Alarms, Events, and Logs

Alarms

Table 1: Feature History

Feature	Release Information	Description
Optimization of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.5.1a Cisco SD-WAN Release 20.5.1 Cisco vManage Release 20.5.1	This feature optimizes the alarms on Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

Feature	Release Information	Description
Grouping of Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.11.1a Cisco vManage Release 20.11.1	The following enhancements are added to alarms: • Alarms are filtered and grouped for devices and sites based on severity. • View alarm details for a single site in the **Overview** dashboard. • View alarms for a particular device by clicking the … icon in the **Monitor > Devices** window. • View the top five alarms for a particular site in the **Monitor > Overview** window by choosing the **Site Topology** view icon and clicking the site. • View events related to an alarm in the **Related Event** column in the alarms filter.
Heatmap View for Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the alarms as **Critical**, **Major**, or **Medium & Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of alarms in a severity level.
Alarm Notifications Using WebHooks	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Configure a WebHook URL in Cisco SD-WAN Manager to receive alarm notifications in Webex or Slack.
Alarm Notifications Using Custom WebHooks Over Management VPN 512	Cisco IOS XE Catalyst SD-WAN Release 17.16.x Cisco Catalyst SD-WAN Manager Release 20.16.1	Configure alarm notifications using custom webhooks over management VPN 512 for increased security in a single-tenant or a multitenant setup.

Feature	Release Information	Description
Cloud OnRamp for SaaS Alarms	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	A Cisco IOS XE Catalyst SD-WAN device triggers three new alarms. These alarms indicate the status of CoR-SaaS application paths. This feature adds a **path-status** field to the **cloudexpress-application-change** notification. Alarms are categorized into into Major, Medium and Minor based on the path status (unreachable, reachachable, disabled).
Policy Download Failure Alarm	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download fails.

Information About Alarms

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

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

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

When a site is down, Cisco SD-WAN Manager reports the following alarms:

- Site down
- Node down
- TLOC down

Cisco SD-WAN Manager 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 SD-WAN Manager intelligently suppresses redundant alarms. For example, if all the TLOCs in a node are down, Cisco SD-WAN Manager 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	

Scenario	Alarms Displayed	
Link 1 down Link 2 up.	bfd-tloc-1_down	bfd-tloc-1_down
Link 1 down Link 2 down	bfd-site-1_down bfd-node-1_down, bfd-tloc-1_down, and bfd-tloc-2_down are suppresed 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

Alarms Details

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

The Cisco SD-WAN Manager generates alarms when a state or condition changes, such as when a software component starts, transitions from down to up, or transitions from up to down. The severity indicates the seriousness of the alarm. When you create email notifications, the severity that you configure in the notification determines which alarms you can receive email notifications about.

Alarm States

Cisco SD-WAN Manager 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.

Note From Cisco vManage Release 20.11.1, the Medium alarms appear in green and the Minor alarms appear in blue.

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

To view alarm details such as alarm name, sevcerity, and alarm description:

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

2. Click **Export** to export data for all alarms to a file in CSV format.

   Cisco SD-WAN Manager downloads data from the alarms table to the default download location of your browser. The data is downloaded as a CSV file with the name *alarms-mm-dd-yyyy.csv*.

3. Open the downloaded file to view alarm details.

For detailed information on each alarm, please see Cisco IOS XE Catalyst SD-WAN Alarms Guide.

Alarm Fields

Alarm messages can contain the following fields that provide more information about the alarm:

Table 2: Alarm Fields

Field	Description
Acknowledged	Whether the alarm has been viewed and acknowledged. This field allows Cisco SD-WAN Manager to distinguish between alarms that have already been reported and those that have not yet been addressed. To acknowledge an alarm, use the following API post call: https://*vmanage-ip-address*:8443/dataservice/alarms/markviewed Specify the data as: {“uuid”: [<*uuids of alarms to acknowledge*>]}
Active	Whether the alarm is still active. For alarms that are automatically cleared, when a network element recovers, the alarm is marked as "active":false.
Cleared By	Universally Unique IDentifier (UUID) of alarm to clear current alarm.
Cleared Time	Time when alarm was cleared. This field is present of for alarms whose "active" field is false.
Component	The software component for this alarm.
Devices	List of system IP addresses or router IDs of the affected devices.
Entry Time	Time when the alarm was raised, in milliseconds, expressed in UNIX time.
Message	Short message that describes the alarm.
Possible Causes	Possible causes for the event.
Rule Name Display	Name of the alarm. Use this name when querying for alarms of a particular type.
Suppressed	Whether this alarm is suppressed by other alarm.
Tenant	Indicates the tenant ID.
Severity	Severity of the alarm: critical, major, medium, minor.
Severity Number	Integer value for the severity: 1 (critical), 2 (major), 3 (medium), 4 (minor)
UUID	Unique identifier for the alarm

Field	Description
Values	Set of values for all the affected devices. These values, which are different for each alarm, are in addition to those shown in the "devices" field.
Values Short Display	Subset of the values field that provides a summary of the affected network devices.

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

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

View Alarms

You can view alarms from the Cisco SD-WAN Manager dashboard by clicking the bell icon at the top-right corner. The alarms are grouped into Active or Cleared.

From Cisco vManage Release 20.11.1, when you click the bell icon at the top-right corner, the **Notifications** pane is displayed. Click the gear icon in this pane to filter or group alarms based on the following criteria:

- **Object**: Alarms are grouped based on the device for which the alarm is generated.
- **Severity**: Alarms are grouped based on the alarm severity.
- **Type**: Alarms are grouped based on the alarm type.

By default, alarms are displayed for the last 24 hours.

