugging process	E
FTMD_SYSLOG_DPI_FLOW_OOM	1000024	Out-of-memory status for DPI flows: %s	Memory status for SAIE flows Note In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_DPI_WRITE_OFF	1000032	Turning off writing DPI records to disk	SAIE records are no longer being written to disk Note In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.	E
FTMD_SYSLOG_END	1999999	Terminating FTM process	Forwarding table management process ending	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB6 memory to accommodate larger tables):	IPv6 forwarding table size is being increased	E
FTMD_SYSLOG_FIB_GROW	1000012	Growing FIB memory to accommodate larger tables):	IPv4 forwarding table size is being increased	E
FTMD_SYSLOG_IF_STATE	1000001	VPN %lu Interface %s %s,	FTM detected interface state change	E
FTMD_SYSLOG_LR_ADD	1000027	LR: Adding Iface %s as LR	Last-resort interface is being added	E
FTMD_SYSLOG_LR_ADD	1000027	LR: Iface %s has become an LR	Interface has become a last-resort interface	E
FTMD_SYSLOG_LR_DEL	1000028	LR: Found iface %s while looking for iface %s	Last-resort interface found while looking for another interface	E
FTMD_SYSLOG_LR_DEL	1000028	LR: iface %s has become non-LR. Hence set OPER UP on that interface	Last-resort interface has become an active interface	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_LR_DEL	1000028	LR: Iface %s has become a non-LR LR: Removing Iface %s as LR	Messages related to an interface that is no longer a last-resort interface	E
FTMD_SYSLOG_LR_DOWN	1000030	LR: At least one bfd session of non-LR is active LR: At least one non-LR's bfd session in Up LF bfd session = SIP: %s DIP:%s SPORT:%u DPORT:%u PROTO:%u is Up for at least &u interval msec LR: Bringing LR's wan if Down in %u msec LR: Bringing LR's wan if Down right away LR: Cleared LR down_in-progress	Messages related to shutting down an interface of last resort	E
FTMD_SYSLOG_LR_UP	1000029	LR: All bfd sessions gone down. Setting LR %s's OPER state to UP	Last-resort interface's status set to Up because no other circuits on the router are active	E
FTMD_SYSLOG_LR_UP	1000029	LR: Bring LR's wan if up immediately as no other circuit's bfd sessions are up	Last-resort interface activated because no other circuits on the router are active	E
FTMD_SYSLOG_LR_UP	1000029	LR: Starting hold up timer immediately !!	Hold timer for last-resort interface activated because no other circuits on the router are active	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_NAT_FLOW_ADD	1000039	NAT flow add: Private %s, Public %s	FTM detected the addition of a NAT flow with the specified private and public IP addresses	E
FTMD_SYSLOG_NAT_FLOW_DELETE	1000040	NAT flow delete: Private %s, Public %s	FTM detected the deletion of a NAT flow with the specified private and public IP addresses	E
FTMD_SYSLOG_PIM_DOWN	1000017	—	FTM detected that PIM ended	E
FTMD_SYSLOG_PIM_UP	1000018	—	FTM detected that PIM started	E
FTMD_SYSLOG_ROUTE_ADD_FAIL	1000004	Route Add for prefix %s Failed. Reason %s	FTM failed to add a route received from the RTM	E
FTMD_SYSLOG_ROUTE_VERIFY	1000033	Successfully verified RIB and FIB routes on the Cisco vEdge device	FTM verified the routes in the router's RIB and FIB	E
FTMD_SYSLOG_ROUTE_VERIFY_FAIL	1000034	—	RIB and FIB router verification failed	E
FTMD_SYSLOG_SIGTERM	1000005	Received Cleanup signal. Exiting gracefully	FTM received termination signal from sysmgr and is about to go down	E
FTMD_SYSLOG_START	1000001	Starting FTM process	Forwarding table management process starting	E
FTMD_SYSLOG_TCPD_STATE	1000035	Sent tcp_opt_disable successfully for vpn %ld	Disabling of TCP options was successful on the interface	E
FTMD_SYSLOG_TUNNEL_ADD_FAIL	1000015	Tunnel Add to TLOC %s.%s Failed. Reason %s	Failed to add new TLOC; reported by TTM	E
FTMD_SYSLOG_WWAN_STATE	1000025	Bring %s last resort circuit	Up or down status of circuit of last resort	E
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN came up	Circuit of last resort came up	E

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_WWAN_STATE	1000025	Connection to WWAN went down	Circuit of last resort went down	E

Priority: Notice

Message	Number	Message Format	Description	Action
FTMD_SLA_CLASS_DEL	1000022	Sla class %s at index %d removed: loss = %d%%, latency = %d ms, jitter = %d ms	SLA class deleted	A
FTMD_SLA_CLASS_MOD	1000021	Sla class %s at index %d modified: loss = %d%%, latency = %d ms, jitter = %d ms	SLA class changed	A
FTMD_SLA_CLASS_VIOLATION	1000023	[%lu] SLA class violation application %s %2:%u. %s:&u protocol: %d dscp: %d %s, status - %s	SLA class violation for application in specified VPN, with specified source address and port, destination address and port, protocol, DSCP, and reason	A
FTMD_SYSLOG_DOT1X_HOST	1000031	Host %s denied access on interface %s in single host mode	An 802.1X interface in single-host mode is denying access, because it has already granted access to a client	E
FTMD_SYSLOG_FLOW_LOG	1000026	%s	FTM detected a new flow	E
FTMD_SYSLOG_FP_CORE_FAIL	1000013	FP core watchdog expired (rc = %d). %s, rc, action_str	FTM detected that FP may not be functioning; device will reboot soon	A
FTMD_SYSLOG_PMTU_LOWERED	1000016	Tunnel %s/%d -> %s/%d MTU Changed to %u due to Path-MTU Discovery,	MTU size on a tunnel changed due to path MTU discovery	E
FTMD_SYSLOG_ZBFW_FLOW_ADD	1000037	ZBF flow created zone-air %s key %s src_vpn %d dst_vpn %d expiry secs %d state %s	FTM detected the creation of a zone pair	E
FTMD_SYSLOG_ZBFW_FLOW_DEL	1000038	ZBF flow deleted zone-air %s key %s src_vpn %d dst_vpn %d state %s	FTM detected the deletion of a zone pair	E

Priority: Critical

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_BUFFER_POOL_LOW Note This error message is available from Cisco SD-WAN Release 20.7.1.	1000041	Critical Alert: Buffer Pool <num>; available buffers are x% of total buffers	FTM detected that the specified buffer pool has gone below 20% of its capacity	E

Priority: Warning

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_BUFFER_POOL_LOW Note This error message is available from Cisco SD-WAN Release 20.7.1.	1000041	Warning Alert: Buffer Pool <num>; available buffers are x% of total buffers	FTM detected that the specified buffer pool has gone below 50% of its capacity	E
FTMD_SYSLOG_TTM_DOWN	1000008	Connection to TTM went down. p_msgq %p p_ftm %p,	FTM connection with TTM went down; BFD sessions will be cleared	E
FTMD_SYSLOG_TTM_UP	1000007	Connection to TTM came up. p_msgq %p p_ftm %p,	FTM connected with TTM	E
FTMD_TUNNEL_SLA_CHANGED	1000019	SLA changed for session: %s.%u->%s:%u->%s:%u. New loss = %d%%, latency = %d ms, jitter = %d ms, SLA Classes: %s (0x%x) %s%s	FTM detected SLA changes on a tunnel	E