Alternatively, follow these steps to view alarms from the **Alarms** screen in Cisco SD-WAN Manager.

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

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

   The alarms are displayed in graphical and tabular formats.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

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.

From Cisco vManage Release 20.11.1, a new column called **Related Event** is added to the alarms page. This column displays events, related to an alarm, that occurs around the time the alarm is generated.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, you can use the following commands to view more details about alarms:

- **show sdwan alarms detail**: Provides detailed information about each alarm separated by a new line.
- **show sdwan alarms summary**: Provides alarm details such as the timestamp, event name, and severity in a tabular format.

The following is a sample output of the **show sdwan alarms detail** command:

```
vm5#show sdwan alarms detail

alarms 2023-06-01:00:38:46.868569
 event-name     geo-fence-alert-status
 severity-level minor
 host-name      Router
 kv-pair        [ system-ip=:: alert-type=device-tracking-stop alert-msg=Device Tracking
stopped in Geofencing Mode latitude=N/A longitude=N/A geo-color=None ]
-----------------------------------------------------

alarms 2023-06-01:00:38:47.730907
 event-name     system-reboot-complete
 severity-level major
 host-name      Router
 kv-pair        [ ]
-----------------------------------------------------

alarms 2023-06-01:00:39:00.633682
 event-name     pki-certificate-event
 severity-level critical
 host-name      Router
 kv-pair        [ trust-point=Trustpool event-type=pki-certificate-install
valid-from=2008-11-18T21:50:24+00:00 expires-at=2033-11-18T21:59:46+00:00 is-ca-cert=true
subject-name=cn=Cisco Root CA M1,o=Cisco issuer-name=cn=Cisco Root CA M1,o=Cisco
serial-number=2ED20E7347D333834B4FDD0DD7B6967E ]
-----------------------------------------------------
```

The following is a sample output of the **show sdwan alarms summary** command:

```
vm5#show sdwan alarms summary

time-stamp                    event-name                                    severity-l

-------------------------------------------------------------------------------------------
2023-06-01:00:38:46.868569      geo-fence-alert-status                        minor

2023-06-01:00:38:47.730907      system-reboot-complete                        major

2023-06-01:00:39:00.633682      pki-certificate-event                       critical

2023-06-01:00:39:00.644209      pki-certificate-event                       critical

2023-06-01:00:39:00.649363      pki-certificate-event                       critical

2023-06-01:00:39:00.652777      pki-certificate-event                       critical

2023-06-01:00:39:00.658387      pki-certificate-event                       critical

2023-06-01:00:39:00.661119      pki-certificate-event                       critical

2023-06-01:00:39:00.665882      pki-certificate-event                       critical

2023-06-01:00:39:00.669655      pki-certificate-event                       critical

2023-06-01:00:39:00.674912      pki-certificate-event                       critical

2023-06-01:00:39:00.683510      pki-certificate-event                       critical

2023-06-01:00:39:00.689850      pki-certificate-event                       critical

2023-06-01:00:39:00.692883      pki-certificate-event                       critical

2023-06-01:00:39:00.699143      pki-certificate-event                       critical

2023-06-01:00:39:00.702386      pki-certificate-event                       critical
```

```
2023-06-01:00:39:00.703653      pki-certificate-event                       critical

2023-06-01:00:39:00.704488      pki-certificate-event                       critical

2023-06-01:00:39:01.949479      pki-certificate-event                       critical

2023-06-01:00:40:38.992382      interface-state-change                        major

2023-06-01:00:40:39.040929      fib-updates                                   minor

2023-06-01:00:40:39.041866      fib-updates                                   minor
```

For more information, see *Troubleshooting Commands* in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

Filter Alarms

You can filter alarms to view details about alarms of interest.

Set Alarm Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **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 SD-WAN Manager displays the alarms in both table and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

Set Advanced Alarm Filters

From Cisco vManage Release 20.11.1, you can set advanced filters to search for alarms that are generated by sites or devices. To set advanced filters:

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.
2. Click **Advanced Filter**.
3. In the **Object Type** drop-down menu, choose either **Site** or **Device** for which you want to view alarms.
4. In the **Object List** drop-down menu, choose either **Site ID** or **Device IP** for which you want to view alarms.

   You can choose more than one site or device.
5. In the **Severity** drop-down menu, choose one or more alarm severity levels from the drop-down list.

6. In the **Type** drop-down menu, choose one or more alarm names from the drop-down list.
7. Click **Apply Filters** to view alarms that match the filter criteria.

   The **Custom Filter Condition** allows you to filter alarms based on the OR condition, for example, 1 OR 2 OR 3.

You can add up to five filters. To delete a filter, click the **Bin** icon.

Cisco SD-WAN Manager displays the alarms in both table and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays alarms.

Export Alarms

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

Cisco SD-WAN Manager downloads data from the alarms table to the default download location of your browser. The data is downloaded as a CSV file with the name *alarms-mm-dd-yyyy.csv*, where mm, dd, and yyyy are the month, day, and year that the file was downloaded.

Alarms data displayed on the graph can also be looked up in the downloaded 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 downloaded file against a date and time range between 15/Feb/2022 3:00 AM and 15/Feb/2022 3:29 AM.

Alarm Notifications

You can configure Cisco SD-WAN Manager to send email notifications when alarms occur on devices in the overlay network.

Enable Email Notifications

Configure SMTP and email recipient parameters to enable email notifications for alarms. Configure the SMTP and email recipient parameters on this screen:

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. In **Alarm Notifications**, choose **Enabled**.