Priority: Error

Message	Number	Message Format	Description	Action
FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register bfd show data cb	FTM failed to register data callback with confd; device may reboot	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	Failed to register policer show data cb	FTM failed to register data callback with confd; device may reboot	AE
FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to register data cb, __FUNCTION__	FTM failed to register data callback with confd; device may reboot	AE

FTMD_SYSLOG_CONFD_FAIL	1000003	%s: Failed to send oper data reply - %s (%d) : %s,	FTM failed to respond correctly to confd; some show commands may not work	A
FTMD_SYSLOG_FP_COREDUMP	1000011	FP Core %d Died. Core file recorded at %s,	FTM detected an FP crash; device will reboot soon	AE
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of forwarding interface records	Interface not added because of insufficient forwarding interface database records	A
FTMD_SYSLOG_IFADD_FAIL	1000014	Failed to add interface %s in vpn %lu. Out of snmp interface indices	Interface not added because of insufficient SNMP interface indices	A
FTMD_SYSLOG_INIT_FAIL	1000002	vconf_module_init returned %d	FTM failed to start with confd	A
FTMD_SYSLOG_LR_DEL	1000028	LR: LR is not enabled...while we are trying to remove iface %s as last resort	Interface being removed is not configured as a last-resort interface	A
FTMD_SYSLOG_LR_DEL	1000028	LR: Unable to remove iface %s as LR	Interface is no longer a last-resort interface so it cannot be deleted	A
FTMD_SYSLOG_RTM_DECODE_FAIL	1000006	Bad RTM Msg: Msg-Type %u Msg-Len %u len: %u decoded-len %u,	Could not process route or interface change message from RTM	A
FTMP_SYSLOG_SPURIOUS_TIMER	1000010	Spurious timer ignored what = %#x arg = %p,	Internal error	A

GPS: Global Positioning System

Priority: Informational

Message	Number	Message Format	Description	Action
GPS_SYSLOG_END	2599999	Terminating GPS	GPS process is ending	E
GPS_SYSLOG_GGA_FIX	2500002	GGA %d:%d:%d lat=%f lon=%f alt=%f sat=%d hdop %f fix%d	GPS fix information	E
GPS_SYSLOG_GSA_FIX	2500004	GSA %s pdop=%f hdop=%f vdop=%f	GPS satellite and dilution of precision (DOP) information	E

Message	Number	Message Format	Description	Action
GPS_SYSLOG_PSTOP	2500005	Polling disabled Stopping polling timers	Messages related to polling for GPS information	E
GPS_SYSLOG_RMC_FIX	2500003	RMC %s %d %d lat=%f lon=%f speed %f course=%s status valid	Essential minimum GPS information	E
GPS_SYSLOG_START	2500001	Starting GPS	GPS process is starting	E

IGMP: Internet Group Management Protocol

Priority: Informational

Message	Number	Message Format	Description	Action
IGMP_SYSLOG_END	1800001	Terminating IGMP	IGMP process is ending	E
IGMP_SYSLOG_START	1899999	Starting IGMP	IGMP process is starting	E

LIBBSS: UNIX BSS Library

Unused Messages

Message	Number	Message Format	Description	Action
LIBBSS_SYSLOG_END	1699999	Terminating libbss	UNIX BSS library process is ending	E
LIBBSS_SYSLOG_START	1600001	Starting libbss	UNIX BSS library process is starting	E

LIBCHMGR: Chassis Manager Library Process

Unused Messages

Message	Number	Message Format	Description	Action
LIBCHMGR_SYSLOG_END	1599999	Terminating libchmrg	Chassis manager library process is ending	E
LIBCHMGR_SYSLOG_START	1500001	Starting libchmgr	Chassis manager library process is starting	E

MSGQ: Message Queue Process

Unused Messages

Message	Number	Message Format	Description	Action
MSGQ_SYSLOG_END	899999	Terminating msgq	Message queue process is ending	E
MSGQ_SYSLOG_START	800001	Starting msgq	Message queue process is starting	E

OMP: Overlay Management Protocol

Priority: Informational or Other

Message	Number	Message Format	Description	Action
OMP_NUMBER_OF_CISCO_VSMARTS	400005	Number of Cisco vSmarts connected: %u	Number of Cisco vSmart Controllers to which device is connected (on Cisco vEdge devices only)	E
OMP_PEER_STATE_CHANGE	400002	%s peer %s state changed to %s,	OMP peer stated changed to up or down	E
OMP_POLICY_CHANGE	400007	Using policy from peer %s,	Forwarding policy received from Cisco vSmart Controller (on Cisco vEdge devices only)	E
OMP_STATE_CHANGE	400003	Operational state changed to %s,	OMP internal operational state changed	E
OMP_TLOC_STATE_CHANGE	400004	TLOC %s state changed to %s for address-family: %s,	TLOC state changed	E

Priority: Notice

Message	Number	Message Format	Description	Action
OMP_SYSLOG_END	400006	Terminating	OMP process is stopping	E
OMP_SYSLOG_START	400001	Starting	OMP process is starting	E

PIM: Protocol-Independent Multicast Process

Priority: Informational

Message	Number	Message Format	Description	Action
IGMP_SYSLOG_END	1900001	Terminating	PIM process is ending	E

Message	Number	Message Format	Description	Action
IGMP_SYSLOG_START	1999999	Starting	PIM process is starting	E

Priority: Notice

Message	Number	Message Format	Description	Action
PIM_SYSLOG_IF_STATE_CHANGE	1900003	VPN %lu Interface %s %s	In specified VPN, interface state changed to up or down	E
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s state changed to up	PIM neighbor came up	E
PIM_SYSLOG_TUNNEL_STATE_CHANGE	1900004	Tunnel %s state changed to %s	Tunnel used for PIM when down or came up	E

Priority: Error

Message	Number	Message Format	Description	Action
PIM_SYSLOG_NBR_STATE_CHANGE	1900002	Neighbor %s stated changed to down	PIM neighbor went down	E

POLICY: Policy Process

Unused Messages

Message	Number	Message Format	Description	Action
POLICY_SYSLOG_END	799999	Terminating policy	Policy process is ending	E
POLICY_SYSLOG_START	700001	Starting policy	Policy process is starting	E

RESOLV: Resolver Process

Unused Messages

Message	Number	Message Format	Description	Action
RESOLV_SYSLOG_END	2000001	Terminating resolver	Resolver process is ending	E
RESOLV_SYSLOG_START	2099999	Starting resolver	Resolver process is starting	E

SNMP Listener Process

Unused Messages

Message	Number	Message Format	Description	Action
SNMP_SYSLOG_END	2100001	Terminating SNMP listener	SNMP listener process is ending	E
SNMP_SYSLOG_START	2199999	Starting SNMP listener	SNMP listener process is starting	E

SYSMGR: System Manager Process

The system manager process (daemon) spawns, monitors, and terminates all the processes in the system, and it collects and logs vital system information, such as memory and CPU status.

Priority: Informational

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE1_INFO	200041	Generated authorized keys on %s, p_sysmgr->cfg.my_personality	Generated authorized keys for SSH-based login between the Cisco vManage server and the Cisco SD-WAN device	E
SYSMGR_CONFD_PHASE2_SUCCESS	200007	Confd Phase2 Up	Successful device bringup	E
SYSMGR_DAEMON_START	200017	Started daemon %s @ pid %d in vpn %lu,	System manager started process in VPN	E
SYSMGR_DAEMON_UP	200011	Daemon %s @ pid %d came up in vpn %lu (%d %d)	Daemon started by system manager came up as expected	E
SYSMGR_SIGTERM	200001	Received sigterm, stopping all daemons except confd	System manager received termination signal and will initiate termination of all processes	E
SYSMGR_VPN_DESTROY	200022	vpn %lu destroy. lookup returned %p	Stopping all processes in VPN	E

Priority: Notice

Message	Number	Message Format	Description	Action
SYSMGR_CLOCK_SET	200025	System clock set to %s	System clock set by user	E
SYSMGR_CONFD_CDB_NOT_INITED	200031	Confd db initialization not complete. Deleting cdb and starting afresh.	First-time initialization of configuration database	E
SYSMGR_CONFD_PHASE1_INFO	200041	Install successfully completed from %s to %s	Failed to read installation ID; will fall back to default	E
SYSMGR_CORE_FILE_COMPRESSED	200045	—	Core file was compressed	E
SYSMGR_DAEMON_EXIT_NORMAL	200021	—	A process terminated normally	E
SYSMGR_DAEMON_RESTARTED	200043	—	A process restarted	E
SYSMGR_DISK_ALERT_OFF	200036	Disk usage is below 60%%.	Disk usage is below threshold	E
SYSMGR_MEMORY_ALERT_OFF	200058	System memory usage is below 50%	System memory usage is below 50%	E
SYSMGR_MISC	200065	—	Miscellaneous message	E
SYSMGR_REBOOT	200038	System going down for a reboot.. (%s), reason	System manager initiating a device reboot, possibly because of a process failure	E
SYSMGR_SHM_FAIL	200042	Created shared memory %s	Successfully initialized shared memory for communication with other processes	E

Message	Number	Message Format	Description	Action
SYSMGR_SHUTDOWN	200040	System shutting down.. (%s), reason	System manager is powering down the device; device will not come back up unless it is physically power-cycled	A
SYSMGR_SYSTEM_GREEN	200050	System up with software version %s	System status is green, indicating that all processes came up as expected	E
SYSMGR_SYSTEM_RED	200051	System status red (software version '%s')	System status is red, possibly because of a process failure	A
SYSMGR_SYSTEM_START	200002	Starting system with Cisco SD-WAN software version %s	System has stated; usually one of the first messages during device bringup	E
SYSMGR_TIMEZONE_SET	200028	System timezone changed from %s to %s	System timezone changed as result of configuration change	E
SYSMGR_UPGRADE_AUTO_CONFIRMED	200063	—	A software upgrade was automatically confirmed	E
SYSMGR_UPGRADE_NOT_CONFIRMED	200049	—	A software upgrade was as not confirmed	E
SYSMGR_UPGRADE_PENDING_CONFIRMATION	200059	—	A software upgrade is pending confirmation	E

Message	Number	Message Format	Description	Action
SYSMGR_VDEBUG_LOG_CLEANUP_NEEDED	200066	Debug logs exceed expected storage quota. Performing age-based cleanup to restore debug logging operations.	Debug logs were deleted to create space	A
SYSMGR_DAEMON_TERMINATED	200020	—	A process terminated	E
SYSMGR_WATCHDOG_EXPIRED	200062	—	The watchdog process expired	A

Priority: Warning

Message	Number	Message Format	Description	Action
SYSMGR_CORE_FILE_DELETED	200044	—	Core file was deleted	A
SYSMGR_DAEMON_RESTART_ABORTED	200060	—	The restarting of a process was terminated.	A
SYSMGR_DAEMON_STOP	200018	Stopping daemon %s @ pid %d. Sending signal %d	System manager stopped a daemon	E
SYSMGR_DISK_ALERT_ORANGE	200054	Disk usage is above 75%%. Please clean up unnecessary files.	Disk usage is above 75%	E
SYSMGR_DISK_ALERT_YELLOW	200035	Disk usage is above 60%%. Please clean up unnecessary files.	Disk usage is above 60%	E
SYSMGR_FILE_DELETED	200064	Deleted file %s (size %lu MB) to recover disk space	File deleted to free up disk space	A
SYSMGR_MEMORY_ALERT_ORANGE	200056	System memory usage is above 75%%	System memory usage is above 75%	E
SYSMGR_MEMORY_ALERT_YELLOW	200057	System memory usage is above 60%%	System memory usage is above 60%	E

Priority: Error

Message	Number	Message Format	Description	Action
SYSMGR_BAUD_RATE_SET	200046	Console baud rate changed to '%d', baud_rate	Console baud rate changed	E
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in OS to '%d'	Failed to set user-specified console baud rate in Linus	A
SYSMGR_BAUD_RATE_SET_FAIL	200047	Failed to set console baud rate in U-boot to '%d'	Failed to set user-specified console baud rate in Uboot	A
SYSMGR_CLOCK_SET_FAIL	200026	Cannot set system clock to %s	Failed to set system clock to time specified by user	A
SYSMGR_CONFD_CDB_INIT_OPEN_FAIL	200030	Failed to open cdb init file (%s)	Failed to open the configuration database	A
SYSMGR_DAEMON_EXIT_FAIL	200023	—	A process could not terminate	A
SYSMGR_CONFD_DATA_CB_REGISTER_FAIL	200010	Failed to register data cb	Failed to register data callback function with confd; device may reboot	A
SYSMGR_CONFD_CDB_DEL_FAIL	200032	Failed to remove cbd directory '%s'	Failed to reinitialize configuration database to recover from failure	AE
SYSMGR_CONFD_FORK_FAILURE	200003	Cannot move confd to phase2 (err %s)	Failed to move confd to Phase 2; device will reboot soon	A

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate archive keys	Failed to generate keys required for archiving configuration	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate authorized keys on %s, p_sysmgr->cfg.my_personality	Failed to generate keys required for SSH-based login between the Cisco vManage server and the Cisco SD-WAN device	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to generate SSH keys for archive	Failed to generate SSH keys	E
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get install id from file, using 00_00	Failed to read previous system version	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to get previous version, using 0.0	Failed to read system version	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Failed to transition confd to phase1. Re-initializing CDB..	Conf module failed to move to Phase 1, indicating a possible configuration database failure; device will reboot soon	A
SYSMGR_CONFD_PHASE1_FAILURE	200005	Verified that archive keys exist	Verified that configuration archive keys exist	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to get current version, using 0.0	Failed to read system version file	A

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to open %s, version_file	Failed to open system version file	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to read %s, version_file	Failed to read system version file	A
SYSMGR_CONFD_PHASE2_FAILURE	200006	Failed to transition confd to phase2	Confid module failed to move to Phase 2, indicating a possible configuration database failure; device will reboot soon	A
SYSMGR_CONFD_REPLY_FAIL	200009	Failed to send oper data reply - %s (%d)	Failed to reply to confd; some show commands may not work	A
SYSMGR_CONFD_SETPGID_FAILURE	200004	setpgid(0,0) failed: %d	Process group failed to start	A
SYSMGR_DAEMON_DOWN	200012	Daemon %s [%u] went down in vpn %lu,	Process started by system manager went down	A
SYSMGR_DAEMON_EXECSV_FAILURE	200016	execv %s failed	Internal failure occurred while starting a process	A
SYSMGR_DAEMON_FORK_FAILURE	200014	Cannot start daemon %s: %s	Internal failure occurred while starting a process	A