   From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.
3. Check the **Email Settings** check box.
4. Choose the security level for sending the email notifications. The security level can be **None**, **SSL**, or **TLS**.
5. In the **SMTP Server** field, enter the name or the IP address of the SMTP server to receive the email notifications.
6. 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.
7. In the **From address** field, enter the full email address to include as the sender in email notifications.

8. 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.
9. 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.
10. Click **Save**.

Note The email is sent from Cisco SD-WAN Manager 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**, check whether **Alarm Notifications** is enabled and, **Email Settings** check box is checked.

From Cisco Catalyst SD-WAN Manager Release 20.13.1, click the toggle button to enable cloud services.

From Cisco Catalyst SD-WAN Manager Release 20.15.1, configure Slack or Webex webhooks to receive alarm notifications.

To send email notifications when alarms occur:

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

   From the Cisco SD-WAN Manager menu, choose **Monitor** > **Alarms**.
2. Click **Alarm Notifications**. A list of configured notifications is displayed in the table.
3. Click **Add Alarm Notifications**.
4. In the **Notification Name** field, enter a name for the email notification. The name can be up to 128 characters and can contain only alphanumeric characters.
5. Expand the **Alarm Type** filter and do the following to configure the parameters:
   - From the **Object Type** drop-down list, choose a site or device you want to view the alarms for.
   - From the **Object List** drop-down list, choose a site ID or a device based on the type of object you have selected.
   - From the **Severity** drop-down list, choose the alarm severity.
   - From the **Types** drop-down list, choose an alarm type.
6. Expand the **Delivery Method** filter and click the following options to configure the alarm delivery method.
   a. Check the **Email** check box to trigger an email an alarm notification event occurs.
      1. In the **Email** field, enter one or more email addresses.
      2. (Optional) Click **Add New Email List** and enter an email list, if desired.
      3. 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.

b. Check the **WebHook** check box to trigger an HTTP callback to a webhook channel when an alarm notification event occurs.

1. From the **Choose a Channel for Webhook** drop-down list, choose a webhook channel to receive alarm notifications in
   - Cisco Webex
   - Slack
   - Custom
2. In the **WebHook URL** field, enter the URL of the webhook server.

   To create a webhook URL for Slack, go to *api.slack.com* see the section "Sending messages using incoming webhooks".

   To create a webhook URL for Webex, go to WebEx App Hub and see the section Incoming Webhooks.
3. In the **WebHook Threshold** field, enter the threshold value.

   The value you enter indicates the number of notifications that you receive for that webhook URL per minute. For example, if the **WebHook Threshold** value is 2, you receive two notifications for that webhook URL per minute. Notifications that are generated beyond the threshold are not delivered.
4. (Optional) From Cisco Catalyst SD-WAN Manager Release 20.16.1, if you have chosen **Custom** from the **Choose a Channel for Webhook** option, configure these additional parameters:

Field	Description
Username	Enter a username for authentication.
Password	Enter a password for authentication.
Network Connectivity	
Source VPN	From the drop-down list, choose a source VPN. • **0**: Transport VPN • **512**: Management VPN. Configure these fields if you have specified the tenant to manage the webhook notification services. These fields do not appear if they are managed by the provider. • (Optional) **Source Subnet**: Enter the VPN IP subnet (VXLAN tunnel VPN IP subnet) where the webhook server is located. • (Optional) **Destination VPN**: Enter the destination VPN of the webhook server.

7. Click **Add**.

View and Edit Email Notification

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

   From the Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

   From the Cisco SD-WAN Manager 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 SD-WAN Manager menu, choose **Monitor** > **Logs** > **Alarms**.

   From the Cisco SD-WAN Manager 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**.

Events

Table 3: Feature History

Feature Name	Release Information	Description
Event Notifications Support for Cisco IOS XE Catalyst SD-WAN Devices	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r	This feature adds support for event notifications, for Cisco IOS XE Catalyst SD-WAN devices.

Feature Name	Release Information	Description
Monitoring Event Trace for OMP Agent and SD-WAN Subsystem	Cisco IOS XE Catalyst SD-WAN Release 17.2.1r Cisco SD-WAN Release 20.1.1	This feature enables monitoring and controlling the event trace function for a specified SD-WAN subsystem. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems.
Grouping of Events	Cisco vManage Release 20.11.1 Cisco IOS XE Catalyst SD-WAN Release 17.11.1a	The following enhancements are added to events: • Events are filtered and grouped based on severity for devices and sites. • View events for a particular device by clicking the … icon in the **Monitor > Devices** window. • View the top five events for a particular site in the **Monitor > Overview** window by choosing the **Site Topology** view icon and clicking the site.
Heatmap View for Events	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	In the heatmap view, a grid of colored bars displays the events as **Critical**, **Major**, or **Minor**. You can hover over a bar or click it to display additional details at a selected time interval. The intensity of a color indicates the frequency of events in a severity level.
Policy Enforcement Status	Cisco Catalyst SD-WAN Manager Release 20.18.1	Raised when a data policy download is successful.

Information About Events

When something of interest happens on an individual device in the overlay network, the device reports the event in the following ways:

- Send a notification to Cisco SD-WAN Manager. Cisco SD-WAN Manager filters the event notifications and correlates related events, and it consolidates major and critical events into alarms.
- Send an SNMP trap to the configured trap target. For each SNMP trap that a device generates, the device also generates a corresponding notification message.
- Generate 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.

Notifications are messages that the device sends to the Cisco SD-WAN Manager server.

Note All task logs, including activity logs, adminstration, and device logs, are always displayed in UTC timezone. This is the default and only supported timezone for these logs, irrespective of the Cisco SD-WAN Manager or local timezone settings.

Events Details

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

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

   The screen displays events in both graphical and tabular format.