Message	Number	Message Format	Description	Action
SYSMGR_DAEMON_INACTIVE	200033	Daemon %s[%lu] @ pid %d died. Rebooting device..	System manager detected a process failure and is about to reboot the device	A
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to daemon %s. err %d	Failed to establish message queue with process; device may reboot soon	A
SYSMGR_DAEMON_MSGQ_FAILURE	200013	Could not start msgq to quagga daemon %s. err %d	Failed to establish message queue with routing process; device may reboot soon	A
SYSMGR_DAEMON_SETAFFINITY_FAILURE	200061	—	The scheduling of a process failed	E
SYSMGR_DAEMON_SETPGID_FAILURE	200015	setpgid(0,0) failed	Internal failure setting process group of a process	A
SYSMGR_DAEMON_STOPPED	200019	Daemon %s @ pid %u terminated - %s	Daemon started by system manager terminated; device may reboot soon (except for the Cisco vBond Orchestrator)	A

Message	Number	Message Format	Description	Action
SYSMGR_RTC_CLOCK_SET_FAIL	200027	Cannot set hardware clock to %s - %s (errno	Failed to update hardware clock to system time specified by user	A
SYSMGR_SHM_FAIL	200042	Failed to close shared memory %s with an error %d	Failed to completely and properly close the shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to map shared memory %s	Failed to initialize shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to open shared memory %s with an error %d	Failed to open shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to truncate shared memory %s with an error %d	Failed to initialize shared memory for communication with other processes	E
SYSMGR_SHM_FAIL	200042	Failed to unmap shared memory %s	Failed to completely and properly close shared memory for communication with other processes	E

Message	Number	Message Format	Description	Action
SYSMGR_SWITCHBACK_FAILED	200053	Software upgrade to version %s failed because of %s	Software upgrade failed	A
SYSMGR_TIMEZONE_SET_FAIL	200029	Failed to set system timezone to %s (rc = %d)	Failed to set system timezone to timezone specified by user	A
SYSMGR_TRACE_ERROR	200024	—	A trace error occurred	A

Priority: Critical

Message	Number	Message Format	Description	Action
SYSMGR_CONFD_INIT_FAIL	200008	Sysmgr child in charge of migrating confd/ncs to phase2 exited with error code %d	System manager detected a confd process failure; device may reboot	AE
SYSMGR_DISK_ALERT_RED	200034	Disk usage is above 90%% (critically high). Please clean up unnecessary files.	Disk usage is above 90%	AE
SYSMGR_MEMORY_ALERT_RED	200055	System memory usage is above 90%% (critically high)	System memory usage is above 90%	AE
SYSMGR_REBOOT_HALTED	200039	Reboot (reason: %s) terminated...too many reboots	System manager stopped short of rebooting the device because it detected too many reboots in a short period of time	AE
SYSMGR_UPGRADE_FAILED	200052	Software upgrade to version %s failed because of reason	Software upgrade failed	AE

TCPD: TCP Options Process

Priority: Informational

Message	Number	Message Format	Description	Action
TCPD_MSGQ_SERVER	2800002	Server Exception: %s	Proxy server did not accept connection	E

Message	Number	Message Format	Description	Action
TCPD_PROXY	2800004	Enabled TCP_OPT for vpn %lu: %s:%u %s Starting sysmgr_app object tcpd<->ftmd channel established tcpd<->ftmd = Will try connecting	Messages related to starting a proxy	E
TCPD_PROXY	2800004	tcpd error counters -%s	Count of TCP option errors	E
TCPD_SYSLOG_END	2800001	Terminating TCP options	TCP options process ending	E
TCPD_SYSLOG_START	2899999	Starting TCP options	TCP options process starting	E
TCPD_SYSMGR_APP	2800003	%s Exception: %s %s - Sysmgr app::connect -Exception - %s	Messages related to the connection between the system manager and the TCP proxy process	E

Priority: Debug

Message	Number	Message Format	Description	Action
TCPD_SYSMGR_APP	2800003	%s - Registering for send_hello-msg %s: Sending following register msg Sending msg of length %u %s - Sysmgr app::connect %s - Write %u bytes %s - Wrote register msg %u	Messages related to the connection between the system manager and the TCP proxy process	E

TRACKER: Interface Tracker Process

Priority: Informational

Message	Number	Message Format	Description	Action
TRACKER_SYSLOG_CONN_DOWN	1700003	Connection to %s %s Down	Connection to interface is down	E
TRACKER_SYSLOG_CONN_UP	1700002	Connection to %s %s Up	Connection to interface is up	E
TRACKER_SYSLOG_END	1700001	Terminating	Interface tracker process is ending	E
TRACKER_SYSLOG_START	1799999	Starting	Interface tracker process is starting	E

VCONF: Cisco SD-WAN Configuration Process

Priority: Informational

Message	Number	Message Format	Description	Action
VCONF_SYSLOG_END	1400001	Terminating	Configuration process is ending	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s process name: %s process id: %s reason: %s	Configuration at specified date and time for a process, with reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s status: %s install id: %s message %s	Configuration at specified date and time, with specified status (minor, major)	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reason: %s	Configuration at specified date and time, with reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s reboot reason: %s	Configuration at specified date and time, with reboot reason	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s username: %s remote host: %s	Configuration at specified date and time, for username and remote host	E
TRACKER_SYSLOG_NOTIFICATION	1400002	Notification: %d/%d?%d %d:%d:%d %s severity level: %s hostname: %s system-ip %s vpn id: %s if name: %s mac addr: %s ip-addr: %s	Configuration at specified date and time, for VPN, interface, MAC address, and IP address	E
VCONF_SYSLOG_START	1499999	Starting	Configuration process is starting	E

VDAEMON: Cisco SD-WAN Software Process

Priority: Informational

Message	Number	Message Format	Description	Action
VDAEMON_SYSLOG_DOMAIN_ID_CHANGE	500006	System Domain-ID changed from '%d' to '%d',	System domain ID changed	E
VDAEMON_SYSLOG_END	599999	—	Process ending	E
VDAEMON_SYSLOG_ORG_NAME_CHANGE	500008	System Organization-Name changed from '%s' to '%s'	System organization name changed	E
VDAEMON_SYSLOG_PEER_STATE	500003	Peer %s Public-TLOC %s Color %u %s,	Peer state changed to up or down	E
VDAEMON_SYSLOG_SITE_ID_CHANGE	500005	System Site-ID changed from '%d' to '%d'	System site ID changed	E
VDAEMON_SYSLOG_START	500001	—	Process starting	E
VDAEMON_SYSLOG_SYSTEM_IP_CHANGE	500007	System-IP changed from '%s' to '%s'	System IP address changed	E

Priority: Error

Message	Number	Message Format	Description	Action
VDAEMON_BOARD_ID_CHALLENGE_FAILED	500002	—	Board ID could not be verified	E
VDAEMON_BOARD_ID_INIT_FAILED	500001	—	Board initialization failed because board ID could not be verified	E
VDAEMON_SYSLOG_CERT_STORE_FAIL	500009	Certificate store init failed	Certificate not stored	AE
VDAEMON_SYSLOG_PEER_AUTH_FAIL	500004	Peer %s Public-TLOC %s Color %u %s	Authentication with a vdaemon peer failed	E
VDAEMON_SYSLOG_PEER_STATE	500003	Failed to read system host name	Internal error reading system hostname; device will not register with the Cisco vManage server or ZTP will fail	A

VRRP: Virtual Router Redundancy Protocol

The VRRP process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
VRRPD_STATE_CHANGE	600002	Group %d, interface %s, vpn %lu state changed to %s	VRRP interface state change	E
VRRPD_SYSLOG_END	699999	Terminating VRRPD	VRRP process is ending	E
VRRPD_SYSLOG_START	600001	Starting VRRPD	VRRP process is starting	E

WLAN: Wireless LAN Process

The wireless LAN process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
WLAN_SYSLOG_END	2300001	Terminating wlan	WLAN process is ending	E
WLAN_SYSLOG_START	2399999	Starting wlan	WLAN process is starting	E

WWAND: Cellular Process

The wireless WAN process runs only on Cisco vEdge devices.

Priority: Informational

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_ADMIN_DWL	2400010	Cellular%d interface is set for deletion	Cellular interface is about to be deleted	E
WWAN_SYSLOG_ADMIN_DOWN	2400009	Cellular%d interface is set to admin down	Cellular interface is administratively Down	E
WWAN_SYSLOG_ADMIN_UP	2400008	Cellular%d interface is set to admin up	Cellular interface is administratively Up	E
WWAN_SYSLOG_CONNECT	2400002	Connected to Cellular%d modem	Connection to cellular modem established	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_CONNECT_DATA	2400006	—	—	E
WWAN_SYSLOG_DATA_MONITOR	2400032	Info: %lld bytes left Info: exceeded by %lld bytes	Information about amount of data remaining in billing cycle	E
WWAN_SYSLOG_DATA_SESSION	2400019	Data session started successfully	Data session on cellular interface started successfully	E
WWAN_SYSLOG_DATA_SESSION_BEARER	2400028	Data bearer changed to %s (%lx)	Data carrier changed	E
WWAN_SYSLOG_DATA_SESSION_DISCONNECT	2400023	Data session disconnect: restarting session	Data session was disconnected and is restarting	E
WWAN_SYSLOG_DATA_SESSION_DISC_REASON	2400024	Data session disconnect reason: %s	Reason data session was disconnected	E
WWAN_SYSLOG_DATA_SESSION_DISC_VERB	2400025	Data session disconnect reason verbose: %s	More information about why data session disconnected	E
WWAN_SYSLOG_DATA_SESSION_DOMAIN	2400026	Packet-switched domain state change to %s: registration: %s ran: %s if: %s	Packet-switched domain changed	E
WWAN_SYSLOG_DATA_SESSION_DORMANCY	2400029	Dormancy state changed to %s	Session dormancy state changed	E
WWAN_SYSLOG_DATA_SESSION_NETWORK	2400027	Network registration changed to %s: domain: %s ran: %s if: %s	Network registration changed	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_DATA_SESSION_START	2400018	Starting data session on Cellular%e	Data session on cellular interface is starting	E
WWAN_SYSLOG_DATA_SESSION_STATE	2400020	Data session state changed to %s	Data session status	E
WWAN_SYSLOG_DATA_SESSION_STOP	2400022	Data session stopped successfully	Data session stopped	E
WWAN_SYSLOG_DISCONNECT	2400003	Disconnected LTE modem %d	Disconnection from LTE modem	E
WWAN_SYSLOG_END	2400001	Terminating WWAND	Ending WWAN process	E
WWAN_SYSLOG_FIRMWARE	2400007	Failed to get firmware details after upgrade on modem %d Firmware upgrade failed on modem %d Firmware upgrade successful on modem %d Upgrading firmware configuration on modem %d Upgrading firmware image on modem %d	Messages related to firmware upgrade on the cellular modem	E
WWAN_SYSLOG_LR_DOWN	2400012	%s%d: bringing down	Last-resort interface is shutting down	E
WWAN_SYSLOG_LR_UP	2400011	%s%d: bringing up	Last-resort interface is starting	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_MODEM_ACTIVATION	2400039	Modem activation status: %s (%lu)	Modem actual state and status	E
WWAN_SYSLOG_MODEM_PMODE	2400017	Modem is not in online mode Modem is not in online mode (tmp: %s degrees C) Modem power state is: %s (prev: %s) Modem set to %s (prev: %s) Powered off the modem %d	Messages related to modem power mode status	E
WWAN_SYSLOG_MODEM_STATE	2400034	Modem device state changed to %s	Modem state changed	E
WWAN_SYSLOG_MODEM_TEMP	2400037	Modem temperature %d degree C: %s	Modem temperature and state	E
WWAN_SYSLOG_MODEM_UP	2400035	WWAN cellular%d modem is back up	Modem reconnected	E
WWAN_SYSLOG_OMA_DM_DONE	2400041	Modem OMA DM configuration completed	Modem OMA-DM configuration finished	E
WWAN_SYSLOG_OPER_DOWN	2400014	Cellular%d set if down	Cellular interface is operationally Down	E
WWAN_SYSLOG_OPER_UP	2400013	Cellular%d set if up	Cellular interface is operationally Up	E

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_PROFILE_CHECK	2400030	Profile %lu with PDP: %s APN: %s Auth: %s User: %s	Cellular profile information	E
WWAN_SYSLOG_REBOOT	2400040	Cellular%d modem mode updated: rebooting; %s reason	Reason why cellular modem rebooted	E
WWAN_SYSLOG_SDK_DOWN	2400005	SDK got terminated: %s	Connection to software development kit terminated	E
WWAN_SYSLOG_SDK_UP	2400004	Connected to Cellular%d sdk process	Connection to cellular software development kit established	E
WWAN_SYSLOG_SIM_STATUS	2400033	SIM status changed to: %s	SIM status changed	E
WWAN_SYSLOG_START	2499999	Starting WWAND	Starting WWAN process	E
WWAN_SYSLOG_TRACK_GW_UP	2400015	Cellular%d gateway %s is reachable	Cellular gateway is reachable	E

Priority: Error

Message	Number	Message Format	Description	Action
WWAN_SYSLOG_AUTO_PROFILE_MISS	2400031	Manually configure APN profile for the data connection	Data session could not start because required APN could not be located	E
WWAN_SYSLOG_MODEM_DOWN	2400036	WWAN cellular%d modem went down	Modem is disconnected	E
WWAN_SYSLOG_MODEM_RESET	2400038	Failed to recover Cellular %d modem	Connection to modem could not be reestablished	E
WWAN_SYSLOG_TRACK_GW_DOWN	2400016	Cellular%d gateway %s is not reachable	Cellular gateway is not reachable	E

Troubleshoot a Device

You can troubleshoot connectivity or traffic health for all devices in the overlay network.

Troubleshoot Common Cellular Interface Issues

Resolve Problems with Cellular Interfaces

This topic describes the most common issues and error messages that occur with cellular connections from the router to the cellular network, and the steps to resolve them.