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays the events.

2. Click **...** and choose **Device Details** to view detailed information about any event generated on a device.

View Events by 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
 !
```

To view information about a device on which an event was generated, for Cisco IOS XE Catalyst SD-WAN devices, you can use the **show sdwan notification stream** 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.

```
Device# show sdwan notification stream
notification
 eventTime 2020-03-03T02:50:04.211317+00:00
sla-change
  severity-level major
  host-name SanJose
  system-ip 4.4.4.103
  src-ip 10.124.19.15
  dst-ip 10.74.28.13
  proto ipsec
  src-port 12426
  dst-port 12346
  local-system-ip 4.4.4.103
  local-color default
  remote-system-ip 4.4.4.106
  remote-color biz-internet
  mean-loss 17
  mean-latency 13
  mean-jitter 19
  sla-classes None
  old-sla-classes Voice-And-Video
!
!
```

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.6.3, the **alarms alarm bfd-state-change syslog** command is used to view the BFD state change syslog message for any BFD state change event in the device. For complete details, see alarms alarm bfd-state-change syslog command.

```
Device(config-system)# alarms alarm bfd-state-change syslog
Device(config-alarm-bfd-state-change)# commit
```

Here is an example for BFD state change syslog message:

```
Jul 10 07:09:07.583: %Cisco-SDWAN-vm5-FTMD-5-NTCE-1000009: BFD-session 10.1.15.15:12346 ->
 10.1.16.16:12366,
local-tloc-index: 32775 -> remote-tloc-index: 32777, TLOC- local sys-ip: 172.16.255.15,
local color: lte -> remote
sys-ip: 172.16.255.16, remote color: lte, encap: IPSEC, new state->UP delete:false,
reason:REMOTE_FSM
```

Running configuration after enabling BFD state change:

```
 Device# show sdwan running-config
system
 gps-location latitude 35.0
 gps-location longitude -120.0
 system-ip             170.16.1.1
 simulated-devices     27 2
 simulated-color       red blue
 simulated-wan-ip      192.168.1.1
 domain-id             1
 site-id               10000
 admin-tech-on-failure
 organization-name     "vIPtela Inc Regression"
 vbond 10.0.12.26
 alarms alarm bfd-state-change
  syslog
 !
!
```

View Events

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

   From Cisco Catalyst SD-WAN Manager Release 20.12.1, the heatmap view displays the events.

2. Click **...** and choose **Device Details** to view device details for a specific event.

FailoverEvents

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.16.1

Failover events notify users of SIM failover events. A SIM failover event occurs when the currently active cellular link, whether with the primary or secondary SIM or carrier, loses connection and switches to the other SIM or carrier. When this happens, the device sends a **sim-fail-over** event to Cisco SD-WAN Manager.

Filter Events

Set Event Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Click the **Filter** icon from the search box.
3. Choose the time of the event from the **Event Time** drop-down list.
4. Choose the name of the host, from the **Hostname** drop-down list.
5. Choose the system IP of the devices from the **System IP** drop-down list to view generated events.
6. Choose the event name, from the generated events, from the **Name** drop-down list. You can choose more than one event name.
7. Choose the event severity level from the **Severity** drop-down list.

   The events generated by Cisco Catalyst SD-WAN devices are classified as:

   a. Critical—indicates that action needs to be taken immediately.

   b. Major—indicates that the problem needs immediate attention from you but, is not critical enough to bring down the network.

   c. Minor—is informational only.

8. Choose one or more components that caused the event from the **Component** drop-down list.
9. Choose the relevant event details from the **Details** drop-down list.

View the filtered events in Cisco SD-WAN Manager both as tabular and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, view the events in a heatmap format.

Set Advanced Event Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Events**.
2. Click the **Advanced Filter** option.

3. In the **Object Type** drop-down menu, choose either **Site** or **Device** for which you want to view events.
4. In the **Object List** drop-down menu, choose either **Site ID** or **Device IP** for which you want to view events.

   You can choose more than one site or device.
5. In the **Severity** drop-down menu, choose one or more event severity levels from the drop-down list.
6. In the **Type** drop-down menu, choose one or more event names from the drop-down list.
7. Click **Apply Filters** to view events that match the filter criteria.
8. The **Custom Filter Condition** enables you in filtering events based on the OR condition, for example, 1 OR 2 OR 3.
9. Click the **+** icon and add up to five filters.
10. Click the **Bin** icon to delete a filter.

View the filtered events in Cisco SD-WAN Manager both as tabular and graphical formats.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, view the events in a heatmap format.

Export Events

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

Cisco SD-WAN Manager downloads data from the events table to the default download location of your browser. The data is downloaded as a CSV file with the name *events-mm-dd-yyyy.csv*, where mm, dd, and yyyy are the month, day, and year that the file was downloaded.

Monitor Event Notifications

To monitor and control the event trace function for a specified SD-WAN subsystem, use the **monitor event-trace** command in privileged EXEC mode. Event trace provides the functionality to capture the SD-WAN traces between the SD-WAN daemons and SD-WAN subsystems. For more information on the commands, see monitor event-trace sdwan and show monitor event-trace sdwan.

ACL Log

Use the ACL Log screen to view logs for access lists (ACLs) configured on a router. Routers collect ACL logs every 10 minutes.

Set ACL Log Filters

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **ACL Log**.

   Cisco vManage Release 20.6.x and earlier: From the Cisco SD-WAN Manager menu, choose **Monitor** > **ACL Log**.
2. Click the **Filter**.

3. In the VPN field, choose the entity, for which you are collecting ACL logs, from the drop-down list. You can choose only one VPN.
4. Click **Search** to search for logs that match the filter criteria.

Cisco SD-WAN Manager displays a log of activities in table format.

Audit Logging

Table 4: Feature History

Feature Name	Release Information	Description
Compare Template Configuration Changes Using Audit Logs	Cisco IOS XE Catalyst SD-WAN 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. The **Config Diff** option shows configuration changes made to the template, comparing the current configuration and previous configuration. The **Config Diff** option is available for audit logs to view the configuration changes when a template is not attached to a device.
Enhancements to Audit Logging	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature introduces enhanced audit logging to monitor unauthorized login activity.

Information About Protecting Against Unauthorized Login Activity

Cisco SD-WAN Manager displays a log of activities both in table and graphical format.

These logs enable traceability which is essential in co-management environments and for governance purposes. These logs provide insights in the form of events which are generated based on the audit logs.

From Cisco Catalyst SD-WAN Manager Release 20.12.1, the audit logs are enhanced to capture high login frequency and failed login attempts to Cisco SD-WAN Manager.

Configure a Lockout Policy for Cisco SD-WAN Manager Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

1. Enter system configuration mode.

   system

2. Enter aaa configuration mode.

   aaa

3. Configure the lockout policy, which prevents new login attempts after reaching a threshold of failed attempts.

   The **fail-attempts** keyword indicates the number of failed attempts to log in. The **fail-interval** keyword indicates the time span in which to count failed login attempts. The **lockout-interval** keyword specifies how long Cisco SD-WAN Manager waits before allowing new login attempts.

   See aaa lockout-policy for information about the ranges and defaults for each parameter.

   lockout-policy lockout-interval *lockout-duration* **fail-interval** *fail-duration* **fail-attempts** *fail-count*

The following is a complete configuration example for a lockout policy:

```
system
 aaa
  lockout-policy
   lockout-interval 600
   fail-interval    60
   fail-attempts    5
  !
 !
!
```

In the above example, **fail-attempts** is 5, **fail-interval** is 60, and **lockout-interval** is 600. The result is that if there are 5 failed attempts to log in within 60 seconds, then the Cisco SD-WAN Manager does not allow additional attempts for a period of 600 seconds (10 minutes).

Verify a Lockout Policy for Cisco SD-WAN Manager

To verify the lockout policy configuration, use the **show running-config system aaa lockout-policy** command.

Configure a Login-Rate Alarm Threshold for Cisco SD-WAN Manager Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This procedure enables an alarm when the number of logins to the Cisco SD-WAN Manager reaches a specified threshold.

1. Enter system configuration mode.

   system

2. Enter alarms configuration mode.

```
alarms
```

3. Configure a login-rate threshold.

   The **interval** keyword indicates the time span in which to count logins to Cisco SD-WAN Manager. The **num-logins** keyword specifies the number of logins within the specified interval that trigger an alarm.

   See login-rate for information about the ranges for each parameter.

   ```
   login-rate {interval login-interval | num-logins login-count}
   ```

Note There is no default value for **login-interval** and **num-logins**.

The following is a complete example for configuring a login-rate threshold:

```
system
 alarms
  login-rate
  interval 60
  num-logins 3
 !
!
!
```

Verify a Login-Rate Alarm Threshold for Cisco SD-WAN Manager

To verify the login rate alarm configuration, use the **show running-config system alarms** command.

```
vmanage# show running-config system alarms
system
 alarms
  login-rate
    interval 60
      num-logins 3
      !
    !
  !
```

Monitor Notifications of Failed Login Attempts to Cisco SD-WAN Manager

To view the history of failed login attempts, use the **show alarms history** command.

In the following example, there were two failed login attempts, after which Cisco SD-WAN Manager prevented additional login attempts.

```
vmanage# show alarms history | inc aaa-user
07/10    16:07:18      aaa-login-anomaly    major    user-name:test    remote:host:192.0.2.1
07/10    16:07:10      aaa-login-anomaly    major    user-name:test    remote:host:192.0.2.1
07/10    16:07:00      aaa-user-locked      major    user-name:test    remote:host:192.0.2.1
```

Monitor System Login Rate Alarms

To view alarms configured by the **login-rate** command, showing when the number of logins to Cisco SD-WAN Manager exceeds a configured threshold, use the **show alarms history** command, and view alarms of type **system-login-rate**.

```
vmanage# show alarms history
```

```
DATE    TIME        TYPE                  SEVERITY    DETAILS
-----------------------------------------------------------------
07/10   16:08:05   system-login-rate      minor    num-logins:3 time-interval:60
login-message:3 logins were done in 0 hours 1 minutes 8 seconds
07/10   16:08:05   system-login-change    minor    user-name:admin    user-id:145
```

View Audit Log Information

1. From the Cisco SD-WAN Manager menu, choose **Monitor** > **Logs** > **Audit Log**.

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

Cisco SD-WAN Manager displays a log of activities both in table and graphical format.

2. Click **Filter** and choose one or more modules to filter the view.

   You can choose more than one **Module** type.

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

   Cisco SD-WAN Manager 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.

4. To view detailed information about any audit log, for the desired row in the table, click **...** and choose **Audit Log Details**.

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

5. To view configuration changes made to a **Template** type **Module**, for the desired row in the table, click **...** adjacent to a log row for a template module, and choose **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**.

Note You can view changes to previous and current configurations made only where the module type is template.

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

   Starting from Cisco IOS XE Catalyst SD-WAN 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 Log of Configuration Template Activities

To view a log of activities related to creation of configuration templates and the status of attaching configuration templates to devices:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Devices**.
2. Choose **WAN Edge List** or **Controllers**, and choose a device.
3. For the desired device, click **...** and choose **Template Log**.

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 Catalyst 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 SD-WAN Manager, 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 SD-WAN Manager menu, choose **Administration** > **Settings** and, ensure that **Data Stream** is enabled.
2. From the Cisco SD-WAN Manager 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 SD-WAN Manager 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//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1sauth.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//DmiA0d0JU1rOt91CMTVGkscm9wLSYQrI1s
```