Insufficient Radio Signal Strength

Problem Statement

The cellular module in the router cannot detect a radio signal from the service provider network.

Identify the Problem

- The signal strength displayed in the Cisco vManage Cellular Status screen or with the **show cellular status** CLI command, or in the Cellular Radio screen or with the **show cellular radio** command is no signal, poor, or good. It should be excellent. The following table lists the ranges of signal strengths:

Table 11:

Signal	Excellent	Good	Fair	Poor	No Signal
Received signal strength indicator (RSSI)	> -58 dBm	-81 through -58 dBm	—	-82 through -95 dBm	< -96 dBm
Reference signal receive power (RSRP)	-44 through -90 dBm	-91 through -105 dBm	-106 through -120 dBm	-121 through -140 dBm	< -140 dBm
Reference signal receive quality (RSRQ)	-3 through -8 dB	-9 through -12 dB	—	-13 through -20 dB	< -20 dB
Signal-to-noise ratio (SNR)	> 10 dB	6 through 10 dB	0 through 5 dB	< 0 dB	—

- The wireless LED on the router is lit (solid or blinking) and is red, orange or yellow, or it is blinking green. It should be solid green.

Resolve the Problem

1. Examine the router to verify that both basic antennas are correctly installed.
2. Contact the service provider to verify that the location has coverage.
3. Move the router to a new location within the building.
4. Procure an additional external cabled antenna and connect it to the router.

Modem Status Remains in Low-Power Mode

Problem Statement

End users cannot connect to the cellular network, and the modem status remains in low-power mode.

Identify the Problem

- End users cannot connect to the cellular network.
- The error message "Missing or unknown APN" is generated.
- The signal strength is less than excellent.

Resolve the Problem

1. Verify that there is sufficient radio signal strength. If there is not, follow the instructions in the Insufficient Radio Signal Strength section.

2. Verify that the cellular0 interface is operational. When the cellular interface is shut down, the modem status is set to Low Power mode. To do this, from the Cisco vManage menu, choose **Monitor > Devices**.

Cisco vManage Release 20.6.x and earlier: To do this, from the Cisco vManage menu, choose **Monitor > Network**.

Then click **Real Time**, and from the **Device Options** drop-down list, choose **Interface Detail**.

To do this from the CLI, use the **show interface** command. Check that the Admin Status and Oper Status values are both Up.

3. Verify that the modem temperature is not above or below the threshold temperatures. To view the modem temperature, from the Cisco vManage menu, choose **Monitor > Devices** and select the router.

Cisco vManage Release 20.6.x and earlier: To do this, from the Cisco vManage menu, choose **Monitor > Network**.

Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Modem**.

From the CLI, use the **show cellular modem** command.

4. Check that the access point name (APN) in the profile for the cellular0 interface matches the name expected by your service provider. Some service providers require that you configure the APN, and they include configuration instructions in the SIM card package.

- a. To check which APN name is configured, from the Cisco vManage menu, choose **Monitor > Devices** and select the router.

Cisco vManage Release 20.6.x and earlier: To do this, from the Cisco vManage menu, choose **Monitor > Network**.

Then click **Real Time**, and from the **Device Options** drop-down list, choose **Cellular Profiles**.

From the CLI, use the ; **show cellular profiles** command. The APN column shows the name of the APN. Each profile specifies an access point name (APN), which is used by the service provider to determine the correct IP address and connect to the correct secure gateway. For some profiles, you must configure the APN.

- b. If the APN is not the one required by the service provider, configure the correct APN. From the Cisco vManage menu, choose **Configuration > Templates** and use the **Cellular Profile** feature template.

To configure this from the CLI, use the **cellular cellular0 profile apn** command.

- If none of the previous steps works, reset the cellular interface.

Error Messages

The following table list the most common error messages that are displayed regarding cellular interfaces:

Table 12:

Error Message	Problem Statement	How Do I Fix the Problem
Authentication failed	End user authentication failed, because the service provider cannot authenticate either the user's SIM card or the Cisco vEdge device SIM card.	Contact the cellular service provider.
Illegal ME	The service provider denied access to an end user, because the end user is blocked from the network.	Contact the cellular service provider.
Illegal MS	The service provider denied access to an end user, because the end user failed the authentication check.	Contact the cellular service provider.
Insufficient resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
IPv4 data call throttled	The SIM card being used in the Cisco vEdge device requires that you configure static APN.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Missing or unknown APN	End users cannot connect to the cellular network, either because an APN is required and is not included in the cellular profile or because the APN could not be resolved by the service provider.	See the profile's APN, as described in Modem Status Remains in Low-Power Mode , above.
MS has no subscription for this service	The service provided denied access to an end user, because the end user has no subscription.	Contact the cellular service provider.
Network failure	The service provider network is experiencing difficulties.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.

Error Message	Problem Statement	How Do I Fix the Problem
Network is temporarily out of resources	The service provider network is experiencing congestion because of insufficient resources and cannot provide the requested service to an end user.	The Cisco vEdge device automatically tries to reconnect. (The duration between retries depends on the service provider.) If the issue does not resolve itself, contact the cellular service provider.
Operator has barred the UE	The service provided denied access to an end user, because the operator has barred the end user.	Contact the cellular service provider.
Requested service option not subscribed	The SIM card being used in the Cisco vEdge device requires that you configure a static APN entry.	Verify whether the data plan associated with the SIM card requires a static APN. If so, change the APN to the name specified the SIM card instructions, as described in Modem Status Remains in Low-Power Mode , above.
Service not supported by the PLMN	The Public Land Mobile Network (PLMN) does not support data service.	Contact the cellular service provider.

Troubleshoot WiFi Connections

This topic describes how to check and resolve connection problems between a WiFi client and a WiFi network that is provided by a WiFi router. The procedures described here are applicable to devices that support WiFi only.

Check for WiFi Connection Problems

If a WiFi client is unable to connect to a WiFi network when a router is providing the WiFi network, follow these steps to determine the source of the problem. To perform each step, use a method appropriate for the WiFi client.

1. Verify that the WiFi client can locate the service identifier (SSID) advertised by the router. If the client cannot find the SSID, see the section, SSID Not Located.
2. Verify that the WiFi client can connect to the SSID advertised by the router. If the client cannot connect to the SSID, see the section, SSID Connection Fails.
3. Verify that the WiFi client has been assigned an IP address. If the client cannot obtain an IP address, see the section, Missing IP Address.
4. Verify that the WiFi client can access the Internet. If the client cannot connect to the Internet, see section, Internet Connection Failure.
5. If the WiFi client connection is slow or if you notice frequent disconnects, see section, WiFi Speed Is Slow.

Resolve Problems with WiFi Connections

This section describes the most common issues that occur with WiFi connections between a WiFi client and a router, and it describes steps to resolve the issues.

SSID Not Located

Problem Statement

The WiFi client cannot locate the SSID advertised by the router.

Resolve the Problem

1. Ensure that the basic service set identifier (BSSID) address for the SSID is valid:
 - a. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
 - b. Choose a device from the device list that appears.
 - c. From the left pane, choose WiFi. The right pane displays information about WiFi configuration on the router.
 - d. In the right pane, locate the SSID. Check that the BSSID for this SSID does not have a value of 00:00:00:00:00:00.
 - e. If the BSSID is 00:00:00:00:00:00, the WLAN (VAP) interface for this SSID may be misconfigured. Ensure that the WLAN interface has been added to a bridge during the configuration process. To view the running configuration of the device, from the Cisco vManage menu, choose **Configuration > Devices**. For the desired device, click ...and choose **Running Configuration**.

To view the running configuration of the device from the CLI, use the **show running-config** command. To add the WLAN interface to a bridge — from the Cisco vManage, choose **Configuration > Templates**.

Click **Feature Templates**, and choose the **Bridge** feature template.



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

2. Eliminate static channels. A static channel is one where you explicitly configure the radio channel rather than allowing the router to automatically select the best radio channel. A slow static channel may appear to be an unreachable SSID.
 - a. View the current SSID channel setting for the router. To do this, from the Cisco vManage menu, choose **Monitor > Devices** and choose a device from the list of devices that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose WLAN Clients or WLAN Radios.
From the CLI, use the **show wlan clients** or **show wlan radios** command.
 - b. If the channel is set to a specific number, change the value to "auto". To do this, use the WiFi Radio feature template in Cisco vManage.
From the CLI, use the **wlan channel auto** command.

3. Ensure that the WiFi client is using the same radio band as the router, either 2.4 GHz (for IEEE 802.11b/g/n) or 5 GHz (for IEEE802.11a/n/ac):
 - a. Check which radio band the WiFi client supports.
 - b. Check the router's Select Radio setting. To do this, from the Cisco vManage menu, choose **Monitor > Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Radios**.

From the CLI, use the **show wlan radios** command.
 - c. If the router and WiFi client radio band settings do not match, either change the WiFi client's radio band or change the settings on the router so that they match. To do this, use the Wifi Radio feature template.

From the CLI, use the **wlan** command.

SSID Connection Fails

Problem Statement

The WiFi client can locate the SSID advertised by the router but cannot connect to it.

Resolve the Problem

1. If you configure passwords locally on the router, ensure that the WiFi client's password matches the SSID's password.
2. If you are using a RADIUS server, ensure that the RADIUS server is reachable and that the WiFi client's username and password match the RADIUS configuration:
 - a. To verify that the RADIUS server is reachable from the router, ping the server. To do this in Cisco vManage, ping a device. From the CLI, use the **ping** command.
 - b. Check for matching passwords on the RADIUS server and WiFi client.
3. Ensure that you do not exceed the maximum number of clients for this SSID:
 - a. Verify the number of used clients and the maximum number of clients:
 - From the Cisco vManage menu, choose **Monitor > Devices** and choose a device from the device list that appears. From the left pane, select WiFi. In the right pane, locate the SSID. Check the No. of Clients field. If the used/maximum values are equal, no more clients can connect to this SSID.
 - From the CLI, use the **show wlan interfaces detail** command.
 - b. If needed, increase the maximum clients setting for your SSID. To do this use the WiFi SSID feature template in Cisco vManage.

From the CLI, use the **max-clients** command.
4. Ensure that the WiFi client supports WPA2 management security:
 - a. Check your Management Security setting. To do this, from the Cisco vManage menu, choose **Monitor > Devices** and choose a device from the device list that appears. Then click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Interfaces**.

From the CLI, use the **show wlan interfaces** command. If the management security value is set to "required," the WiFi client must support WPA2 security.

- b. If necessary, change the Management Security setting for your SSID to "optional" or "none." To do this in Cisco vManage, use the WiFi SSID feature template.

From the CLI, use the **mgmt-security** command.

Missing IP Address

Problem Statement

The WiFi client can connect to the SSID, but cannot obtain an IP address.

Resolve the Problem

Ensure that a DHCP server is reachable and has an available IP address in its address pool:

1. If the router is acting as a DHCP helper (DHCP relay agent), ping the DHCP server to ensure that it is reachable from the router. From the CLI, use the **ping** command.
2. If you are using a remote DHCP server, check that the remote DHCP server has an available IP address in its address pool.
3. If the router is acting as the local DHCP server:
 - a. View the number of addresses being used. From the Cisco vManage menu, **Monitor > Devices** and choose a device from the device list that appears. Next, click **Real Time**, and from the **Device Options** drop-down list, choose **DHCP Servers**.

From the CLI, use the **show dhcp server** command.

- b. Compute the number of IP addresses in the pool based on the configured DHCP address pool size and the number of addresses excluded from the DHCP address pool. To view these values in Cisco vManage, from the Cisco vManage menu, choose **Configuration > Devices**. For the desired router, click **...** and choose **Running Configuration**.

To view them from the CLI, use the **show running-config** command.

- c. If necessary, increase the range of addresses in the router's DHCP address pool using the DHCP-Server feature template in Cisco vManage.

Internet Connection Failure

Problem Statement

The WiFi client is connected to the SSID and has an IP address, but it cannot connect to the Internet.

Resolve the Problem

Ensure that the WiFi client has received the correct default gateway and DNS settings from the DHCP server:

1. If the DHCP server is remote, check the settings on the server.
2. If the router is the DHCP server, ensure that the default gateway and DNS server settings are the same as those on the WiFi client. To view the settings in Cisco vManage, from the Cisco vManage menu, choose **Monitor > Devices**, and choose a device from the device list that is displayed. Click **Real Time**, and in the **Device Options** drop-down list, choose **DHCP Interfaces**.

From the CLI, use the **show dhcp interface** command.

WiFi Speed Is Slow

Problem Statement

The WiFi client can connect to the Internet, but the connection speed is slow.

Resolve the Problem

Allow the router to choose the best WiFi channel:

1. View the current SSID channel setting for the router. To do this in Cisco vManage, from the Cisco vManage menu, choose **Monitor > Devices**, and choose a device from the device list that is displayed. Click **Real Time**, and in the **Device Options** drop-down list, choose **WLAN Clients**.

From the CLI, use the **show wlan clients** or **show wlan radios** command.

2. If the channel is set to a specific number, change the value to "auto". To do this in Cisco vManage, use the WiFi Radio feature template.

From the CLI, use the **wlan channel auto** command.

View Audit Log Information

Set Audit Log Filters

Table 13: Feature History

Feature Name	Release Information	Description
Compare Template Configuration Changes Using Audit Logs	Cisco IOS XE Release 17.9.1a Cisco vManage Release 20.9.1	This feature introduces a Config Diff option for audit logs of device templates and feature templates to view the configuration changes when a template is not attached to a device.

1. From the Cisco vManage menu, choose **Monitor > Logs > Audit Log**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Audit Log**.
2. Click the **Filter**.
3. In the **Module** field, choose the entity for which you are collecting audit logs. You can choose more than one entity.
4. Click **Search** to search for logs that match the filter criteria.

Cisco vManage displays a log of activities both in table and graphical format.

Export Audit Log Data in CSV Format

To export data for all audit logs to a file in CSV format, click **Export**.

Cisco vManage downloads all data from the audit logs table to an Excel file to a CSV format. The file is downloaded to your browser's default download location and is named Audit_Logs.csv.

View Audit Log Details

To view detailed information about any audit log:

1. Choose the audit log row of from the table
2. For the desired row, click ... and choose **Audit Log Details**.

The **Audit Log Details** dialog box opens, displaying details of the audit log.