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 Catalyst 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 SD-WAN Manager 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 Catalyst 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 5:

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

Note The SYSLOG format for viptela daemons before Cisco Catalyst SD-WAN Manager Release 20.15.x:

%<FACILITY>-<host>-<MNEMONIC>-<SEVERITY>-<SEVERITY-name>-<SEVERITY>-<MessageId>: <MESSAGE TEXT>ex:*Dec 11 09:36:27.358: %Cisco-SDWAN-NR-C8200-1N-4T-FTMD-5-NTCE-1000026: **HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src: 192.168.104.16/0 Dst: 192.168.104.20/0 Proto: 1 TOS: 0 LogReason: SDWAN_SERV_ICMP_EXCEPT_TS Count: 1Bytes: 114

New SYSLOG format for viptela daemons starting from Cisco Catalyst SD-WAN Manager Release 20.15.x:

%<FACILITY>-<SEVERITY>-<MNEMONIC>: <MESSAGE TEXT>ex: Dec 20 18:47:33.237: %SDWAN-5-FTMD : **HSL-LOGGING IMPLICIT-ACL** : VPN-0 Src: 10.1.17.14/12346 Dst: 192.168.60.100/12346 Proto: 17 TOS: 192 LogReason: SDWAN_SERV_UDP Count: 1Bytes: 171 Ingress-Interface: GigabitEthernet2 Egress-Interface: GigabitEthernet2

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

Cisco SD-WAN Manager Logs

Table 6: Feature History

Feature Name	Release Information	Description
Manage Log Size	Cisco Catalyst SD-WAN Manager Release 20.16.1	This feature lets you temporarily increase the log size for troubleshooting purposes.

When something of interest happens on a Cisco SD-WAN Manager device or a cluster, the device reports it. One of the ways it reports is by generating a logging message. Then the message is placed in a log file in the /var/log/nms directory on the local device.

Configure Cisco SD-WAN Manager Logs

Cisco SD-WAN Manager logs with a priority level of information to the local device's hard disk, is enabled by default. Log files are placed in the local /var/log/nms directory. By default, each log file is 16 MB in size. Cisco SD-WAN Manager rolls over and stores up to 10 log files every day. After creating 10 files, it discards the oldest one to make room for new Cisco SD-WAN Manager logs.

You can configure the following log files:

- vmanage-server
- vmanage-server-statistics
- vmanage-server-olap
- vmanage-server-deviceconfig-template
- vmanage-server-device-config

Manage Log Size

From Cisco Catalyst SD-WAN Manager Release 20.16.1, you can temporarily increase the log size to 250 MB for troubleshooting purposes. Use the Cisco Catalyst SD-WAN REST API call provided in the Cisco Developer Documentation.

When you restart Cisco SD-WAN Manager, the log size reverts to 16 MB by default.

View Cisco SD-WAN Manager Logs

1. From the Cisco SD-WAN Manager menu, choose **Tools** > **Operational Commands**.
2. Click **Generate Admin Tech for Manager** > **Logs** and click **Generate** to collect the logs from all the Cisco SD-WAN Managers in the system.

   Click the ellipsis icon under **Actions**, choose **Generate Admin Tech** > **Logs**, and click **Generate** to collect logs from a particular device in the system.
3. Click **Show admin-tech List** to view the progress of the download. You can access the file when it's available.

To view the contents of the Cisco SD-WAN Manager log file from the CLI, use the **show log** command. For example:

```
Device# show log nms/vmanage-server.log
```

Note All task logs, including activity logs, adminstration, and device logs, are always displayed in UTC timezone. This is the default and only supported timezone for these logs, irrespective of the Cisco SD-WAN Manager or local timezone settings.

Cisco SD-WAN Manager Log Files

Cisco SD-WAN Manager records logs that meet or exceed the default or configured priority in the /var/log/nms directory on the local device. Some of these files include:

- vmanage-server.log
- vmanage-appserver.log
- vmanage-server-olap.log
- vmanage-server-device-config.log
- vmanage-server-rest.log

Cisco SD-WAN Manager Log Format

Cisco SD-WAN Manager logs generated by the Cisco Catalyst SD-WAN software is of the following format:

```
                Date - Log Level - Restful API Tracing ID - Host Name - Class - Thread -
Tenant ID [Optional]
                 - message
```

Here is an example of a log entry using the local6 facility at the 'INFO' level:.

```
04-Apr-2023 10:22:27,969 CST INFO [af7c0465-1fca-4e6d-8d39-6c03b1357b4b] [vmanage_scale1]
[VmanageSyslogLogger] (default task-3459) |default| deviceAction: Request for action
```

View Log of Certificate Activities

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

To view the status of certificate-related activities, use the Cisco SD-WAN Manager **Configuration** > **Certificates** window.