View Changes to a Configuration Template

You can view changes for previous and current configuration made on a template. To view configuration changes made to a template, do the following:

1. Click the audit log row in the table where the module type is a template.
2. Click ... adjacent to the template module and click **Config Diff**.

The **Config Difference** pane displays a side-by-side view of the differences between the configuration that was originally in the template and the changes made to the configuration. To view the changes inline, click **Inline Diff**.

To view the updated configuration on the device, click **Configuration**.

Starting from Cisco IOS XE Release 17.6.1a and Cisco SD-WAN Release 20.6.1, for template and policy configuration changes, the **Audit Logs** option displays the action performed. To view the previous and current configuration for any action, click **Audit Log Details**. Audit logs are collected when you create, update, or delete device or feature templates, and localized or centralized, and security policies. Audit logs shows the changes in API payloads when templates or policies are attached or not attached.

View and Monitor Cellular Interfaces

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

Monitor Cellular Interfaces

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

Verify Signal Strength

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage 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 14:

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 vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage 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 Real Time Monitoring Options

Table 15: Feature History

Feature Name	Release Information	Description
Additional Real Time Monitoring Support for Routing, License, Policy, and Other Configuration Options	Cisco IOS XE Release 17.6.1a Cisco SD-WAN Release 20.6.1 Cisco vManage Release 20.6.1	This feature adds support for real-time monitoring of numerous device configuration details, including routing, policy, Cloud Express, Cisco vBond Orchestrator, TCP optimization, SFP, tunnel connection, license, logging, and Cisco Umbrella information. Real-time monitoring in Cisco vManage is similar to using show commands in the CLI of a device. There are many device configuration details for Cisco vManage. However, only a subset of the device configuration details is added in Cisco IOS XE Release 17.6.1a and Cisco vManage Release 20.6.1.
Additional Real Time Monitoring Support for AppQoE and Other Configuration Options	Cisco IOS XE Release 17.9.1a Cisco SD-WAN Release 20.9.1 Cisco vManage Release 20.9.1	This feature adds support for real-time monitoring of AppQoE and other device configuration details in Cisco vManage.

View AppQoE Information

Minimum release: Cisco vManage Release 20.9.1

To view AppQoE information on a device, perform the following steps:

- From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
- Choose a device from the list of devices that is displayed.
- Click **Real Time** in the left pane.
- Click **Device Options**, and choose one the following commands:

Device Option	Command	Description
AppQoE Active Flow Details	show sdwan appqoe flow flow-id [flow_id]	Displays the details of a single specific flow.
AppQoE Expired Flows Summary	show sdwan appqoe flow closed all	Displays the summary of AppQoE expired flows.
AppQoE Active Flows Summary	show sdwan appqoe flow vpn-id [vpn_id] server-port [server_port]	Displays flows for a specific VPN.
AppQoE Expired Flow Details	show sdwan appqoe flow closed flow-id [flow_id]	Displays the AppQoE Expired Flow details for a single specific flow.

View a Configuration Commit List

Minimum release: Cisco vManage Release 20.9.1

To view a configuration commit list on a device, perform the following steps:

- From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
- Choose a device from the list of devices that is displayed.
- Click **Real Time** in the left pane.
- Click **Device Options**, and choose the following command:

Device Option	Command	Description
Configuration Commit List	show configuration commit list	Displays the configuration commit list.

View the System Clock

Minimum release: Cisco vManage Release 20.9.1

To view the system clock on a device, perform the following steps:

- From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
- Choose a device from the list of devices that is displayed.
- Click **Real Time** in the left pane.
- Click **Device Options**, and choose the following command:

Device Option	Command	Description
System Clock	show clock	Displays the system clock date and time.

View TCP Optimization Information

View WAN Throughput

If TCP optimization is enabled on a router, you can view information about how the optimization affects the processing and throughput of TCP data traffic on the router:

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. Choose a device from the list of devices that displays.
3. In the left pane, click **WAN Throughput**. The right pane displays the WAN throughput, in megabits per second.

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

- Chart Options bar—Located directly under the device name, this bar includes the Filter Options drop-down and time periods. Click **Filter** to limit the data to display based on VPN, local TLOC color, destination IP address, remote TLOC color, and remote system IP address. Click a predefined or custom time period for which to display data.
- Average optimized throughput information in graphical format.
- WAN graph legend—Identifies non-optimized and TCP optimized packet throughput.

The lower part of the right pane shows the hourly average throughput and the total optimized throughput, both in megabits per second.

Click **TCP Optimization–Connections** in the left pane to view status information about all the tunnels over which the most TCP-optimized traffic is flowing. The upper part of the right pane contains the following elements:

- TCP Optimization Connections in graphical format.
- Connection State boxes—Select the connection state or states to view TCP optimization information.

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

- Filter criteria.
- Flow table that lists information about each of the tunnels, including the tunnel's connection state.

View TCP-Optimized Flows for Cisco vEdge Devices

To view information about TCP-optimized flows on a Cisco vEdge device:

1. From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
2. Choose a device from the list of devices that is displayed.
3. Click **Real Time** in the left pane.
4. Click **Device Options**, and choose one of the following commands:



Note The following options are available when you choose a Cisco vEdge device.

Device Option	Command	Description
TCP Optimization Active Flows	show app tcp-opt	Displays information about active TCP-optimized flows.
TCP Optimization Expired Flows	show app tcp-opt	Displays information about expired TCP-optimized flows.
TCP Optimization Summary	show app tcp-opt	Displays a summary of the TCP-optimized flows.

View TLOC Loss, Latency, and Jitter Information

- From the Cisco vManage menu, choose **Monitor > Devices**.
Cisco vManage Release 20.6.x and earlier: From the Cisco vManage menu, choose **Monitor > Network**.
- Choose a device from the list of devices that is displayed.
- In the left pane, click **TLOC** under the **WAN** area. The right pane displays the aggregated average loss or latency/jitter information for all TLOC colors.

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

- Chart Options— Includes the Chart Options drop-down and time periods. Click Chart Options to select the type of data to view. Click a predefined or custom time period for which to view data.
- TLOC information in graphical format. The time interval in the graph is determined by the value of the BFD application-aware routing poll interval .
- TLOC graph legend—Choose a TLOC color to display information for just that TLOC.

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

- Search box—Includes the Search Options filter.
- TLOC color table that lists average jitter, loss, and latency data about all TLOCs. By default, the first six colors are selected. 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 TLOC colors. You can select and view information for a maximum of 30 TLOCs at one time.
 - Click **Application Usage** to the right to view the SD-WAN Application Intelligence Engine (SAIE) flow information for that TLOC.

**Note**

-
- Beginning with Cisco vManage Release 20.8.1, the **Application Usage** column and the **Application Usage** links are removed from the **Monitor > Devices > WAN – Tunnel** window. After you have configured on-demand troubleshooting for a device, you can view SAIE usage data based on the selected filters or based on application families sorted by usage.
 - In Cisco vManage Release 20.7.x and earlier releases, the SD-WAN Application Intelligence Engine (SAIE) flow is called the deep packet inspection (DPI) flow.

For more information on configuring on-demand troubleshooting, see [On-Demand Troubleshooting](#). For more information on viewing SAIE flows, see [View SAIE Flows](#).