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

Binary Trace for Cisco Catalyst SD-WAN Daemons

Table 7: Feature History

Feature Name	Release Information	Description
Binary Trace for Cisco Catalyst SD-WAN Daemons	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a	Binary trace enhances the troubleshooting of Cisco Catalyst SD-WAN daemons. Binary trace logs messages from the daemons in a binary format. Messages are logged faster in the binary format, improving the logging performance, and use lesser storage space than in the ASCII format. The binary trace CLI allows you to set the debug levels for additional process modules compared to the **debug** command. From Cisco IOS XE Catalyst SD-WAN Release 17.4.1a, binary trace is supported for the following Cisco Catalyst SD-WAN daemons: • fpmd • ftm • ompd • vdaemon **Note** Starting from Cisco Catalyst SD-WAN Control Components Release 20.15.1, when using the `debug vdaemon all` command, a warning will be displayed about the potential impact on the network performance. • cfgmgr

Binary trace collects messages from process modules and records the information in a binary format. You can configure the level at which binary trace logs messages and view the recorded messages for tracing and troubleshooting errors in process execution.

Binary trace improves run-time performance by recording messages faster in the binary format than is possible while recording messages in the ASCII format. The binary format also allows for more efficient storage than the ASCII format. The messages are decoded from the binary format to an ASCII format when you view or save the trace to file.

Supported Cisco Catalyst SD-WAN Daemons

Binary trace is supported for the following Cisco Catalyst SD-WAN daemons and their modules:

Cisco Catalyst SD-WAN Daemons	Supported from Release
• fpmd • ftm • ompd • vdaemon • cfgmgr	Cisco IOS XE Catalyst SD-WAN Release 17.4.1a

Configure Binary Trace Level

Configure the binary trace level for one or all modules of a Cisco Catalyst SD-WAN process on a specific hardware slot.

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **set platform software trace** *process slot module level*

Example:

```
Device# set platform software trace fpmd R0 config debug
```

Configures the trace level for one or all the modules of a Cisco Catalyst SD-WAN process executing on the specified hardware slot.

- *process*: Specify a Cisco Catalyst SD-WAN process from among fpmd, ftm, ompd, vdaemon, cfgmgr.
- *slot*: Hardware slot from which process messages must be logged.
- *module*: Configure the trace level for one or all the modules of the process.
- *level*: Select one of the following trace levels:
  - debug: Debug messages
  - emergency: Emergency possible message
  - error: Error messages
  - info: Informational messages

- noise: Maximum possible message
- notice: Notice messages
- verbose: Verbose debug messages
- warning: Warning messages

View Binary Trace Level

View the binary trace levels for the modules of a Cisco Catalyst SD-WAN process executing on a specific hardware slot.

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show platform software trace level** *process slot*

Example:

```
Device# show platform software trace level fpmd R0
```

Displays the binary trace levels for all the modules of the process on the specified hardware slot.

- *process*: Specify a Cisco Catalyst SD-WAN process from among fpmd, ftm, ompd, vdaemon, cfgmgr.
- *slot*: Hardware slot from which process messages must be logged.

View Messages Logged by Binary Trace for a Cisco Catalyst SD-WAN Process

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show logging process** *process-name* [*filtering-options*]

Example:

```
Device# show logging process fpmd internal fru R0 reverse
```

Displays logs of the specified process or processes.

For *process-name*, specify a process from among fpmd, ftm, ompd, vdaemon, cfgmgr. You can also specify a comma-separated list of processes, for example, `fpmd, ftm`.

If you do not specify any *filtering-options*, command displays logs of the binary trace level information and higher severity levels that have been collected in the last 10 minutes.

For more information on the filtering options, see the command page for **show logging process**.

View Messages Logged by Binary Trace for All Cisco Catalyst SD-WAN Processes

Before you begin

Access the SSH terminal for the device through Cisco SD-WAN Manager or open a telnet session to access the CLI.

Procedure

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode. Enter your password if prompted.

Step 2 **show logging profile sdwan** [*filtering-options*]

Example:

```
Device# show logging profile sdwan start last boot
```

Displays logs of all Cisco Catalyst SD-WAN processes and their modules in chronological order.

If you do not specify any *filtering-options*, command displays logs of the binary trace level information and higher severity levels that have been collected in the last 10 minutes.

For more information on the filtering options, see the command page for **show logging profile sdwan**.

Traffic Logs

Table 8: Feature History

Feature	Release Information	Description
Cisco Catalyst SD-WAN Analytics Traffic Logs Integration and Insights	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature introduces traffic logs and security connection event logs in SD-WAN Manager powered by SD-WAN Analytics for filtered data retrieval.

Information about traffic logs

Traffic logs is a network flow monitoring tool integrated into Cisco Catalyst SD-WAN Analytics. It allows authorized users to access and visualize filtered firewall connection event logs derived from voluminous flow records. Users can submit queries specifying criteria such as time frame, site name, devices to get logs on-demand.

Note Up until Cisco Catalyst SD-WAN Manager Release 20.14.1, Cisco SD-WAN Manager opens a new window for Cisco SD-WAN Analytics.

Note Cisco Catalyst SD-WAN Manager Release 20.15.1 and Cisco Catalyst SD-WAN Manager Release 20.16.1 do not support the traffic logs feature.

Note From Cisco Catalyst SD-WAN Manager Release 20.18.1, Cisco SD-WAN Manager displays Cisco SD-WAN Analytics using a dynamic navbar in a converged user interface. You can see the traffic logs Tab when Cisco SD-WAN Analytics is enabled. Click on this tab to render the Cisco SD-WAN Analytics page.

Click on any other Cisco SD-WAN Manager menu or tab to go back to Cisco SD-WAN Manager.

Benefits of traffic logs

- Provides detailed visibility into raw flow logs, including firewall connection events and related attributes.

- Supports scalable processing and analysis of high-volume flow data.
- Enables users to filter logs of interest to quickly narrow down large datasets, even across millions of records.
- Utilizes SD-WAN Analytics to deliver both the frontend and backend as a cloud-based solution.

Restrictions for traffic logs

- Only one request can be made at a time across the fabric.

  All users of the fabric have to wait for this request to complete.
- There are rate limits at the fabric level.

  24 requests can be made in a period of 24 hours, and 24 exports can be made in a period of 24 hours, which is calculated across all users of the fabric.
- Maximum of five devices can be queried at a time.
- Maximum time duration for filtering is seven days.
- The data fetched for a log query is limited to within the last month.
- Export is limited to 1,048,576 rows to be compatible with tools like Excel.

Generate traffic logs using Cisco SD-WAN Manager

Before you begin

In the Cisco SD-WAN Manager menu, go to **Adminstration** > **Settings** and enable **Cloud Services**.

Procedure

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

Step 2 Click the **Traffic Logs** tab.

Step 3 In the query builder section, specify the mandatory filters:

- Time period
- Site(s) (maximum five)
- Device(s) (maximum five)

Step 4 Click the **Get Logs** button.

Note
If available, the last traffic logs request would be fetched and visualized by default.

Table 9:

Field	Description
Event Time (in UTC)	Displays the exact date and time thta the event was logged, recorded in Coordinated Universal Time (UTC) for standardization.
Site	Displays the physical location, office, or branch where the event was generated.
Hostname	Displays the name given to a device on a network, which can be used to identify it. It can be up to 128 characters long.
System IP	Displays the IP address assigned to the system or device that generated the event log.
VPN ID	Displays an identifier (such as a number or string) representing the specific VPN tunnel or connection involved in the event.
Source IP	Displays the IP address from which the network traffic originated.
Destination IP	Displays the IP address to which the network traffic was sent.
Source Port	Displays the port number used by the source device in the network communication
Destination Port	Displays the port number used by the destination device in the network communication.
Protocol	Displays the communication protocol used for the network session.
Application Name	Displays the name of the application or service associated with the network traffic
Username/SGT	Displays the account name or ID of the user associated with the event, if available.
Firewall Rule	Displays the specific rule within the firewall that matched and processed the event.
FW Policy	Displays the name or identifier of the firewall policy that applies to the traffic or event.
FW Action	Displays the action taken by the firewall for this event.

Note

For the firewall attribute columns to be populated, you need to set NGFW policies up in Cisco SD-WAN Manager.

What to do next

Click the **Export** button to download the results for offline analysis.

Troubleshoot traffic logs

If you wish to troubleshoot traffic logs, contact Cisco TAC for assistance.

Safety Barriers

Table 10: Feature History

Feature	Release Information	Description
Safety barriers	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	Safety barriers protect the Cisco SD-WAN Controller during resource constraints by monitoring CPU, memory, and disk usage. When thresholds are exceeded, safety barriers generate alarms and restrict services that can further impact resource availability.

Safety Barriers

The safety barriers protect the Cisco Catalyst SD-WAN Controller when system resources such as CPU, memory, and disk experience heavy usage. This feature provides resource-safeguarding actions and generates alarms in Cisco SD-WAN Manager to prevent system-wide critical failures. This feature acts as a guard to maintain the stability and reliability of only Cisco Catalyst SD-WAN Controllers.

Safety barriers provide regulating mechanisms to prevent system meltdowns caused by uncontrolled resource consumption. You can configure safety barriers using CLI or CLI template:

```
Device (config)# system safety-barriers
```

Safety barriers are disabled by default. All CPU or memory restrictive actions take place only when the safety barrier is configured on Cisco Catalyst SD-WAN Controller.

CPU alarm and actions

A CPU Barrier alarm is generated when CPU usage exceeds the 80% threshold for 300 seconds. Restrictive actions for CPU and Memory occur only if the safety-barriers are configured.

The following CPU actions take place to avoid system failure:

- Under high CPU barrier conditions, any system or policy configurations from Cisco SD-WAN Manager are delayed and re-attempted for five minutes, before indicating the failure.

- The following show commands (internal and external) are rejected:
  - **show omp tlocs**
  - **show omp services**
  - **show omp routes**
  - **show omp ipv6-routes**
  - **show omp peer**
  - **show omp l2-statuses**
  - **show omp l2-services**
  - **show omp l2-routes**
  - **show tenant omp**
  - **show internal/support omp rib vroute**
  - **show internal/support omp rib-list**
  - **show internal/support ttmd groups**
  - **show internal/support ttmd links**
  - **show internal/support ttmd tlocs**
- **clear omp all** is rejected

Disk alarm and actions

A Disk Barrier alarm is generated when disk usage exceeds the 80% threshold for 5 seconds. The following disk actions take place to avoid system failure:

- Core files and admin tech files in the disk are cleaned up based on their age. Files are deleted in this order:
  - Admin techs and image files in home directories older than 2 days,
  - crash files in /var/crash/ older than 30 days,
  - admin tech files in /var/admin-tech older than 30 days,
  - crash files in /var/crash/ older than 7 days,
  - admin tech files in /var/admin-tech older than 7 days,
  - crash files in /var/crash/ older than 2 days
  - admin tech files in /var/admin-tech older than 2 days.

Memory alarm and actions

A Memory Barrier alarm is generated when memory usage exceeds the 80% threshold for 300 seconds. The following memory actions take place to avoid system failure:

- No new control connections are allowed for any new edge sites added to the overlay.
- Clear control connections are rejected.
- OMP peering is not allowed.
- No new RIB Ins (Routing Information Base) for existing peers are allowed.
- Configuration of Control-Policy sequences involving **Set TLOC**, **Set TLOC-List**, or **Set Service** is not allowed.

For more information about safety barrier alarms, refer to Alarm Details in the *Cisco IOS XE Catalyst SD-WAN Alarms Guide*.